ISSN 2616-7182

Л.Н. Гумилев атындағы Еуразия ұлттық университетінің

ХАБАРШЫСЫ

BULLETIN

of the L.N. Gumilyov Eurasian
National University

ВЕСТНИК

Евразийского национального
университета имени Л.Н. Гумилева

МАТЕМАТИКА. ИНФОРМАТИКА. МЕХАНИКА сериясы

MATHEMATICS. COMPUTER SCIENCE. MECHANICS Series

Серия **МАТЕМАТИКА. ИНФОРМАТИКА. МЕХАНИКА**

№2(123)/2018

1995 жылдан бастап шығады

Founded in 1995

Издается с 1995 года

Жылына 4 рет шығады

Published 4 times a year

Выходит 4 раза в год

Астана, 2018
Astana, 2018

Редакцияның мекенжайы: 010008, Қазақстан, Астана қ., Сәтпаев к-сі, 2, 408 бөлме.
Тел: (7172) 709-500 (ішкі 31-428). E-mail: *vest_math@enu.kz*

Жауапты хатшы, компьютерде беттеген
А. Нұрболат

Л.Н. Гумилев атындағы Еуразия ұлттық университетінің хабаршысы.
МАТЕМАТИКА. ИНФОРМАТИКА. МЕХАНИКА сериясы
Меншіктенуші: ҚР БжҒМ "Л.Н. Гумилев атындағы Еуразия ұлттық университеті" ШЖҚ РМК
Мерзімділігі: жылына 4 рет.
Қазақстан Республикасының Ақпарат және коммуникациялар министрлігімен тіркелген.
27.03.2018ж. № 17000-ж тіркеу куәлігі.
Тиражы: 20 дана
Типографияның мекенжайы: 010008, Қазақстан, Астана қ., Қажымұқан к-сі ,12/1,
тел: (7172)709-500 (ішкі 31-428).

Editorial address: 2, Satpayev str., of. 408, Astana, Kazakhstan, 010008
Tel.: (7172) 709-500 (ext. 31-428)
E-mail: *vest_ math@enu.kz*

Responsible secretary, computer layout:
A. Nurbolat

Bulletin of the L.N. Gumilyov Eurasian National University.
MATHEMATICS. COMPUTER SCIENCE. MECHANICS Series
Owner: Republican State Enterprise in the capacity of economic conduct "L.N. Gumilyov Eurasian National University" Ministry of Education and Science of the Republic of Kazakhstan
Periodicity: 4 times a year
Registered by the Ministry of Information and Communication of the Republic of Kazakhstan.
Registration certificate №17000-ж from 27.03.2018.
Circulation: 20 copies
Address of printing house: 12/1 Kazhimukan str., Astana, Kazakhstan 010008;
tel: (7172) 709-500 (ext.31-428).

Адрес редакции: 010008, Казахстан, г. Астана, ул. Сатпаева, 2, каб. 408
Тел: (7172) 709-500 (вн. 31-428). E-mail: *vest_ math@enu.kz*

Ответственный секретарь, компьютерная верстка
А. Нурболат

Вестник Евразийского национального университета имени Л.Н. Гумилева.
Серия МАТЕМАТИКА. ИНФОРМАТИКА. МЕХАНИКА
Собственник: РГП на ПХВ "Евразийский национальный университет имени Л.Н. Гумилева" МОН РК
Периодичность: 4 раза в год.
Зарегистрирован Министерством информации и коммуникаций Республики Казакстан.
Регистрационное свидетельство №17000-ж от 27.03.2018г.
Тираж: 20 экземпляров. Адрес типографии: 010008, Казахстан, г. Астана, ул. Кажымукана, 12/1, тел.: (7172)709-500 (вн.31-428).

Л.Н. ГУМИЛЕВ АТЫНДАҒЫ ЕУРАЗИЯ ҰЛТТЫҚ УНИВЕРСИТЕТІНІҢ ХАБАРШЫСЫ. МАТЕМАТИКА. ИНФОРМАТИКА. МЕХАНИКА СЕРИЯСЫ

№2(123)/2018

МАЗМҰНЫ

МАТЕМАТИКА-ИНФОРМАТИКА

Темиргалиев Н. Ковэю мен Макферсонның спектралды тесті кездейсоқтық талаптарын қандай мөлшерде қанағаттандырса, сондай дәрежеде кездейсоқ болатын Лехмердің сызықты конгруэнтті тізбегінің элементарлы құрылуы 8

Алексеева Л.А., Дадаева А.Н., Айнакеева Н.Ж. Термосерпімді стерженьдердің стационарлы емес динамикасы теңдеулерінің фундаментальді және жалпыланған шешімдері 56

Волосивец С.С., Голубов Б.И. Герц және Морри-Герц кеңістіктерінде бөлшектік модификацияланған Харди және Харди-Литтлвуд операторлары 66

Илолов М., Рахматов Дж.Ш. Айқын емес жылуөткізгіштік теңдеуі үшін бастапқы-шектік есеп туралы 71

BULLETIN OF L.N. GUMILYOV EURASIAN NATIONAL UNIVERSITY.
MATHEMATICS. COMPUTER SCIENCE. MECHANICS SERIES
№2(123)/2018

CONTENTS

MATHEMATICS-COMPUTER SCIENCE

Temirgaliyev N. Elementary construction of the linear congruent Lehmer sequence with the degree of randomness that is required by the spectral test of Coveyou and MacPherson 8

Alexeyeva L.A., Dadayeva A.N., Ainakeyeva N.Zh. Fundamental and generalized solutions of the equations of the non-stationary dynamics of thermoelastic rods 56

Volosivets S.S., Golubov B.I. Hardy and Hardy-Littlewood fractional modified operators in the Hertz and Morrey-Hertz spaces 66

Ilolov M., Rahmatov J.Sh. On initial-boundary problem for fuzzy heat equation 71

ВЕСТНИК ЕВРАЗИЙСКОГО НАЦИОНАЛЬНОГО УНИВЕРСИТЕТА ИМЕНИ Л.Н.ГУМИЛЕВА. СЕРИЯ МАТЕМАТИКА. ИНФОРМАТИКА. МЕХАНИКА

№2(123)/2018

СОДЕРЖАНИЕ

МАТЕМАТИКА-ИНФОРМАТИКА

Темиргалиев Н. Элементарное построение линейной конгруэнтной последовательности Лехмера с той степенью случайности, с какой требованиям случайности отвечает спектральный тест Ковэю и Макферсона 8

Алексеева Л.А., Дадаева А.Н.,Айнакеева Н.Ж. Фундаментальные и обобщенные решения уравнений нестационарной динамики термоупругих стержней 56

Волосивец С.С., Голубов Б.И. Дробные модифицированные операторы Харди и Харди-Литтлвуда в пространствах Герца и Морри-Герца 66

Илолов М., Рахматов Дж.Ш. О начально-граничной задаче для нечеткого уравнения теплопроводности 71

МАТЕМАТИКА-ИНФОРМАТИКА
MATHEMATICS-COMPUTER SCIENCE

.

Л.Н. Гумилев атындағы Еуразия ұлттық университетінің хабаршысы. Математика. Информатика. Механика сериясы, 2018, 2(123), 8-55 беттер
http://bulmathmc.enu.kz, E-mail: vest_math@enu.kz

МРНТИ: **28.17.19**

Н. Темиргалиев

Институт теоретической математики и научных вычислений,
Евразийский национальный университет им. Л. Н. Гумилева, Астана, Казахстан
(E-mail: ntmath10@mail. ru)

Элементарное построение линейной конгруэнтной последовательности Лехмера с той степенью случайности, с какой требованиям случайности отвечает спектральный тест Ковэю и Макферсона

Аннотация: Идеи случайного числа и случайной последовательности не поддаются абсолютной формализации. Взамен чего по тем или иным соображениям предлагаются массивы Генераторов случайных чисел, по ним создаются методы проверки (тестирования) их на случайность. Последовательности, прошедшие такой экзамен объявляются случайными, а каждый её элемент случайным числом, – в результате различных видов случайности столько, сколько проверочных тестов.

Статья посвящена полному решению задачи в постановках, объектах и продолжительной респектабельной историей исследования с поучительными выводами, в совокупности находящихся, надеемся, в высших эшелонах Компьютерных наук: Генератор Лехмера (1949 год) – один из самых популярных, если не самый популярный датчик и спектральный тест Ковею и Макферсона 1965 года создания как *«наиболее совершенный из имеющихся тестов»,* оба в связке с 50-летней историей, в развитии подробно изложенной во всех изданиях монографии *«Искусство программирования»* Дональда Эрвина Кнута с 1969 года по настоящее время, стало быть, бывшей в постоянной разработке. Именно, мало что проясняющая односторонняя оценка сверху главной числовой характеристики случайности ν_s с пессимистическим прогнозом *«было бы очень трудно вычислить точность* ν_s *, когда* $s \geq 10$ » заменена на неожидаемую асимптотическую при всех $s \geq 2$ – в чем в идеале состояла задача и в этом состоит её решение.

Генератор случайных чисел Лехмера или же *Линейная конгруэнтная последовательность* максимального периода есть, по определению, рекуррентная последовательность $\langle X_n \rangle$ целых неотрицательных чисел

$$X_{n+1} = (aX_n + c) \bmod N, n \geq 0, \tag{0.1}$$

где

$$N - \textit{модуль}\ 0 < N,\ a - \textit{множитель}\ 0 \leq a < N,$$
$$c - \textit{приращение}\ 0 \leq A < N, X_0 - \textit{начальное значение}\ 0 \leq X_0 < N,$$

целые числа $a > 1, N > a, \tau(a,N) \geq 2$ и $1 \leq \lambda(a,N) \equiv \frac{(a-1)^{\tau(a,N)}}{N} < (a-1)^{\tau(a,N)-1})$ связаны сравнениями $(a-1)^{\tau(a,N)} \equiv 0 \,(\mathrm{mod} N)$ и $(a-1)^{\tau(a,N)-1} \not\equiv 0 \ (\mathrm{mod} N)$.

Как это часто встречается, в этом случае тоже, вся проблема сводится к четко формулируемой математической задаче (все мотивировки и детали приведены в самом тексте статьи): при заданных $s \geq 2$ и $\tau \geq 2$ и растущем N найти асимтотику величины (все параметры – целые положительные числа)

$$\sup\left\{\nu_s(a,N) : 2 \leq a < N, (a-1)^{\tau} \equiv 0(\mathrm{mod} N), (a-1)^{\tau-1} \not\equiv 0(\mathrm{mod} N)\right\}, \tag{0.2}$$

где

$$\nu_s(a,N)=\inf\left\{\sqrt{m_1^2+\cdots+m_s^2}: m=(m_1,...,m_s)\in Z^s, m\neq 0, \sum_{j=1}^{s} m_j a^{j-1}\equiv 0\,(\mathrm{mod} N)\right\}.$$

Тем самым, задача заключается в указании числа $a=a(N)$ с как можно большим значением величины $\nu_s(a,N)$, тогда как при всех a,N и s известны только неравенства $\nu_s(a,N)\le \gamma(s)N^{\frac{1}{s}}$. Как и всякая оценка сверху, это неравенство может быть сильно завышенным, поэтому задачи не решает.

В данной работе в зависимости от всех возможных, и поэтому обеспечивающих полное решение исследуемой задачи, соотношений между параметрами s,τ и λ получены новые и окончательные результаты по спектральному тестированию (ST), носящие асимптотический характер:

$$\mathbf{ST}: \nu_2\left(a,N;(a-1)^2=N\right)=(a-1)\sqrt{1-2\frac{a-2}{(a-1)^2}}=\sqrt{N}\sqrt{1-2\frac{\sqrt{N}-1}{N}},$$

$$\mathbf{ST}\,(2\le s=\tau): N^{\frac{1}{s}}\left(1-(b_s-1)N^{-\frac{1}{s}}\right)=a-b_s\le \nu_s\left(a,N;(a-1)^s=N\right)\le$$

$$\le\sqrt{a^2+1}=N^{\frac{1}{s}}\sqrt{1+2N^{-\frac{1}{s}}+2N^{-\frac{2}{s}}},$$

$$\mathbf{ST}\,(2\le s<\tau,\lambda\ge 1): (N\lambda)^{\frac{1}{\tau}}\left(1-(b_s-1)(N\lambda)^{-\frac{1}{\tau}}\right)=(a-b_\tau)\le$$

$$\le\nu_s\left(a,N;(a-1)^\tau=N\lambda,1\le\lambda\le(a-1)^{\tau-s}\right)\le\sqrt{a^2+1}=(N\lambda)^{\frac{1}{\tau}}\sqrt{1+2(N\lambda)^{-\frac{1}{\tau}}+2(N\lambda)^{-\frac{2}{\tau}}},$$

$$\mathbf{ST}\,(s>\tau\ge 2,\lambda\ge 1): \nu_s\left(a,N;(a-1)^\tau=N\lambda,\lambda\ge 1\right)\le\sqrt{\sum_{k=0}^{\tau}\left(\binom{\tau}{k}\right)^2},$$

где $(-b_m)$ *есть наибольший по модулю отрицательный биномиальный коэффициент в разложении* $(a-1)^m$ *по степеням* a*:* $b_2=2,b_3=3,b_4=4,b_5=10,b_6=20,b_7=35,b_8=56$, $b_9=126,b_{10}=252,b_{11}=462,b_{12}=792,b_{13}=1716,b_{14}=3432,b_{15}=6435,...$ *и т. д.*

Все построения по этой теме в монографии Д. Кнута «Искусство программирования» носят полуэмпирический характер – выдвигаются теоретические положения на основе которых проводятся статистические эксперименты. К тому же, Д. Кнут на примере казалось бы несомненно случайного подбора параметров в методе *«середин квадратов»* фон Неймана приходит к выводу, что чисто экспериментальные поиски ненадежны и всегда нужна какая-то теория.

Нами проведено чисто теоретическое исследование.

Как это следует из оценок снизу во всех ST-утверждениях, все они с точностью стремящегося к 1 при возрастании N явно выписываемого (что имеет решающее значение в практических применениях) множителя $\overline{\gamma_N}$ имеют вид $\overline{\gamma_N}\cdot N^{\frac{1}{s}}\le\nu_s(a,N)$.

Это означает, что одновременно решены две задачи (с единственным ограничением – вычислительными возможностями компьютерной техники)

a. Количество случайных чисел N *должно и может быть произвольно большим,*

b. Основная характеристика случайности $\nu_s(a,N)$ *должна и может быть столь угодно большой при всех* $s\ge 2$.

При этом, главная часть $N^{\frac{1}{s}}$ величины s-мерной точности генератора $\langle X_n\rangle$ из-за малого показателя $1/s$, известного как *«проклятие размерности»*, требует от N в обратной к ней степени s быть большим (этим повторяется величина скорости приближения квадратурной формулы с равномерной сеткой и равными весами в численном интегрировании).

Возникает новая задача *«В каждом конкретном случае применения Генератора случайных чисел* (0.1)–(0.2) *выяснить, какими большими должны быть* N *и* $\nu_s(a,N)$ *?»*. Разумеется, это отдельная задача, быть может, даже нетривиальная.

Асимптотически точные оценки сверху $\nu_s(a,N) \leq \overline{\overline{\gamma_N}} \cdot N^{\frac{1}{s}} \left(\overline{\overline{\gamma_N}} \to 1\right)$ выступают в роли гаранта не взять N и $\nu_s(a,N)$ неоправданно большими с сопровождающими большими затратами при реализации.

За исключением случая $s = 2$ все ST-утверждения не точные, а асимптотические, что никак не ограничивает применений – требуются не точные значения N и $\nu_s(a,N)$, а только приблизительные в нужных по контексту случая границах.

Если от неосязаемой напрямую оценки $\nu_s(a,N)$ перейти к непосредственной проверке случайности через *«частотность»* (это свойство также называют *равномерной распределенностью*, от случайности требуется много больше), в которой числа $0,1,\ldots N-1$ надо переставить в другом порядке $X_0,\ldots,X_{N-1}$ как биективное отображение на себя таким образом, чтобы для любого сегмента $[\alpha,\beta]$ из $[0,1]$ количество чисел $\frac{X_n}{N}$ попавших в $[\alpha,\beta]$ должно быть близко $(\beta-\alpha)$, то обнаруживается, что всякая последовательность Лехмера с максимальным периодом изначально равномерно распределена с неулучшаемой оценкой отклонения $\frac{1}{N}$, что следует отнести к ее замечательным свойствам. Тем самым, проблематика заключается только в показателе случайности $\nu_s(a,N)$

Ключевые слова: Генератор случайных чисел Лехмера, спектральный тест Ковэю и Макферсона, линейная конгруэнтная последовательность, максимальный период, асимптотическое равенство, многомерная точность генератора случайных чисел.

§1. Введение, постановка задачи с её историей и основные результаты в статистической интерпретации

В математике и в компьютерных науках нет общего определения случайности числа и последовательностей чисел (как, впрочем, нет и определения алгоритма): вопрос *«Что такое случайная последовательность?»* в [1-2] так и остается без ответа в ключе *«Нужно предложить количественное определение случайного поведения»*.

Исследования в практической теории случайности с выходом на реальные последовательности разбиваются на два русла:

1. Предлагаются по тем или иным соображениям Генераторы случайных чисел, *«в известной мере зависящих от того, для каких применений служит эта последовательность».*
2. Создаются методы проверки (тестирования) Генераторов на случайность.

Последовательности, порожденные данным Генератором и выдержавшие данное тестовое испытание, объявляются случайными, а каждый её элемент случайным числом. В итоге, различных видов случайности столько, сколько проверочных тестов.

Конечно, в родственной теории вероятностей есть *случайная величина*, но это только специализированное название обычной измеримой числовой функции в Лебеговой теории меры. Также отметим, что если бы, например, требовалось установить непрерывность какой-либо функции, то надо проверить выполнение или невыполнение для этой функции однозначных, после Карла Вейерштрасса, требований в определении непрерывности (и больше ничего!). В связи с чем, по-видимому, целесообразно всегда называть *«Последовательность случайна по такому-то тесту»*, т.е. в каждом случае указывать по какому тесту данная числовая последовательность случайна.

В данной статье дано полное и, в известном смысле, окончательное решение проблемы тестирования методом Ковэю и Макферсона 1965 года создания Генератора Лехмера (1949 год) – одного из самых популярных, если не самого популярного датчика случайных чисел.

Результатом проведенного исследования является сведение задачи построения линейных конгруэнтных последовательностей случайных настолько, насколько требованиям случайности отвечает спектральный тест Ковэю и Макферсона, к элементарному подбору согласованной между собой пары – *«волшебных-магических»* целых положительных чисел, определяющих искомый Генератор Лехмера.

Тем самым, в статье решена задача с 50-летней историей в динамике попыток во времени подробно изложенной во всех изданиях монографии «Искусство программирования» Дональда Эрвина Кнута с 1969 года по настоящее время, стало быть, бывшей в постоянной разработке, когда неинформативная односторонняя оценка сверху главной числовой характеристики случайности заменена на всеобъемлющую асимптотическую, что никак не ожидалось, но было получено.

Перейдем к точным определениям и формулировкам. Поскольку по теме статьи требуются статистические обоснования и интерпретации, а также проводится критический анализ утверждений и положений по спектральному тестированию линейных конгруэнтных последовательностей с максимальным периодом, то, для большей точности, позволим себе обширное, надеемся без злоупотреблений, цитирование [1] и [2]. Также подчеркнем, что, за исключением $X_0 = 0$, все встречающиеся здесь параметры $a, N, c, s, \lambda, \tau$ и др. – целые положительные числа (независимо от того, сообщается об этом или нет).

Начнем с определения генератора случайных чисел ([2, стр. 29]): «*В настоящее время наиболее популярными генераторами случайных чисел являются генераторы, в которых используется следующая схема, предложенная Д. Г. Лехмером (D. H. Lehmer) в 1949 году [см. Proc. 2nd Symp. on Large-Scale Digital Calculating Machinary (Cambridge, Mass.: Harvard University Press, 1951, 141-146)]. Выберем четыре "волшебных числа":*

$$\begin{aligned} N,&\quad \textit{модуль}\quad 0 < N \\ a,&\quad \textit{множитель}\quad 0 \le a < N \\ c,&\quad \textit{приращение}\quad 0 \le c < N \\ X_0,&\quad \textit{начальное значение}\quad 0 \le X_0 < N. \end{aligned} \tag{1.1}$$

Затем получим желаемую последовательность случайных чисел $\langle X_n \rangle$, *полагая*

$$X_{n+1} = (aX_n + c) \bmod N, n \ge 0. \tag{1.2}$$

Эта последовательность называется ***линейной конгруэнтной последовательностью.***

Получение остатков по модулю N отчасти напоминает предопределенность, когда шарик попадает в ячейку крутящегося колеса рулетки».

По самому определению рекуррентных последовательностей, к которым относится и (1.2), первое повторение ранее встречавшегося числа образуют цикл, который затем повторяется бесконечное число раз. Это свойство присуще всем последовательностям вида $X_{n+1} = f(X_n)$, где f преобразует конечное множество само в себя (см. [1, стр. 23] и [2, стр. 29]). Повторяющийся цикл называется *периодом.*

В следующем критерии заключены все возможные способы выбора a и c в (1.1)-(1.2), которые дают максимальный период длины N (элегантное доказательство дано в [16]):

Теорема А. *Длина периода линейной конгруэнтной последовательности* (1.1)-(1.2) *равна N тогда и только тогда, когда*

i) c и N - взаимно простые числа;

ii) $a-1$ кратно p для любого простого p, являющегося делителем N;

iii) $a-1$ кратно 4, если N кратно 4.

Всюду ниже будем считать, что последовательность (1.1)-(1.2) удовлетворяет всем условиям теоремы А и, потому, имеет период длины N.

При этом, целые положительные числа a и N, удовлетворяющие теореме А, связаны сравнениями (см. [2, стр. 43-45], [1, стр. 36-39])

$$(a-1)^{\tau(a,N)} \equiv 0 \,(\mathrm{mod} N) \text{ и } (a-1)^{\tau(a,N)-1} \not\equiv 0 \,(\mathrm{mod} N), \tag{1.3}$$

где $\tau(a,N) \ge 2$.

Показатель $\tau(a,N)$, однозначно определяемый по a и N, называют *потенциалом* последовательности (1.1)–(1.2).

Далее, при заданных a и N, и зависящего от них $\tau(a,N)$, сравнения (1.3) также однозначно определяют целое $\lambda(a,N) \equiv \frac{(a-1)^{\tau(a,N)}}{N}$ такое, что

$$(a-1)^{\tau(a,N)} = N\lambda(a,N)(\tau(a,N) \geq 2, \quad 1 \leq \lambda(a,N) < (a-1)^{\tau(a,N)-1}). \tag{1.4}$$

Подчеркнем, и это требуется для дальнейшего, с любыми a и N, удовлетворяющими Теореме А, однозначно связаны два числа – потенциал $\tau(a,N) \geq 2$ и $\lambda(a,N) \geq 1$.

С позиций приведенных выше сведений, вернемся к определению (1.1)-(1.2) со свойством (1.3).

Линейная конгруэнтная последовательность с максимальным периодом N есть, по определению, реккурентная последовательность вычетов по модулю N

$$X_{n+1} = (aX_n + c) \bmod N\,(n = 0, 1, ..., N-1)\,, \tag{1.5}$$

зависящая от X_0, N, a и c, удовлетворяющих Теореме А. Саму же последовательность будем обозначать через разные эквивалентные записи

$$\langle X_n \rangle = \langle X_n\,(a,N,c,X_0)\rangle_{n=0}^{N-1} = \langle X_n\,(a,N)\rangle_{n=0}^{N-1} = \langle X_n\,(a,N)\rangle. \tag{1.6}$$

Если период последовательности (1.1) – (1.2) имеет длину N, что предполагается выполненным для (1.5), то в ней каждое из чисел $0, 1, ..., N-1$ появляется, понятно, ровно один раз. Стало быть, в этом случае выбор X_0 не влияет на длину периода, поэтому за X_0 можно принять любые из этих чисел, в данной статье условимся полагать $X_0 = 0$.

Также, $1 \leq c < N$ есть любое положительное целое, взаимно простое с N, которое, опятьже для определенности, можно полагать равным 1, что не исключает возможности в приложениях замены этих двух чисел на любое разрешенное другое.

После этих соглашений, последовательность зависит только от a и N, $2 \leq a < N$, поэтому из обозначений (1.6) оставим последнее (и, когда это не приведет к недоразумениям, то и короткое первое обозначение).

Саму конечную (периодическую с периодом N) последовательность (1.5) будем называть *«Генератор случайных чисел»*, или же, точнее, *«Генератор случайных чисел Лехмера»,* иногда коротко *«Генератор»* или *«последовательность $\langle X_n \rangle$»*, а также *«Линейная конгруэнтная последовательность» и «Линейный конгруэнтный метод».*

Разумеется, к последовательности (1.1)–(1.2), равно как и ко всем другим датчикам, предъявляются различные требования на случайность.

Многочисленные теоретические и эмпирические тесты на случайность, по крайней мере основные из них, подробно описаны в [1-2].

Все наше внимание будет сосредоточено на следующем из них [2, стр. 116, Раздел 3.3.4. **А. Идеи, служащие обоснованием критерия**]: *«Наиболее важные испытания для проверки, насколько случайной будет последовательность, связаны со свойствами совместных распределений s последовательных элементов последовательности, и спектральный критерий как раз и используется для проверки гипотез об этих распределениях. Если задана последовательность $U_n = \frac{X_n}{N}$ с периодом N, то для построения критерия необходимо проанализировать множество всех N точек $\{(U_n, U_{n+1}, ..., U_{n+s-1})\,|0 \leq n < N\}$ в s-мерном пространстве».*

Тем самым, появляется ещё один параметр $s \geq 2$, который отвечает за независимость последовательности s- мерных векторов

$$\left(X_n, X_{n+1}, ..., X_{n+(s-1)}\right),$$

в котором количественная характеристика независимости выражается через величину – ***s-мерную точность генератора случайных чисел,***

$$\nu_s\,(a,N) \equiv \nu_s\,(a,N;\ \textit{связь между}\ a,N,s,\tau,\lambda\ \textit{в виде}\ (a-1)^{\tau} = N\lambda\ \textit{из}\ (1.3)\text{–}(1.4))\,, \tag{1.7}$$

к мотивированному определению которого переходим (в более подробном изложении см. ниже в §2).

Математическим обоснованием *спектрального теста*, содержание которого составляет исследование величины, обозначенного в (1.7), служит *«конечное преобразование Фурье»* функций, описывающих идеальную и желательную случайности.

Именно, изучается спектр, т. е. *«номера»* $m = (m_1, \dots, m_s)$ *«больших коэффициентов Фурье* $\hat{f}(m)$ *»* (в данном случае не только ненулевых, но и со всеми значениями по абсолютной величине равными 1), - отсюда и название *«спектральный тест».*

В качестве меры *«случайности»* линейных конгруэнтных последовательностей (1.5) с множителем a и максимальным периодом N принимается величина (следует обратить особое внимание на то обстоятельство, что определение в своих мотивировках дается не для произвольных последовательностей (1.1)–(1.2), а только для имеющих максимальный период, что существенно используется при обосновании ST-метода(см. [1, стр. 107-108], формулы (1.6) – (1.8))):

$$\nu_s(a, N) = min\sqrt{m_1^2 + \cdots + m_s^2}, \tag{1.8}$$

где минимум берется по всем s-наборам целых чисел $(m_1, \dots, m_s)\,(m_1, \dots, m_s) \neq (0, 0, \dots, 0)$, являющихся решениями сравнения

$$m_1 + am_2 + \cdots + a^{s-1}m_s \equiv 0\,(mod N), \tag{1.9}$$

или, что то же самое, принадлежащих решетке (см. [12], К. Шерниязов)

$$\left\{ (m_1, ..., m_s) = (u_1, ..., u_s) \begin{pmatrix} N & 0 & \cdots & 0 \\ -a^2 & 1 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ -a^{s-1} & 0 & \dots & 1 \end{pmatrix} : \quad (u_1, u_2, ..., u_s) \in Z^s \right\},$$

вследствие чего (1.8) записывается в виде (см. [2, стр. 120] и [1, стр. 113])

$$\nu_s^2(a, N) = \inf\left\{ \left(Nu_1 - au_2 - \ldots - a^{s-1}u_s\right)^2 + u_2^2 + ... + u_s^2 : \ (u_1, ..., u_s) \neq (0, ..., 0) \right\}. \tag{1.10}$$

Сам спектральный критерий заключается в задаче нахождения минимального значения $\sqrt{m_1^2 + \ldots + m_s^2}$ в (1.8) по $(m_1, ..., m_s)$ из (1.9) , или же, что то же самое, величины (1.10).

Характеристика этого метода испытаний генераторов случайных чисел дана в [1, стр. 105] и [2, стр. 116]: «*Важный тест для проверки случайности полученных на ЭВМ числовых последовательностей сформулировали в 1965 г. Р. Ковэю и Р. Макферсон. Этот тест замечателен тем, что все известные плохие датчики, основанные на линейном конгруэнтном методе, были им забракованы, в то время как все хорошие датчики прошли удовлетворительно!*

Спектральный критерий является наиболее мощным известным до сих пор критерием и заслуживает особого внимания.

Спектральный критерий обладает свойствами как теоретических, так и эмпирических критериев, рассмотренных в предыдущих разделах. Он похож и на теоретические критерии, поскольку проверяет свойства последовательности на полном периоде, и на эмпирические критерии, поскольку для получения результата требует вычислений на компьютере».

Обращение к величине $\nu_s(a, N)$ вызвано тем фактом, что *«Если* ν_s *– наименьшее ненулевое значение «волнового числа»* $\sqrt{m_1^2 + \ldots + m_s^2}$ *для которого* $\hat{f}(m_1, \dots, m_s) \neq 0$ *в линейной конгруэнтной последовательности с максимальным периодом, то последовательность* $X_0/N, X_1/N, X_2/N, \dots$ *можно считать последовательностью случайных чисел, равномерно распределенных между 0 и 1 и представленных с «точностью» или с «ошибкой округления»* $1/\nu_s$ *, причем речь идет о независимости* s *последовательных значений* $X_n, X_{n+1}, ..., X_{n+(s-1)}$ *с усреднением по полному периоду»* (см. [1, стр. 108-109]).

Таким образом, задача заключается в нахождении в условиях (1.3)–(1.4) чисел a, N и s с как можно большим значением величины $\nu_s(a, N)$. В следующей теореме даётся оценка сверху(см. [1, стр. 108] и [2, стр. 133]):

Теорема В. *При всех* a, N *и* s *справедливы неравенства*

$$\nu_s(a, N) \leq \gamma_s N^{\frac{1}{s}}, \tag{1.11}$$

где γ_s *принимает значения*

$$(4/3)^{1/4}, 2^{1/6}, 2^{1/4}, 2^{3/10}, (64/3)^{1/12}, 2^{3/7}, 2^{1/2}$$

для $s = 2, 3, 4, 5, 6, 7, 8$ *соответственно.*

Как и всякая оценка сверху, неравенство (1.11) может быть сильно завышенным, поэтому задачи не решает(см. [1, стр. 111]): *«Так как никто не знает, каковы наилучшие достижимые значения* ν_s *, трудно точно определить, какие значения* ν_s *можно считать удовлетворительными».*

Дальнейшее развитие – в нарастании требований: *«До сих пор нельзя сказать, будет ли данный генератор случайных чисел на самом деле удовлетворять спектральному критерию. Успех этого испытания зависит от приложений, так как одни приложения предъявляют более высокие требования, чем другие. Если мы получим, что* $\nu_s \geq 2^{30/s}$ *для* $2 \leq s \leq 6$ *, то будет ли этого достаточно для большинства случаев (хотя автор должен признаться, что выбрал критерий отчасти потому, что 30 делится на 2, 3, 5 и 6) (см. [2, стр. 128])».*

Здесь, в теоремах 1-7 (см. ниже §3), будут даны найдены *«наилучшие достижимые значения* ν_s *».*

Перед тем как перейти к результатам статьи, ещё раз уточним постановку задачи в свете всего вышеизложенного.

Среди многочисленных формулировок проблемы спектрального тестирования генераторов случайных чисел, жирным шрифтом выделим последнее предложение с пессимистическим прогнозом из следующего абзаца в [2, стр. 118]: *«Спектральный критерий основан на значении* ν_s *для малых* s *, скажем,* $2 \leq s \leq 6$ *. Размерности 2, 3 и 4, кажется, адекватны для определения важных недостатков в последовательности. Но так как здесь рассматривается целый период, разумно в некоторой степени быть может осторожными и перейти к другому измерению (или двум). С другой стороны, значения* ν_s *при* $s \geq 10$ *, кажется, не имеют практического значения.* ***(И это хорошо, поскольку было бы очень трудно вычислить точность*** ν_s ***, когда*** $s \geq 10$ ***)****».*

Практическое значение этой тематики так описывается в [2, стр. 21]: *«В течение многих лет те, кому случайные числа были необходимы для научной работы, вынуждены были таскать шары из урны, предварительно хорошо перемешав их, либо бросать игральные кости, либо раскладывать карты. Таблица, содержащая более 40 000 взятых наудачу из отчетов о переписи случайных цифр, была опубликована в 1927 году Л.Х.К. Типпеттом (L.H.C. Tippett).*

С тех пор были построены механические генераторы случайных чисел. Первая такая машина была использована в 1939 году М.Ж. Кендаллом (M. G. Kendall) и Б. Бабингтон-Смитом (B. Babington-Smith) для построения таблицы, содержащей 100 000 случайных цифр. Компьютер Ferranti Mark I, впервые запущенный в 1951 году, имел встроенную программу, использующую резисторный генератор шума, которая поставляла 20 случайных битов на сумматор. Этот метод был предложен А.М. Тьюрингом (A.M. Turing). В 1955 году RANDCorporation опубликовала широко используемые таблицы, в которых содержался миллион случайных цифр, полученных с помощью других специальных устройств. Известный генератор случайных чисел ERNIE применялся на протяжении многих лет для определения выигрышных номеров британской лотереи. [См. статьи Kendall and Babington-Smith J. Royal Stat. Soc. A101 (1938), 147-166; B6 (1939), 51-61, а также дискуссию S. H. Lavington'scMarkIвCACM 21 (1978), 4-12; обозрениевMath. Comp. 10 (1956), 39-43; дискуссию об ERNIEW. E. Thomson, J. RoyalStat. Soc. A122 (1959), 301-333.]

Короче говоря, после изобретения компьютеров начались исследования эффективного способа получения случайных чисел, встроенных программно в компьютеры».

Особо подчеркнем, что здесь изучаются не все возможные последовательности (1.11)–(1.12), а только с максимальным периодом N , что не ограничивает общности, а отсекает менее ценные.

Точно также, определение (1.8)–(1.10) имеет смысл для всех целых положительных a, N и s , и именно для такого общего случая сформулирована Теорема В.

Итак, в условиях Теоремы А заданы произвольные целые положительные числа a и N, но связанные между собой условиями (1.3)–(1.4).

Здесь мы не можем удержаться от своего восторга этой теоремой, поскольку просто перемешать (без повторений!) числа $0,1,...,N-1$ в общем-то простой процедурой (1.5) с легко проверяемыми условиями (1.3) и потому очень доступными для применений a и N само по себе есть замечательный результат. Не менее удивительным представляется возможность выражения посредством конечного преобразования Фурье числового показателя $\nu_s(a,N)$ независимости s последовательных значений генератора случайных чисел (1.5) (по принципу *«Большие значения ν_s соответствуют случайности, малые – отсутствию случайности»*).

Конечно, сами по себе числовые показатели случайности $\nu_s(a,N)$ могут быть достаточно произвольными, но в спектральном тестировании все определяется связанными через условия (1.3)-(1.4) числами a и N в их взаимодействии с s.

Таким образом, вместе с принятыми соглашениями $A=1$ и $X_0=0$, параметры a и N однозначно определяют генератор случайных чисел. Затем, последовательность $\{X_n(a,N)\}_{n=0}^{N-1}$ подвергается испытанию на случайность методом спектрального тестирования при выбранном $s\geq 2$, для чего надо связать между собой параметры N,a и s.

Условия (1.3)–(1.4) определяют взаимосвязь между a и N через $\tau(a,N)$ и $\lambda(a,N)$. Поэтому исследуемая задача относительно s распадается на следующие попарно непересекающиеся случаи

$$\begin{aligned}
&1^\circ. \quad s=\tau(a,N)=2, \quad 1\leq\lambda(a,N),\\
&2^\circ. \quad s=\tau(a,N)\geq 3, \quad 1\leq\lambda(a,N),\\
&3^\circ. \quad 2\leq s<\tau(a,N), \quad 1\leq\lambda(a,N),\\
&4^\circ. \quad 2\leq\tau(a,N)<s, \quad 1\leq\lambda(a,N).
\end{aligned} \tag{1.12}$$

Теперь определимся с обозначениями. Как всегда Z^s будет означать целочисленную решетку евклидова пространства R^s, Z_0^s есть Z^s без точки $(0,...,0)$.

Через $A|B$ будем обозначать предложение « *A делит B* » с ее отрицанием в виде $A\not| B$.

Для положительных последовательностей A_N и B_N вводим обозначение $A_N\lesssim B_N$, если для всех задействованных N (и здесь, и всюду в этом абзаце) выполнено $A_N\leq\gamma_N B_N$, или, что то же самое, $\gamma_N^{-1}A_N\leq B_N$, где $\gamma_N\to 1$, стало быть, и $\gamma_N^{-1}\to 1$ при $N\to\infty$. Через $A_N\eqsim B_N$ будем обозначать одновременное выполнение $A_N\lesssim B_N$ и $B_N\lesssim A_N$. Также будем использовать знак Виноградова $A_N\ll B_N$ записи неравенства $A_N\leq c\cdot B_N$ при некотором $c>0$, и $A_N\asymp B_N$ при одновременном выполнении $A_N\ll B_N$ и $B_N\ll A_N$.

Всюду в статье будем полагать, что $(t\geq 1)\,1<p_1<\cdots<p_t$-простые числа, $\aleph_1,...,\aleph_t$ и $r_1,...,r_t$-целые положительные числа, $N=p_1^{\aleph_1}\cdots p_t^{\aleph_t}$ и $a=d\times p_1^{r_1}\cdots p_t^{r_t}+1$, где целое положительное число d взаимно просто с N, т. е. в разложении d на простые нет $p_1,...,p_t$.

Отметим, что ниже в формулировках теорем будут указаны точные значения γ_N, что обеспечивает эффективные вычислительные применения полученных результатов.

В данной статье получен полный ответ на вопрос истинном порядке $\nu_s\left(a,N;(a-1)^{\tau(a,N)}=N\lambda(a,N)\right)$ (эта проблема поставлена в 1969 году в [1], в последующих, спустя десятилетия, изданиях ответа на тот вопрос не находим).

Условия (1.3)–(1.4) обсуждаются в Лемме 10 в §3, однако нижеследующие теоремы 1-7 будут доказаны без учета этих условий. Сейчас же вернемся к основному объекту исследования этой статьи – линейным конгруэнтным последовательностям с максимальным периодом.

Итак, даны целые числа $a\geq 2, N>a$ и $s\geq 2$, по которым определяется функция

$$g_s(u_1,...,u_s)\equiv g_s(u_1,...,u_s;a,N)=\sqrt{(Nu_1-au_2-\cdots-a^{s-1}u_s)^2+u_2^2+\cdots+u_s^2}.$$

В следующих теоремах при различных связях вида $(a-1)^\tau=N\lambda$ между ними (впрочем, охватывающих все случаи в (1.12)) для величины

$$\nu_s(a,N;(a-1)^\tau=N\lambda)=\inf_{(u_1,...,u_s)\in Z_0^s,(a-1)^\tau=N\lambda} g_s(u_1,...,u_s;a,N)$$

находятся точное значение при $s = 2, \lambda = 1$ и (в остальных случаях) асимптотический порядок (с явно выписанными множителями $\gamma_N \to 1$ при них).

Перед тем как приступить к формулировкам теорем, обратимся к ещё одной характеристике случайности, выраженной уже через $\nu_s(a, N)$.

Мера эффективности $\mu_s(a, N)$ *множителя* a *для заданного максимального периода* N вводится как *«относительно независимое от* N *»*правило определения качества генератора случайных чисел N (см. [2, стр. 128]): *«В некоторых случаях хорошо бы иметь правило для определения, удовлетворяет ли датчик критерию, относительно независимое от* N *чтобы можно было сказать, что некоторый множитель хорош либо плох по отношению к другим множителям для заданного* N, *непроверяя остальных. Разумной мерой, заслуживающей быть показателем для определения, насколько хорош заданный генератор, мог бы быть объем эллипсоида в* s *- мерном пространстве, определенный соотношением*

$$\left(m_1 N - m_2 a - \cdots - m_s a^{s-1}\right)^2 + m_2^2 + \cdots + m_s^2 \le \nu_s^2,$$

так как этот объем стремится к вероятности того, что точка с ненулевыми целыми координатами $(m_1, ..., m_s)$, *которая соответствует решению (1. 9), находится в эллипсоиде. Поэтому предлагаем вычислить этот объем, а именно — показать, что онравен*

$$\mu_s = \frac{\pi^{s/2}\nu_s^s}{(s/2)!N},$$

и рассматривать его как меру эффективности множителя 0 *для заданного* N. *В этой формуле*

$$\left(\frac{s}{2}\right)! = \left(\frac{s}{2}\right)\left(\frac{s}{2} - 1\right)\cdots\left(\frac{1}{2}\right)\sqrt{\pi} \text{ для нечетных } s.$$

Таким образом, для размерностей, меньших или равных шести, эта мера имеет следующие значения:

$$\mu_2 = \pi\nu_2^2/N,\ \mu_3 = \tfrac{4}{3}\pi\nu_3^3/N,\ \mu_4 = \tfrac{1}{2}\pi^2\nu_4^4/N, \mu_5 = \tfrac{8}{15}\pi^2\nu_5^5/N,\ \mu = \tfrac{1}{6}\pi^2\nu_6^6/N\ ».$$

Сформулируем теоремы, в совокупности обеспечивающих *Элементарное построение линейной конгруэнтной последовательности настолько случайной, насколько требованиям случайности отвечает спектральный тест Ковэю и Макферсона с характеристикой* ***«Спектральный критерий является наиболее мощным известным до сих пор критерием и заслуживает особого внимания»***.

Теорема 1 (ST-2)**.** *Пусть дано целое число* $a \ge 5$ *и пусть* $(a-1)^2 = N$. *Тогда*

$$\begin{aligned}\nu_2\left(a, N; N = (a-1)^2\right) &= \sqrt{1 + (a-2)^2} = (a-1) \times \sqrt{1 - 2\frac{a-2}{(a-1)^2}} = \\ &= \sqrt{N - 2\sqrt{N} + 2} = \sqrt{N} \times \sqrt{1 - 2\frac{\sqrt{N}-1}{N}} \approx a \approx \sqrt{N}\end{aligned} \tag{1.13}$$

и

$$\mu_2\left(a; N; N = (a-1)^2\right) = \pi\left(1 - 2\frac{a-2}{(a-1)^2}\right) = \pi\left(1 - 2\frac{\sqrt{N}-1}{N}\right). \tag{1.14}$$

В теоремах 2–6 $(-b_m)$ *есть наибольший по модулю отрицательный биномиальный коэффициент в разложении* $(a-1)^m$ *по степеням* a : $b_2 = 2, b_3 = 3, b_4 = 4, b_5 = 10, b_6 = 20, b_7 = 35, b_8 = 56, b_9 = 126, b_{10} = 252, b_{11} = 462, b_{12} = 792, b_{13} = 1716, b_{14} = 3432, b_{15} = 6435$,... *и т. д.*

Теорема 2. *Пусть числа* $s \ge 3$, $a \ge b_s + 1$ *и* $N > a$ *связаны равенством* $(a-1)^s = N$. *Тогда выполнены следующие соотношения*

$$N^{\frac{1}{s}}\left(1 - (b_s - 1)N^{-\frac{1}{s}}\right) = a - b_s \le \nu_s(a, N; N = (a-1)^s) \le \sqrt{1 + a^2} = N^{\frac{1}{s}}\sqrt{1 + 2N^{-\frac{1}{s}} + 2N^{-\frac{2}{s}}}$$

и

$$\frac{\pi^{\frac{s}{2}}}{\left(\frac{s}{2}\right)!}\left(1-(b_s-1)\,N^{-\frac{1}{s}}\right)^s=\frac{\pi^{\frac{s}{2}}}{\left(\frac{s}{2}\right)!}\left(\frac{a-b_s}{a-1}\right)^s\le\mu_s\left(a,N;N=(a-1)^s\right)\le\frac{\pi^{\frac{s}{2}}}{\left(\frac{s}{2}\right)!}\cdot\frac{\left(1+a^2\right)^{\frac{s}{2}}}{(a-1)^s}=$$

$$=\frac{\pi^{\frac{s}{2}}}{\left(\frac{s}{2}\right)!}\cdot\left(1+2N^{-\frac{1}{s}}+2N^{-\frac{2}{s}}\right)^{\frac{s}{2}},$$

Теорема 3 ($s=\tau=2,\ \lambda\ge 2$). *Пусть параметры* a *и* N *связаны равенством* $(a-1)^2=N\lambda$, *где целое* $\lambda\ge 2$. *Тогда*

$$\sqrt{\frac{N}{\lambda}}\times\sqrt{1-2\frac{\sqrt{N\lambda}-1}{N\lambda}}=\frac{\sqrt{1+(a-2)^2}}{\lambda}\le\nu_2\left(a,N;(a-1)^2=N\lambda,\lambda\ge 2\right)\overset{\lambda|(a-1)}{\le}\frac{\sqrt{2}}{\lambda}(a-1)=\sqrt{\frac{2}{\lambda}}\cdot\sqrt{N},$$

$$\frac{\pi}{\lambda}\cdot\left(1-2\cdot\frac{\sqrt{N\lambda}-1}{N\lambda}\right)=\frac{\pi}{\lambda}\cdot\left(\frac{1+(a-2)^2}{(a-1)^2}\right)\le\mu_2\left(a,N:(a-1)^2=N\lambda,\lambda\ge 2\right)\overset{\lambda|(a-1)}{\le}\frac{2\pi}{\lambda},$$

где в оценке сверху требуется условие $\lambda|\,(a-1)\Leftrightarrow(a-1)\,|N$.

Теорема 4 ($\tau>s=2,(a-1)^\tau=N$). *Пусть даны числа* $\tau>s=2$, $a\ge b_\tau+1$ *и* $N>a$ *такие, что* $N=(a-1)^\tau$. *Тогда*

$$N^{\frac{1}{\tau}}\left(1-(b_\tau-1)\,N^{-\frac{1}{\tau}}\right)=a-b_\tau\le\nu_2\left(a,N;(a-1)^\tau=N\right)\le\sqrt{1+a^2}=N^{\frac{1}{\tau}}\sqrt{1+2N^{-\frac{1}{\tau}}+2N^{-\frac{2}{\tau}}},$$

$$\pi N^{\frac{2}{\tau}-1}\left(1-(b_\tau-1)\,N^{-\frac{1}{\tau}}\right)^2=\pi\frac{(a-b_\tau)^2}{(a-1)^\tau}\le\mu_2\left(a,N;(a-1)^\tau=N\right)\le$$

$$\le\pi\frac{\left(1+a^2\right)}{(a-1)^\tau}=\pi N^{\frac{2}{\tau}-1}\left(1+2N^{-\frac{1}{\tau}}+2N^{-\frac{2}{\tau}}\right).$$

Теорема 5 ($\tau=s\ge 2,\ (a-1)^s=N\lambda,\ \lambda\ge 1$). *Пусть числа* $a\ge b_s+1, N>a, s\ge 2$ *и* $\lambda\ge 2$ *таковы, что* $(a-1)^s=N\lambda$. *Тогда*

$$\frac{N^{\frac{1}{s}}}{\lambda^{1-\frac{1}{s}}}\sqrt{\sum_{k=0}^{s-1}\left(\binom{s-1}{k}\right)^2}=\frac{a-1}{\lambda}\sqrt{\sum_{k=0}^{s-1}\left(\binom{s-1}{k}\right)^2}\overset{\lambda|(a-1)}{\ge}\nu_s\left(a,N;(a-1)^s=N\lambda\right)\ge$$

$$\ge\frac{a-b_s}{\lambda}=\frac{N^{\frac{1}{s}}}{\lambda^{1-\frac{1}{s}}}\left(1-(b_s-1)\,(N\lambda)^{-\frac{1}{s}}\right),$$

и $(\tau=s\ge 2,\ (a-1)^s=N\lambda,\ \lambda\ge 1)$ *:*

$$\frac{\pi^{\frac{s}{2}}}{\left(\frac{s}{2}\right)!}\cdot\frac{1}{\lambda^{s-1}}\left(\sum_{k=0}^{s-1}\left(\binom{s-1}{k}\right)^2\right)^{\frac{s}{2}}=\frac{\pi^{\frac{s}{2}}}{\left(\frac{s}{2}\right)!}\cdot\frac{1}{\lambda^{s-1}}\cdot\frac{(a-b)^s}{(a-1)^s}\overset{\lambda|(a-1)}{\ge}\mu_s\left(a,N;(a-1)^s=N\lambda\right)\ge$$

$$\ge\frac{1}{\lambda^{s-2}}\cdot\left(\frac{a-bs}{a-1}\right)^s=\frac{\pi^{\frac{s}{2}}}{\left(\frac{s}{2}\right)!}\cdot\frac{1}{\lambda^{s-1}}\left(1-(b_s-1)\,(N\lambda)^{-\frac{1}{s}}\right)^s,$$

где в оценке сверху предполагается выполнение условия $\lambda|\,(a-1)\Leftrightarrow(a-1)^{\tau-1}|N$.

Теорема 6 ($2\le s<\tau,(a-1)^\tau=N\lambda,1\le\lambda\le(a-1)^{\tau-s}$). *Если* a,N,s,τ *и* λ *связаны равенством* $(a-1)^\tau=N\lambda$ *и неравенствами* $a\ge b_s+1,2\le s<\tau,1\le\lambda\le(a-1)^{\tau-s}$, *то*

$$(N\lambda)^{\frac{1}{\tau}}\left(1-(b_s-1)\,(N\lambda)^{-\frac{1}{\tau}}\right)=a-b_s\le\nu_s\left(a,N;(a-1)^\tau=N\lambda\right)\le\sqrt{1+a^2}=$$

$$=(N\lambda)^{\frac{1}{\tau}}\sqrt{1+2\,(N\lambda)^{-\frac{1}{\tau}}+2\,(N\lambda)^{-\frac{2}{\tau}}},$$

$$\frac{\pi^{\frac{s}{2}}}{\left(\frac{s}{2}\right)!}\frac{\left((N\lambda)^{\frac{1}{\tau}}\left(1-(b_s-1)\,(N\lambda)^{-\frac{1}{\tau}}\right)\right)^s}{N}=\frac{\pi^{\frac{s}{2}}}{\left(\frac{s}{2}\right)!}\frac{(a-b_s)^s\times\lambda}{(a-1)^\tau}\le\mu_s(a,N;(a-1)^\tau=N\lambda)\le$$

$$\leq \frac{\pi^{\frac{s}{2}}}{\left(\frac{s}{2}\right)!}\frac{\left(1+a^2\right)^{\frac{s}{2}}\times\lambda}{(a-1)^{\tau}} = \frac{\pi^{\frac{s}{2}}}{\left(\frac{s}{2}\right)!}\frac{\left((N\lambda)^{\frac{1}{\tau}}\sqrt{1+2\left(N\lambda\right)^{-\frac{1}{\tau}}+2\left(N\lambda\right)^{-\frac{2}{\tau}}}\right)^{s}}{N}$$

Если же $\lambda=(a-1)^{\tau-s+1}\times...\times(a-1)^{\tau-2}$, *то*

$$v_s(a,N;(a-1)^{\tau}=N\lambda,\lambda=(a-1)^{\tau-s+1},...,(a-1)^{\tau-2})\leq\sqrt{\sum_{k=0}^{s-1}\left(\binom{s-1}{k}\right)^2}$$

и

$$\mu_s(a,N;(a-1)^{\tau}=N\lambda,\lambda=(a-1)^{\tau-s+1}\times...\times(a-1)^{\tau-2})\leq\frac{\pi^{\frac{s}{2}}}{\left(\frac{s}{2}\right)!}\cdot\left(\sum_{k=0}^{s-1}\left(\binom{s-1}{k}\right)^2\right)^{\frac{s}{2}}\cdot\frac{1}{N}.$$

Теорема 7 ($2\leq\tau<s$, $(a-1)^{\tau}=N\lambda$, $\lambda\geq1$). *Пусть даны числа* $a,N>a,s,\tau$ *и* λ *такие, что* $(a-1)^{\tau}=N\lambda, 2\leq\tau<s,\lambda\geq1$. *Тогда*

$$\nu_s\left(a,N;(a-1)^{\tau}=N\lambda\right)\leq\sqrt{\sum_{k=0}^{\tau}\left(\binom{\tau}{k}\right)^2}$$

и

$$\mu_s\left(a,N;(a-1)^{\tau}=N\lambda\right)\leq\frac{\pi^{\frac{s}{2}}}{\left(\frac{s}{2}\right)!}\cdot\left(\sum_{k=0}^{\tau}\left(\binom{\tau}{k}\right)^2\right)^{\frac{s}{2}}\cdot\frac{1}{N}.$$

Как это следует из сформулированных теорем, Линейная конгруэнтная последовательность Лехмера с полным периодом "*волшебна*" при всех $2\leq s\leq\tau$ и теряет это свойство при $\tau<s$, да еще равномерно распределена.

Полученные здесь результаты меняют представление о *«Спектральном тесте»* как о методе *«определения важных недостатков»* в данной последовательности. Напротив, дают полный *«спектральный анализ»* всех возможных линейных конгруэнтных последовательностей с максимальным периодом и среди них выделяют наилучшие генераторы случайных чисел как *«эффективный способ получения случайных чисел, встроенных программно в компьютеры»*.

В каждом издании «Искусство программирования» Д. Кнута «Глава 3. Случайные числа» заканчивается вопросом в пункте 3.6 ВЫВОДЫ:

«В ЭТОЙ ГЛАВЕ было рассмотрено довольно много тем: генерирование случайных чисел, их проверка, их видоизменение при использовании и методы получения теоретических фактов. Возможно, главным для многих читателей был вопрос “Что получено в результате всей этой теории и что такое простой добротный генератор, который можно использовать в программах в качестве надежного источника случайных чисел?”.»

И, далее, на поставленный от имени читателей вопрос дается следующий ответ:

«Подробные исследования в этой главе наводят на хмысль, что следующая процедура позволяет получить простейший генератор случайных чисел для машинного языка большинства компьютеров. В начале программы присвойте целой переменной X *некоторое значение* X_0. *Эта величина* X *используется только для генерирования случайного числа. Как только в программе потребуется новое случайное число, положите*

$$X\leftarrow(aX+c)\bmod m \quad (1)$$

и используйте новое значение X *в качестве случайной величины. Необходимо тщательно выбрать* X_0,a,c *и* m *и разумно использовать случайные числа согласно следующим принципам.*

i) *"Начальное" число* X_0 *может быть выбрано произвольно. Если программа используется несколько раз и каждый раз требуются различные источники случайных чисел, то нужно присвоить* X_0 *последнее полученное значение* X *на предыдущем прогоне или, если это более удобно, присвоить* X_0 *текущие дату и время. Чтобы снова запустить программу с такими же случайными числами (например, при отладке программы), нужно напечатать* X_0, *если иначе его невозможно получить.*

ii) *Число* m *должно быть большим, скажем, по крайней мере* 2^{30}. *Возможно, удобно взять его равным размеру компьютерного слова, так как это делает вычисление* $(aX + c) \bmod m$ *вполне эффективным. В разделе 3.2.1.1 выбор* m *обсуждается более детально. Вычисление* $(aX + c) \bmod m$ *должно быть точным без округления ошибки.*

iii) *Если* m *- степень 2 (т. е. если используется двоичный компьютер), выбираем* a *таким, чтобы* $a \bmod 8 = 5$. *Если* m *- степень 10 (т. е. используется десятичный компьютер), выбираем* a *таким, чтобы* $a \bmod 200 = 21$. *Одновременный выбор* a *и* c *даст гарантию, что генератор случайных чисел будет вырабатывать все* m *различных возможных значений* X *прежде, чем они начнут повторяться (см. раздел 3.2.1.2), и гарантирует высокий "потенциал" (см. раздел 3.2.1.3).*

iv) *Множитель* a *предпочтительно выбирать между* $.01m$ *и* $.99m$, *и его двоичные или десятичные цифры не должны иметь простую регулярную структуру. Выбирая несколько случайных констант, подобных* $a = 3141592621$ *(которые удовлетворяют обоим условиям в (iii)), почти всегда получаем достаточно хороший множитель. Дополнительная проверка, конечно, нужна, если генератор случайных чисел используется регулярно. Например, частичные отношения не должны быть большими, когда для нахождения* $gsda$ *и* m *используется алгоритм Евклида (см. раздел 3.3.3). Множитель должен пройти спектральный критерий (раздел 3.3.4) и несколько критериев, описанных в разделе 3.3.2, прежде чем он получит сертификат качества.*

v) *Значение* c *не существенно, когда* a *- хороший множитель, за исключением того, что* c *не должно иметь общего множителя с* m, *когда* m *-размер компьютерного слова. Таким образом, можно выбрать* $c = 1$ *или* $c = a$. *Многие используют* $c = 0$ *вместе с* $m = 2^c$, *но они жертвуют двумя двоичными разрядами точности и половиной начальных значений, чтобы сэкономить всего несколько наносекунд счета (см. упр. 3.2.1. 2–9).*

vi) *Младшие значащие цифры (справа)* X *не очень случайны, так что решения, основанные на числе* X, *всегда должны опираться, главным образом, на старшие значащие цифры. Обычно лучше считать* X *случайной дробью* X/m *между* 0 *и* 1, *т. е. представлять себе* X *с десятичной точкой слева, а не относиться к* X *как к случайному целому числу между* 0 *и* $m - 1$. *Чтобы подсчитать случайное целое число между* 0 *и* $k - 1$, *нужно умножить его на* k *(но не делить на* k*; см. упр. 3.4. 1-3) и округлить результат.*

vii) *Важное ограничение случайности последовательности (1) обсуждалось в разделе 3.3.4, в котором показано, что "точность" при размерности* t *будет только порядка* $\sqrt[t]{m}$. *Применяя метод Монте-Карло, необходимо использовать случайные последовательности высокой надежности. Их можно получить с помощью технических приемов, описанных в разделе 3. 2. 2.*

viii) *Можно генерировать не больше* $m/1000$ *чисел, иначе последующие будут вести себя подобно предыдущим. Если* $m = 2^{32}$, *значит, новая схема (например, новый множитель a) должна использоваться после генерирования нескольких миллионов случайных чисел.»*

Разумеется, все сформулированные восемь «правил» относятся, главным образом, к машинному языку программирования. Но это уже отдельная эксплуатационная тема. Здесь для нас главное, что среди всего известного в теории случайности (понято, на момент написания книги) в качестве *«добротного»* и *«надежного»* для *«машинного языка большинства компьютеров»* выбран линейный конгруэнтный метод (1).

Не исключено, что это имеет такое объяснение: легко заметить, что Генератор Лехмера (1.2) получается от уравнения прямой $y = ax + c$ образованием рекуррентной последовательности заменами $x = X_n$ и $y = X_{n+1}$.

Многие другие генераторы, как например (см. [1, стр. 41]), *квадратичный конгруэнтный метод* $X_{n+1} = \left(dX_n^2 + aX_n + c\right) \bmod N$, порождаются такими же алгебраическими кривыми,

среди которых линейная функция самая простая, а порожденный ею генератор, согласно известному принципу, самый надежный.

На процитированный выше вопрос читателя и каждый раз обновляемый ответ Д. Кнута в количественно растущих «правилах», в данной статье даётся свой ответ с элементарным в несколько арифметических действий подбором основных параметров a и N через τ и λ при заданном s.

Именно, искомым *«простым и качественным датчиком»*будет выписываемыйв явном виде по целым положительным числам $\tau \geq 2$, $a \geq b_\tau + 1$ и $1 \leq \lambda \leq (a-1)^{\tau-1}$ Генератор случайных чисел

$$X_{n+1} = (aX_n + c)\, mod \frac{(a-1)^\tau}{\lambda} \left(n = 0, ..., \frac{(a-1)^\tau}{\lambda} - 1 \right),$$

где $X_0 = 0$, а $1 \leq c < (a-1)^\tau \,|\lambda$ – любое число, взаимно простое с $a-1$.

При этом, и в этом заключаются новые результаты по спектральному тестированию (ST), выбор параметров следующий:

ST-2: $\nu_2^2\left(a, N; (a-1)^2 = N\right) = (a-1)^2\left(1 - 2\frac{a-2}{(a-1)^2}\right) = N\left(1 - 2\frac{\sqrt{N}-1}{N}\right)$,

ST $(2 \leq s = \tau)$**:** $N^{\frac{2}{s}}\left(1 - (b_s - 1)\, N^{-\frac{1}{s}}\right)^2 = (a - b_s)^2 \leq \nu_s^2\,(a, N; (a-1)^s = N) \leq a^2 + 1 =$
$= N^{\frac{2}{s}}\left(1 + 2N^{-\frac{1}{s}} + 2N^{-\frac{2}{s}}\right)$.

ST $(2 \leq s < \tau, \lambda \geq 1)$**:** $(N\lambda)^{\frac{2}{\tau}}\left(1 - (b_s - 1)\,(N\lambda)^{-\frac{1}{\tau}}\right)^2 = (a - b_\tau)^2 \leq$
$\leq \nu_s^2\left(a, N; (a-1)^\tau = N\lambda, 1 \leq \lambda \leq (a-1)^{\tau-s}\right) \leq a^2 + 1 = (N\lambda)^{\frac{2}{\tau}}\left(1 + 2\,(N\lambda)^{-\frac{1}{\tau}} + 2\,(N\lambda)^{-\frac{2}{\tau}}\right)$,

ST $(s > \tau \geq 2, \lambda \geq 1)$**:** $\nu_s^2\,(a, N; (a-1)^\tau = N\lambda, \lambda \geq 1) \leq \sum_{k=0}^{\tau}\left(\begin{pmatrix} \tau \\ k \end{pmatrix}\right)^2$,

где $(-b_m)$ *есть наибольший по модулю отрицательный биномиальный коэффициент в разложении* $(a-1)^m$ *по степеням* a : $b_2 = 2, b_3 = 3, b_4 = 4, b_5 = 10, b_6 = 20, b_7 = 35, b_8 = 56, b_9 = 126, b_{10} = 252, b_{11} = 462, b_{12} = 792, b_{13} = 1716, b_{14} = 3432, b_{15} = 6435, ...$ *и т. д.*

Здесь во всех ST-утверждениях все оценки снизу с точностью стремящегося к 1 при возрастании N явно выписываемого (что имеет решающее значение в практических применениях) множителя $\gamma_N < 1$ имеют вид $\gamma_N N^{\frac{1}{s}} \leq \nu_s(a, N)$.

Тем самым решены две основные задачи

a. Количество случайных чисел N должно и может быть произвольно большим,

b. Основная характеристика случайности $\nu_s(a, N)$ при всех $s \geq 2$ должна и может быть столь угодно большой через надлежащий выбор N.

При этом, величина s-мерной точности генератора $\langle X_n \rangle$ из-за величины $N^{\frac{1}{s}}$ с «малым» показателем $\frac{1}{s}$ требует от N в обратной ей степени s быть большим. Это перекликается с величиной $N^{-\frac{1}{s}}$ дискренанса (см. например, [10]) – меры распределенности на единичном s-мерном кубе равномерной сетки с N узлами.

Далее, задачи *«**C. Вывод вычислительного метода** ([1, стр. 113]): Приведенные примеры иллюстрируют способы применения спектрального теста. Однако в наших рассуждениях остается, конечно, существенный пробел: существует ли хоть какая-нибудь возможность определить значение ν, затрачивая не слишком много машинного времени? Как, например, можно выяснить, что именно значениям $s_1 = 227$, $s_2 = 983$ и $s_3 = 130$ соответствует минимум суммы $s_1^2 + s_2^2 + s_3^2$ при соблюдении условия $s_1 + 3141592621 s_2 + 3141592621^2 s_3 \equiv 0\,(mod 10^{10})$? Очевидно, что о простом переборе не может быть и речи. »* и *«... построить алгоритм, который эффективно подсчитывает v_s [2, стр. 119]»* решены с превышением – даны формулы на уровне элементарного подсчета.

Поскольку с каждой парой параметров a и $N, a < N$, удовлетворяющих условиям теоремы А, единственным образом связаны числа $\tau\,(a, N) \geq 2$ (см. (1.3), а также Лемму 10), то, возвращаясь к условиям $(a-1)^{\tau(a,N)} = N\lambda\,(a, N)$ из (1.3)-(1.4), полагаяв формулировках теорем 1–7 $\tau = \tau\,(a, N)$ и $\lambda = \lambda\,(a, N)$, будем получать соответствующие результаты для

генератора случайных чисел (1.5) с максимальным периодом N, которые заново переписывать не будем и впредь будем пользоваться как доказанными теоремами, с сохранением их номеров.

В теоремах 3 и 5 в оценках сверху предполагается выполнение условия $\lambda|(a-1)$, откуда следует $N \not| (a-1)^{\tau(a,N)-1}$, т. е. второе условие в (1.3). Справедливые в этих условиях оценки сверху показывают, что соответствующие оценки снизу, вообще говоря, неулучшаемы в смысле асимптотического порядка, поэтому также могут служить основанием для принципиальных выводов.

В итоге, установленные для s-мерной точности $\nu_s(a,N)$ генератора случайных чисел ST-утверждения, снимают *«существенный пробел: существует ли хоть какая-нибудь возможность определить значение ν, затрачивая не слишком много машинного времени?»*.

Если s-точностью генератора случайных чисел $\nu_s \asymp N^{\frac{1}{\tau(a,N)}}$ при $2 \le s \le \tau(a,N)$ более-менее благополучно, то, как это показывают асимптотически точные ST-равенства, при фиксированных 0 и N, где N есть максимальный период генератора случайных чисел, вообще говоря, обеспечение одновременно высоких $\mu_s(a,N)$ для тех же $2 \le s \le \tau(a,N)$, в рамках возможного требуют отдельных вычислений в контексте Теоремы 6 (см. п. 3 из 8°).

Сделаем предварительные выводы из полученных здесь результатов (см. также §4-§5) в контексте концепции *«Только истинное значение ν_s определяет степень случайности»*, в соответствии с чем в [1-2]проведено большое количество теоретических разработок и компьютерных поисков, в которых генератор случайных чисел, т. е. множитель a и модуль N фиксируются и по ним при $s = 2, ..., 6$ вычислены $\nu_s(a,N), \lg \nu_s(a,N)$ и $\mu_s(a,N)$.

1°. В Теореме 1 при $s = 2$ в равенствах (1.13) и (1.14) при условии $N = (a-1)^2$ получены точные значения ν_2 и μ_2 соответственно. Поскольку при фиксированных a и N, $a < N$ величины $\nu_2(a,N) \ge \nu_3(a,N) \ge \dots$ образуют невозрастающую последовательность (см. Лемму 3), то $\nu_2(a,N)$ - наибольшая из них.

При $s = 2$ Теорема 1 (с дополнительными подтверждениями в последующих теоремах 3 и 4) показывает, что по отношению к генераторам случайных чисел с максимальным периодом, оценка в [1, стр. 109] и [2, стр. 133] $\nu_2(a,N) \le N^{\frac{1}{2}} \left(\frac{4}{3}\right)^{\frac{1}{4}}$ при всех N завышена и что на самом деле наименьшая верхняя граница $\nu_2(a,N)$ (наибольшая нижняя тоже!) в точности есть $N^{\frac{1}{2}}\sqrt{1-2\frac{\sqrt{N}-1}{N}}$ и для коэффициента при нем выполнены неравенства $\sqrt{1-2\frac{\sqrt{N}-1}{N}} < 1 < \left(\frac{4}{3}\right)^{\frac{1}{4}} = 1.07\dots$

Далее, обратимся к результатам компьютерного поиска из [2, стр. 130]: *В строках 16 и 23 расположены генераторы Лаво (Lavaux) и Йенсена (Janssens); параметры этих генераторов были найдены на компьютере, чтобы получить хороший множитель в смысле спектрального критерия, для которого μ_2 принимает очень большое значение:*

Таблица 1 – Выборочные результаты применения спектрального критерия

Строка	a	N	ν_2^2	μ_2
16	1664525	2^{32}	4938916874	3.61
23	31167285	2^{48}	3.2×10^{14}	3.60

Сравним эти данные с возможностями Теоремы 1. Согласно (1.13) для этих множителей a имеем:

Строка 16: $a = 1664525, N = (a-1)^2 = 2770640146576$ и $v_2^2 = (a-2)^2 + 1 = 2770636817530$ против 4938916874 в Таблице 1.

Строка 23: $a = 31167285, N = (a-1)^2 = 971399591936656$ и $v_2^2 = (a-2)^2 + 1 = 971399529602090 = 10^{14.987397\dots}$ против 3.2×10^{14} в Таблице 1.

По формуле (1.4) $\mu_2\left(a, N = (a-1)^2\right)$ может принимать сколь угодно близкие к своему, согласно ST-соотношениям, предельному значению – числу π: $\left|\pi - \mu_2\left(a, N = (a-1)^2\right)\right| = 2\pi\frac{a-2}{(a-1)^2} < \frac{2\pi}{a-2}$.

В частности, для множителя $a = 1664525$ из 16-ой строки имеем

$\mu_2\left(a=1664525, N=(a-1)^2=2770640146576\right) = \pi\left(1-0,000001201543984\right)$, против 3.61 Таблице 1, и, соответственно, для $a=31167285$ из 23 строки: $\mu_2(a=31167285, N=(a-1)^2 = 971399591936656) = \pi(1-2\frac{31167283}{971399591936656}) = \pi\left(1-0,000000064169850\right)$ против 3. 60 в Таблице 1.

2°. Ответ на решающий в спектральном тестировании вопрос: *«Так как никто не знает, каковы наилучшие достижимые значения ν_s »* [1, стр. 111] получен в Теореме 2: $\nu_s(a, N; (a-1)^s = N) \asymp N^{\frac{1}{s}}$ и $\mu_s\left(a, N; (a-1)^s = N\right) \tilde{\asymp} \pi^{\frac{s}{2}} / \left(\frac{s}{2}\right)!$.

Более того, как и в случае $s=2$, Теорема 2 при всех $s \geq 3$ позволяет уточнить константы γ_N из Теоремы B ([1, стр. 109] и [2, стр. 133]): если $N > \left(\frac{4}{\gamma^2(s)-1}\right)^s$, то $\overline{\gamma}_N(s) \equiv \sqrt{1+2\cdot N^{-\frac{1}{s}}+2N^{-\frac{2}{s}}} < \gamma(s)$, откуда

$$\begin{cases} s=3, & N \geq 3645 \Rightarrow \overline{\gamma}_N(3) < 2^{\frac{1}{6}}, \\ s=4, & N \geq 8697 \Rightarrow \overline{\gamma}_N(4) < 2^{\frac{1}{4}}, \\ s=5, & N \geq 28071 \Rightarrow \overline{\gamma}_N(5) < 2^{\frac{3}{10}}, \end{cases} \qquad \begin{cases} s=6, & N \geq 47206 \Rightarrow \overline{\gamma}_N(6) < \left(\frac{64}{3}\right)^{\frac{1}{12}}, \\ s=7, & N \geq 70730 \Rightarrow \overline{\gamma}_N(7) < 2^{\frac{3}{7}}, \\ s=8, & N \geq 75628488 \Rightarrow \overline{\gamma}_N(8) < 2^{\frac{1}{2}}. \end{cases}$$

То же самое происходит при всех $s \geq 9$, когда *«коэффициент»* $\sqrt{1+2N^{-\frac{1}{s}}+2N^{-\frac{2}{s}}}$ при $N^{\frac{1}{s}}$ во всех этих случаях, в отличие от случая $s=2$, сверху неограниченно приближается к 1 при неограниченном увеличении $N=(a-1)^s$.

В рамках Теоремы B после теорем 1 и 2 собственно можно было бы и закончить поиск *«волшебных-магических»* чисел с максимальным периодом, поскольку они фактически получены в форме
$\nu_s\left(a, N; N=(a-1)^s\right) \asymp N^{\frac{1}{s}} = a-1$ и $\mu_s\left(a, N\right) \asymp \pi^{\frac{s}{2}}\left(\frac{s}{2}\right)!$.

В свете теорем 1–2, вопрос о существовании в оставшихся случаях $2°-4°$ из (1.12) конкурентов к случаю $N=(a-1)^s$ с практической и теоретической точек зрения выглядят занятием малоперспективным, поскольку надо будет найти такие γ'_N и γ''_N, что

$$1-(b_s-1)N^{-\frac{1}{s}} = \overline{\overline{\gamma}}_N < \gamma''_N \leq 1 \leq \gamma'_N < \overline{\gamma}_N = \sqrt{1+2N^{-\frac{1}{s}}+2N^{-\frac{2}{s}}}.$$

Тем не менее, с целью получения полной картины поведения s-точности

$$\nu_s\left(a, N; (a-1)^{\tau(a,N)} = N\lambda(a,N)\right)$$

эти рассмотрения(в их числе и с последующими нетривиальными выводами по эмпирическим данным в [1-2]) продолжены в теоремах 3–7.

3°. Теоремы 3 и 4 в случае $s=2$ посвящены влиянию λ в $(a-1)^s = N\lambda$ и замене s на τ, $\tau > s$ в $(a-1)^s = N$ (при $s=2$ случай $\tau < s$ невозможен!).

При $s=2$ из теорем 3 и 4 следует, что ни увеличение $(a-1)^2$ посредством $\lambda \geq 2$ в $(a-1)^2 = N\lambda$, ни увеличение $\tau > s = 2$ в $(a-1)^\tau = N$ не только не дадут увеличения $\nu_2\left(a, N; (a-1)^2 = N\right) \asymp \sqrt{N}$, даже, наоборот, приведут к ухудшению на множители $\sqrt{\frac{2}{\lambda}}\,(\lambda \geq 2)$ и $N^{\frac{1}{2}-\frac{1}{\tau}}\,(\tau > 2)$ соответственно.

Таким образом, в основном, по-видимому, случае $s=2$, когда обеспечивается наибольшее количество потребностей, да еще дополненной независимостью векторов (X_n, X_{n+1}), наилучшим является генератор $\langle X_n(a,N)\rangle$, построенный по $a, N, a < N$, связанных равенством $(a-1)^2 = N$.

Последующие теоремы посвящены общему случаю $s \geq 2$.

4°. Асимптотически точная при $\lambda|(a-1)$ Теорема 5 даёт точную числовую информацию

$$\nu_s(a, N;\ (a-1)^s = N\lambda,\ 1 \leq \lambda < (a-1)^{s-1}) \tilde{\asymp} \frac{1}{\lambda^{1-\frac{1}{s}}} \cdot N^{\frac{1}{s}},$$

и, одновременно, в точных числовых данных показывает роль λ в соотношении $(a-1)^s = N\lambda$, а именно ухудшает рост $\nu_s(a,N)$ на точный множитель $1\lambda^{1-\frac{1}{s}}$.

5°. Теорема 6 при $\lambda = 1$ дает асимптотически точное решение задачи построения генератора $< X_n(a,N) >$ с одновременно большими $\nu_2(a,N),...,\nu_\tau(a,N)$ для произвольного $\tau > 2$. Именно, при заданных $\tau > 2$ и $M > 0$ надо выбрать a и $N, a < N$ из теоремы А такими, что $(a-1)^\tau = N$ и $N^{\frac{1}{\tau}}(1-(b_\tau-1)\cdot N^{-\frac{1}{\tau}}) > M$, и тогда для всех $s, 2 \le s \le \tau$ имеем $\nu_s(a,N) \ge M$, что следует изнеравенств

$$N^{\frac{1}{\tau}}(1-(b_\tau-1)\cdot N^{-\frac{1}{\tau}}) \le \nu_s(a,N;(a-1)^\tau = N) \le N^{\frac{1}{\tau}}\sqrt{1+2N^{-\frac{1}{\tau}}+2N^{-\frac{2}{\tau}}}\,(2 \le s \le \tau)\,. \quad (1.15)$$

Заключительная Теорема 7, в сочетании с предыдущими, приводит к следующим рекомендациям.

6°. Выводы по s-мерной точности генератора случайных чисел с максимальным периодом. Согласно теоремам 1-7 при $\lambda = 1$ и заданном $\tau(a,N)$ для всех s, $2 \le s \le \tau(a,N)$ будет выполнено асимптотическое равенство

$$\nu_s(a,N;(a-1)^{\tau(a,N)} = N) \asymp N^{\frac{1}{\tau(a,N)}}, \quad (1.16)$$

которое при $s > \tau(a,N)$ обрывается падением до

$$\nu_s(a,N;(a-1)^{\tau(a,N)} = N) \le \sqrt{\sum_{k=0}^{\tau(a,N)} \left(\binom{\tau(a,N)}{k}\right)^2}. \quad (1.17)$$

Подтверждением соотношений (1.15)–(1.17) служит

Таблица 2 – ВЫБОРОЧНЫЕ РЕЗУЛЬТАТЫ ПРИМЕНЕНИЯ СПЕКТРАЛЬНОГО КРИТЕРИЯ

Строка	a	N	ν_2^2	ν_3^2	ν_4^2	ν_5^2	ν_6^2
1	23	10^8+1	530	530	530	530	447
2	2^7+1	2^{35}	16642	16642	16642	15602	252
3	$2^{18}+1$	2^{35}	34359738368	6	4	4	4

Здесь во 2-ой строке $a-1 = 2^7$, $N = 2^{35}$, поэтому $\tau(a,N) = 5$. В соответствии с (1.15)–(1.16) одинаковые значения $\nu_2 = \nu_3 = \nu_4 = 16642$ с пиковым $\nu_5^2 = 15602$ сразу же, в соответствии с (1.17), заканчиваются падением до $\nu_6^2 = 252$.

Для сравнения приведем значения $\nu_s\left(a = 2^7+1, N = 2^{35}, (a-1)^5 = N\right)$, вычисленные по теоремам 1 и 3:

a	N	$\le \nu_2^2$	$\le \nu_3^2$	$\le \nu_4^2$	$\le \nu_5^2$	$\nu_6^2 \le$
2^7+1	2^{35}	16384	15876	15625	14161	252

Отметим, что и 1-ая строка таблицы 2, хотя $a-1 = 22 = 10^{1,342}, \tau = 5,961 \approx 6$ не полностью соответствуют требованию $N = 10^8+1 = (a-1)^\tau$, но при $s = 2,3,4,5$ все ν_s^2 равны 530 с небольшим искажением при $s = 6 \approx \tau$.

Тоже относитсяи к 3-ей строке, когда $\tau = \frac{35}{18} \approx 2$ и потому $\nu_2 = 34359738368$, опять же в согласии с (1.17) последующие ν_s^2 резко падают: $\nu_3^2 = 6, \nu_4^2 = \nu_5^2 = \nu_6^2 = 4$.

7°. Теоремы 5 и 6 выявляют интересную роль $\lambda > 1$ в $\nu_s\,(a,N;(a-1)^\tau = N\lambda)$: если при $\tau = s$ параметр $\lambda > 1$ приводит к уменьшению $N^{\frac{1}{\tau}}$ на множитель $1\Big/\lambda^{1-\frac{1}{s}}$, то при $\tau > s$, $1 \le \lambda \le (0-1)^{\tau-s}$ к увеличению в $\lambda^{\frac{1}{\tau}}$ раз.

В итоге – общая рекомендация по $\lambda \ge 1$: если $\nu_s(a,N), \mu_s\,(a,N)$ надо для одного $s \ge 2$ выбрать наибольшим, то a и N, $a < N$ должны быть связаны равенствами $\lambda = 1$ и $(a-1)^s = N$, если тоже требуется для $s, s+1, \dots s+l$, то выбор τ и λ в $(a-1)^\tau = N\lambda$ должен быть в соотношениях $\tau > s+l$ и $1 \le \lambda \le (a-1)^{\tau-(s+l)}$.

Объединим все предложенные частные рекомендации по построению наилучше возможных генераторов в одном общем.

8°. Правило построения генераторов случайных чисел $\langle X_n\,(a,N)\rangle$ с максимальным периодом по теоремам 1–7.

1. Если при данном $s, s \geq 2$ требуется построить генератор с наибольшим $\nu_s(a,N)$ и $\mu_s(a,N)$, то a и N, $a<N$ должны быть связаны равенством $(a-1)^s = N$, и тогда

$$\nu_2\left(a,N;N=(a-1)^2\right)=\sqrt{1+(a-2)^2}=(a-1)\times\sqrt{1-2\frac{a-2}{(a-1)^2}}=$$

$$=\sqrt{N-2\sqrt{N}+2}=\sqrt{N}\times\sqrt{1-2\frac{\sqrt{N}-1}{N}}\asymp a\asymp\sqrt{N},$$

$$\mu_2\left(a;N;N=(a-1)^2\right)=\pi\left(1-2\frac{a-2}{(a-1)^2}\right)=\pi\left(1-2\frac{\sqrt{N}-1}{N}\right),$$

и, далее, при всех $s, s\geq 3$

$$N^{\frac{1}{s}}\left(1-(b_s-1)N^{-\frac{1}{s}}\right)=a-b_s\leq\nu_s(a,N;N=(a-1)^s)\leq\sqrt{1+a^2}=N^{\frac{1}{s}}\sqrt{1+2N^{-\frac{1}{s}}+2N^{-\frac{2}{s}}},$$

$$\frac{\pi^{\frac{s}{2}}}{\left(\frac{s}{2}\right)!}\left(1-(b_s-1)N^{-\frac{1}{s}}\right)^s=\frac{\pi^{\frac{s}{2}}}{\left(\frac{s}{2}\right)!}\left(\frac{a-b_s}{a-1}\right)^s\leq\mu_s(a,N;N=(a-1)^s)\leq$$

$$\leq\frac{\pi^{\frac{s}{2}}}{\left(\frac{s}{2}\right)!}\cdot\frac{\left(1+a^2\right)^{\frac{s}{2}}}{(a-1)^s}=\frac{\pi^{\frac{s}{2}}}{\left(\frac{s}{2}\right)!}\cdot\left(1+2N^{-\frac{1}{s}}+2N^{-\frac{2}{s}}\right)^{\frac{s}{2}}.$$

Отметим, что при фиксированном s условие $(a-1)^s=N$ множителю $a=d\times p_1^{r_1}\dots p_t^{r_t}+1$ и максимальному периоду $N=d^s\times p_1^{sr_1}\dots p_t^{sr_t}$ предоставляют возможность быть сколь угодно большими.

2. Если при данном $\tau\geq 3$ требуется построить генератор *«с большими (гарантируется не меньше* $(N\lambda)^{\frac{1}{\tau+l}}\asymp a-b_{\tau+l}$ *)»* $v_2(a,N),\dots,v_\tau(a,N)$, то выбирая $a,N,l\geq 1, 1\leq\lambda\leq(a-1)^l=(N\lambda)^{\frac{l}{\tau+l}}$ такими, что $(a-1)^{\tau+l}=N\lambda$, получим при всех $2\leq s\leq\tau$

$$(N\lambda)^{\frac{1}{\tau+l}}\times\left(1-(b_{\tau+l}-1)(N\lambda)^{-\frac{1}{\tau+l}}\right)=a-b_{\tau+l}\leq v_s\left(a,N;(a-1)^{\tau+l}=N\lambda\right)\leq$$

$$\leq\sqrt{a^2+1}=(N\lambda)^{\frac{1}{\tau+l}}\sqrt{1+2(N\lambda)^{-\frac{1}{\tau+l}}+2(N\lambda)^{-\frac{2}{\tau+l}}}.$$

3. Если при данном $\tau\geq 2$ требуется построить генератор *«с большими (гарантируется не меньше* $\asymp\frac{\pi^{\frac{s}{2}}}{\left(\frac{s}{2}\right)!}\cdot\frac{\lambda^{\frac{1}{\tau+l}}}{N^{1-\frac{1}{\tau+l}}}$ *)»* $\mu_2(a,N),\dots,\mu_\tau(a,N)$, то выбирая a,N,l и λ такими, что $(a-1)^{\tau+l}=N\lambda, 1\leq\lambda\leq(a-1)^l=(N\lambda)^{\frac{l}{\tau+l}}$, получим при всех $2\leq s\leq\tau$

$$\frac{\pi^{\frac{s}{2}}}{\left(\frac{s}{2}\right)!}\cdot\frac{(N\lambda)^{\frac{s}{\tau+l}}}{N}\left(1-(b_s-1)(N\lambda)^{-\frac{1}{\tau+l}}\right)^s\leq\mu_s\left(a,N;(a-1)^{\tau+l}=N\lambda\right)=$$

$$=\frac{\pi^{\frac{s}{2}}}{\left(\frac{s}{2}\right)!}\cdot\frac{\nu_s^s\left(a,N;(a-1)^{\tau+l}=N\lambda\right)}{N}\leq\frac{\pi^{\frac{s}{2}}}{\left(\frac{s}{2}\right)!}\cdot\frac{(N\lambda)^{\frac{s}{\tau+l}}}{N}\left(1+2(N\lambda)^{-\frac{1}{\tau+l}}+2(N\lambda)^{-\frac{2}{\tau+l}}\right)^{\frac{s}{2}}.$$

Разумеется, здесь расчет на множитель $\lambda^{\frac{s}{\tau+l}}, 1\leq\lambda\leq(a-1)^l$.

Как это следует из Леммы 9, дальнейшее увеличение λ, вообще говоря, к увеличению $\mu_s\left(a,N;(a-1)^{\tau+l}=N\lambda\right)$ не приведет.

9°. Таким образом, асимптотическая формула ST теоретическии практически в явных асимптотических оценках обеспечивает полную свободу выбора N,s и a с предельно оптимальными показателями. Поэтому, эффективность применения переносится на технические возможности постоянно усовершенствуемых ЭВМ.

Здесь надо не упускать из виду, что, в отличие от неограниченных теоретических и вычислительных возможностей соотношений ST, тут произвол не совсем большой. Действительно, как это отмечено в [3, стр. 34], *«Если учесть, что время жизни Вселенной приблизительно равно 10 млрд.* $=10^{10}$ *лет* $<10^{18}$ *секунд, то ясно, что никакие самые фантастические скорости вычисления не обеспечат требуемой*

точности», в нашем случае $N = 10^{18} * k$, где k- количество действий компьютера в одну секунду: **Summit** , суперкомпьютер IBM, работающий в Национальной лаборатории Oak Ridge (DOHL) Министерства энергетики (DOE), занял первое место с производительностью **122, 3 петафлопса** на высокопроизводительном Linpack (HPL)(https://www.top500.org/lists/2018/06/).

10°. В связи с тем, что при всяком $s \geq 2$ величины N и $\nu_s(a,N)$ могут быть выбраны сколь угодно большими, возникает новая задача *«В каждом конкретном случае применения Генератора случайных чисел выяснить, какими большими должны быть N и $\nu_s(a,N)$?»*. Разумеется, это отдельная задача, быть может, даже нетривиальная.

Одновременно, асимптотически точные оценки сверху $\nu_s(a,N)$ через $N^{\frac{1}{s}}$ позволяют избежать неоправданно больших N и $\nu_s(a,N)$ с сопровождающими большими затратами на реализацию.

За исключением случая $s = 2$ все ST-утверждения не точные, а асимптотические, что никак не ограничивает применений – требуются не точные значения N и $\nu_s(a,N)$, а только приблизительные в нужных по контексту случая границах.

§2. Необходимые сведения по спектральному тестированию

Спектральный тест Р. Ковэю и Р. Макферсона [4] для проверки случайности последовательности $\{X_n\}$ с максимальным периодом N построен на следующих идеях [1 и 2, Раздел 3.3.4].

Для всякого целого положительного s на множестве $A_s \equiv \{t = (t_1, ..., t_s) : t_j = 0, ..., N-1 \ (j = 1, ..., s)\}$ предлагается следующая характеристика случайности

$$f(t_1, ..., t_s) = \frac{1}{N} \sum_{k=0}^{N-1} \delta_{X_k}(t_1) \cdots \delta_{X_{k+(s-1)}}(t_s), \tag{2.1}$$

где здесь и далее $\delta_M(x)$ равно 1 или 0 смотря по тому, кратно или не кратно число x числу M. Эта функция равна среднему арифметическому (плотности) появлений конкретной комбинации $(t_1, ..., t_s)$ в виде s следующих друг за другом членов последовательности $\langle X_n \rangle$: $(t_1, ..., t_s) = \left(X_n, ..., X_{n+(s-1)}\right)$.

В идеально случайной последовательности $\langle Y_n \rangle$ с равномерным распределением любые комбинации $(t_1, ..., t_s)$ должны появляться с одной и той же частотой, поэтому соответствующая ей согласно (2. 1) функция $y(t_1, ..., t_s) \equiv const$, где $const$ равна $\frac{1}{N^s}$. Действительно, каждая комбинация $t = (t_1, ..., t_s)$ в A_s ровно одна, таких же комбинаций всего N^s, поэтому частота, о которой идет речь, как отношение числа появления каждого t к числу всех имеющихся возможностей N^s есть $\frac{1}{N^s}$.

Далее, прямые конечные преобразования Фурье

$$\hat{f}(m_1, ..., m_s) = \sum_{0 \leq t_1, ..., t_s < N} \exp\left(\frac{-2\pi i}{N}(m_1 t_1 + \cdots + m_s t_s)\right) f(t_1, ..., t_s),$$

с возможностью полного однозначного восстановления функции f по формулам обратного конечного преобразования Фурье

$$f(t_1, ..., t_s) = \frac{1}{N^s} \sum_{\substack{m=(m_1,...,m_s): \\ 0 \leq m_j < N (j=1,...,s)}} \exp\left(\frac{2\pi i}{N}(m_1 t_1 + \cdots + m_s t_s)\right) \hat{f}(m_1, ..., m_s),$$

позволяют адекватно перенести исследования на Фурье-образы функции f с возможностью применения этого мощного аналитического аппарата.

Именно, поведение коэффициентов Фурье функции f, описывающей распределение значений изучаемой последовательности $< X_n >$, сравнивается с поведением коэффициентов Фурье функции $y(t) \equiv \frac{1}{N^s}$, описывающей идеально случайную последовательность.

Вычисления показывают (см. [1, Раздел 3.3.4А]), что для линейной конгруэнтной последовательности

$$X_{n+1} = (aX_n + c) \bmod N \ \ (n = 0, 1, 2, ...)$$

с максимальным периодом N коэффициенты Фурье функции f равны

$$\hat{f}(m_1,...,m_s)=\exp\left(\frac{-2\pi ic}{N}-\left(\frac{s(a,m)-s(1,m)}{a-1}\right)\right)\times\delta_N\left(m_1+am_2+\cdots+a^{s-1}m_s\right), \quad (2.2)$$

где $s(a,m)=m_1+am_2...+a^{s-1}m_s$.

Согласно определению $\delta_N(x)$ из (2.2) следует, что $\hat{f}(m_1,...,m_s)\neq 0$ тогда и только тогда, когда

$$m_1+am_2+\cdots+a^{s-1}m_s\equiv 0\,(modN), \quad (2.3)$$

причем во всех таких случаях $\left|\hat{f}(m)\right|=1$.

В то же время, коэффициенты Фурье $\hat{y}(m)\equiv\hat{y}(m_1,...,m_s)$ функции $y(t)$, отвечающей идеально случайной последовательности, в случае $m_j=0\,(modN)$ для всех $j=1,...,s$ равны 1 и равны 0 для всех остальных m.

В итоге, при $m\neq 0$ величины $\hat{f}(m)$ и $\hat{y}(m)$ отличаются друг от друга только при значениях $\hat{f}(m)\neq 0$, т. е. во всех точках множества

$$\begin{aligned}&\left\{m\in Z^s: m\neq 0,\ 0\leq m_j<N(j=1,...s)\ ,\hat{f}(m)\neq 0\right\}\equiv\\&\equiv\left\{m\in Z^s: m\neq 0,\ 0\leq m_j<N(j=1,...s), m_1+am_2+\cdots+a^{s-1}m_s\equiv 0\,(\mathrm{mod}N)\right\}.\end{aligned} \quad (2.4)$$

Предложение Р. Ковэю и Р. Макферсона, составляющее «спектральный тест», состояло в том, чтобы в качестве меры отклонения случайности данной последовательности от случайности идеальной принять наименьшее евклидово расстояние $\sqrt{m_1^2+\cdots+m_s^2}$ элементов множества (2.4) от нулевого $(0,...,0)$.

В связи с чем заметим, что если в спектральном тестировании через определенные по a и N сравнения (2. 3) надо как можно дальше отодвинуть от нуля «номера» m ненулевых коэффициенты Фурье, что измеряется в (1.8)–(1.9), то в численном интегрировании ситуация схожая.

Именно, a и N должны быть такими, чтобы имело место неравенство $(\overline{m}_j=\max\{1;|m_j|\})$

$$\sum_{m_1,...,m_s=-(N-1)}^{N-1}\frac{\delta_N\left(m_1+am_2+\cdots+a^{s-1}m_s\right)}{\overline{m}_1\cdots\overline{m}_s}\leq\frac{\ln^\beta N}{N}\,(\beta>0), \quad (2.5)$$

что будет выполнено, если для всех нетривиальных решений $m=(m_1,\ldots,m_s)$ сравнения (2.3) справедливо неравенств $\overline{m}_1\ldots\overline{m}_s\geq N$ (см. [5, стр. 126-127]).

Таким образом, если в спектральном тестировании нетривиальные решения $m=(m_1,\ldots,m_s)$ сравнения (2.3) должны иметь достаточно большие $\sqrt{m_1^2+\cdots+m_s^2}$, что составляет определение $\nu_s(a,N)$, то в численном интегрировании то же требуется для величины $\overline{m}_1\cdots\overline{m}_s$ в виде выполнения (2.5).

При этом будут достигаться свои цели: в спектральном тестировании – построение хороших генераторов случайных чисел $\langle X_n(a,N)\rangle$, в численном интегрировании по a и N определяются узлы $\left(\left\{\frac{k}{N}\right\},\left\{\frac{ak}{N}\right\},...,\left\{\frac{a^{s-1}k}{N}\right\}\right)$ $(k=1,...,N)$ хорошей квадратурной формулы с равными весами (здесь надо «обойти большие коэффициенты Фурье» классов функций с доминирующей смешанной производной, «номера» m которых образуют т. н. «гиперболические кресты», подробности см. в [5] и, современное состояние, в [6]), где $\{x\}$ есть дробная часть числа x.

В работах [7-12] те же задачи численного интегрирования решались через теорию дивизоров, или, что по сути то же самое, через решетки (что делается и в данной статье).

В данном исследовании основным является представление (1.10), которое при $a_j=a^{j-1}$ $(j=2,...,s)$ непосредственно следует из следующей теоремы, что является ещё одним свидетельством, как говорят [13, стр. 429], исторической надежности математической номенклатуры.

Теорема С (К. Шерниязов, [12]). *Пусть даны целое положительное число* s *и целые числа* $N \geq 2,\ a_1 = 1,\ a_2, ..., a_s$ *, и пусть*

$$V_{N,a_2,...,a_s} = \begin{pmatrix} N & 0 & \cdots & 0 \\ -a_2 & 1 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ -a_s & 0 & \dots & 1 \end{pmatrix}.$$

Тогда справедливы следующие утверждения:

1. *Для всякого вектора* $m = (m_1, m_2, ...m_s) \in Z^s$ *, удовлетворяющего соотношению*

$$m_1 + a_2 m_2 + \cdots + a_s^{s-1} m_s \equiv 0 \,(\mathrm{mod} N) \tag{2.6}$$

найдется вектор $u = (u_1, u_2, ...u_s) \in Z^s$ *такой, что* $m = uV_{N,a_2,...,a_s}$ *, причем для каждого* m *из* Z^s *, удовлетворяющего* (2.6)*, такой вектор и единственен.*

1. *Обратно, для любого* $u = (u_1, u_2, ...u_s) \in Z^s$ *вектор* $m = uV_{N,a_2,...,a_s}$ *является решением сравнения* (2.6).

Таким образом, всю доказательную часть этой статьи можно считать замкнутой по отношению к ИТМиНВ (разумеется, как говорят, «по модулю метода Ковэю-Макферсона»).

§3. Доказательства теорем

Лемма 1. *Справедливы тождества* $((a-1)^\tau = N\lambda)$

$$a - l = (N\lambda)^{\frac{1}{\tau}} \left(1 - (l-1)(N\lambda)^{-\frac{1}{\tau}}\right),$$

$$(a-l)^2 = (N\lambda)^{\frac{2}{\tau}} \left(1 - 2(l-1)(N\lambda)^{-\frac{1}{\tau}} + (l-1)^2 (N\lambda)^{-\frac{2}{\tau}}\right)$$

и

$$a^2 + 1 = (N\lambda)^{\frac{2}{\tau}} \left(1 + 2(N\lambda)^{-\frac{1}{\tau}} + 2(N\lambda)^{-\frac{2}{\tau}}\right).$$

Доказательство. Имеем

$$a - l = (a-l) - (l-1) = (N\lambda)^{\frac{1}{\tau}} - (l-1) = (N\lambda)^{\frac{1}{\tau}} \left(1 - (l-1)(N\lambda)^{-\frac{1}{\tau}}\right),$$

возведя в квадрат которое получаем равенство для $(a-l)^2$,

$$(a-l)^2 = (a-1+1-l)^2 = (a-1)^2 + 2(1-l)(a-1) + (1-l)^2.$$

Далее

$$a^2 + 1 = (a-1+1)^2 + 1 = (a-1)^2 + 2(a-1) + 2,$$

откуда при $(a-1)^\tau = N\lambda$,

$$(a-l)^2 = (N\lambda)^{\frac{2}{\tau}} - 2(l-1)(N\lambda)^{\frac{1}{\tau}} + (l-1)^2 = (N\lambda)^{\frac{2}{\tau}} \left(1 - 2(l-1)(N\lambda)^{-\frac{1}{\tau}} + (l-1)^2 (N\lambda)^{-\frac{2}{\tau}}\right)$$

и

$$a^2 + 1 = (N\lambda)^{\frac{2}{\tau}} + 2(N\lambda)^{\frac{1}{\tau}} + 2 = (N\lambda)^{\frac{2}{\tau}} \left(1 + 2(N\lambda)^{-\frac{1}{\tau}} + 2(N\lambda)^{-\frac{2}{\tau}}\right).$$

Теорема 1 (ST-2)**.** *Пусть дано целое число* $a \geq 5$ *и пусть* $(a-1)^2 = N$ *. Тогда*

$$\nu_2\left(a, N; N = (a-1)^2\right) = \sqrt{1 + (a-2)^2} = (a-1) \times \sqrt{1 - 2\frac{a-2}{(a-1)^2}} =$$

$$= \sqrt{N - 2\sqrt{N} + 2} = \sqrt{N} \times \sqrt{1 - 2\frac{\sqrt{N}-1}{N}} \asymp a \asymp \sqrt{N}$$

и

$$\mu_2\left(a; N; N = (a-1)^2\right) = \pi\left(1 - 2\frac{a-2}{(a-1)^2}\right) = \pi\left(1 - 2\frac{\sqrt{N}-1}{N}\right).$$

Доказательство теоремы 1. Напомним, что $N = (a-1)^2$ и

$$g_2^2(u_1, u_2) \equiv g_2^2(u_1, u_2; a, N) = (Nu_1 - au_2)^2 + u_2^2.$$

Если $u = (u_1,\ u_2) \neq (0,0)$ содержит один нуль, то

$$u_1 \neq 0,\ u_2 = 0 : g_2^2(u_1, 0) = (Nu_1 - a \cdot 0)^2 + 0^2 = N^2 u_1^2 \geq N^2 = g_2^2(1,0)$$

и

$$u_1 = 0,\ u_2 \neq 0 : g_2^2(0, u_2) = (N \cdot 0 - a \cdot u_2)^2 + u_2^2 = \left(a^2+1\right) u_2^2 \geq \left(a^2+1\right) = g_2^2(0,1).$$

Далее, $0 < a < N$ и потому $a + 1 \leq N$, откуда

$$g_2^2(0,1) = a^2 + 1 < a^2 + 1 + 2a = (a+1)^2 \leq N^2 = g_2^2(1,0).$$

Перейдем к случаю $u_1 \cdot u_2 \neq 0$. Если $u_1 \cdot u_2 < 0$, то при $u_1 \geq 1$ и $u_2 \leq -1$:

$$(Nu_1 - au_2)^2 = (Nu_1 + a(-u_2))^2 \geq N^2 u_1^2 \geq N^2,$$

поскольку $a(-u_2) > 0$. То же в случае $u_1 \leq -1, u_2 \geq 1$:

$$(Nu_1 - au_2)^2 = (-N(-u_1) - au_2)^2 = (N(-u_1) + au_2)^2 \geq (N(-u_1))^2 = N^2 u_1^2 \geq N^2,$$

ибо $au_2 > 0$ и $-u_1 \geq 1$.

Таким образом, в случае $u_1 \cdot u_2 < 0$ имеем $g_2^2(u_1, u_2) \geq N^2 > g_2^2(0,1)$.

Пусть теперь $u_1 \cdot u_2 > 0$. Тогда $u_1 \geq 1, u_2 \geq 1$ или $u_1 \leq -1, u_2 \leq -1$. Здесь второй случай сводится к первому:

$$(Nu_1 - au_2)^2 = ((-1)(Nu_1 - au_2))^2 = (N(-u_1) - a(-u_2))^2,$$

где $-u_1 \geq 1$ и $-u_2 \geq 1$.

В основном, получается, случае $u_1 \geq 1$, $u_2 \geq 1$ положим

$$g_2^2(x,y) = (Nx - ay)^2 + y^2, x \geq 1, y \geq 1.$$

Если $x \geq 1$ и $y > a$, то $y \geq a + 1$, и потому

$$g_2^2(x,y) \geq y^2 \geq (a+1)^2 = a^2 + 1 + 2a > a^2 + 1 = g^2(0,1).$$

Если $x \geq 2, 1 \leq y \leq a$ и $a \geq 5$, то

$$Nx - ay \geq 2N - a^2 = 2(a-1)^2 - a^2 = 2a^2 - 4a + 2 - a^2 =$$

$$= a(a-4) + 2 \geq a(5-4) + 2 = a + 2,$$

поэтому

$$g_2^2(x,y) \geq (a+2)^2 = a^2 + 2a + 4 > a^2 + 1 = g_2^2(0,1).$$

Следующий, последний, случай $x = 1,\ \ 1 \leq y \leq a$ сводится к нахождению минимума функции

$$\psi(y) \equiv g^2(1,y) = (N - ay)^2 + y^2$$

при $y = 1, \ldots, a$. Уравнение

$$\psi'(y) \equiv -2a(N - ay) + 2y = 0$$

и эквивалентные ей

$$-aN + a^2 y + y = 0$$

и

$$\left(1 + a^2\right) y = aN,$$

имеет корень $\overline{y}$,

$$\overline{y} = \frac{aN}{1+a^2} = \frac{a(a-1)^2}{a^2+1} = \frac{a\left(a^2-2a+1\right)}{a^2+1} = \frac{a^3+a-2a^2}{a^2+1} = \frac{a\left(a^2+1\right) - 2\left(a^2+1\right) + 2}{a^2+1} =$$

$$= a - 2 + \frac{2}{a^2+1} \quad \left(0 < \frac{2}{a^2+1} \leq \frac{2}{26} = \frac{1}{13}\right),$$

с целой частью $[\overline{y}]$,

$$5 = 3 + 2 \leq a \Leftrightarrow 1 < 3 \leq a - 2 = [\overline{y}] < a - 1 < a.$$

Поэтому, искомый минимум квадратичной функции $\psi(y)$ при $y=1,\dots,a$ есть меньшее из чисел $\psi(a-2)$ и $\psi(a-1)$. Имеем

$$\psi(a-2)=\left((a-1)^2-a(a-2)\right)^2+(a-2)^2=\left(a^2-2a+1-a^2+2a\right)^2+(a-2)^2=1+(a-2)^2$$

и

$$\psi(a-1)=\left(a^2-2a+1-a^2+a\right)^2+(a-1)^2=2(a-1)^2,$$

откуда

$$\psi(a-2)=(a-2)^2+1=a^2-4a+5<2a^2-4a+2=2(a-1)^2=\psi(a-1).$$

Все предыдущие значения $g_2^2(u_1,u_2)$ были не меньше $g_2^2(0,1)=1+a^2$, поэтому наименьшим значением будет

$$1+(a-2)^2=\psi(a-2)=g_2^2(1,(a-2))=g^2\left(1,\sqrt{N}-1\right).$$

Отсюда и из леммы 1 при $l=2$ следует искомое равенство

$$\nu_2\left(a,N;N=(a-1)^2\right)=g_2\left(1,\sqrt{N}-1\right)=\sqrt{1+(a-2)^2}=\sqrt{(a-1)^2-2(a-1)+2}=$$

$$=\sqrt{N-2\sqrt{N}+2}=\sqrt{N}\cdot\sqrt{1-2\cdot\frac{\sqrt{N}-1}{N}}.$$

И, наконец,

$$\mu_2\left(a,N;N=(a-1)^2\right)=\pi\frac{\nu_2^2\left(a,N;N=(a-1)^2\right)}{N}=\pi\frac{N-2\sqrt{N}+2}{N}=$$

$$=\pi\left(1-2\frac{\sqrt{N}-1}{N}\right)=\pi\frac{1+(a-2)^2}{(a-1)^2}=\pi\left(1-2\frac{a-2}{(a-1)^2}\right).$$

Теорема 1 доказана.

Теорема 2. *Пусть числа $s\geq 3, a\geq b_s+1$ и $N>a$ связаны равенством $(a-1)^s=N$. Тогда выполнены следующие соотношения*

$$N^{\frac{1}{s}}\left(1-(b_s-1)N^{-\frac{1}{s}}\right)=a-b_s\leq\nu_s(a,N;N=(a-1)^s)\leq\sqrt{1+a^2}=N^{\frac{1}{s}}\sqrt{1+2N^{-\frac{1}{s}}+2N^{-\frac{2}{s}}}$$

и

$$\frac{\pi^{\frac{s}{2}}}{\left(\frac{s}{2}\right)!}\left(1-(b_s-1)N^{-\frac{1}{s}}\right)^s=\frac{\pi^{\frac{s}{2}}}{\left(\frac{s}{2}\right)!}\left(\frac{a-b_s}{a-1}\right)^s\leq\mu_s(a,N;N=(a-1)^s)\leq$$

$$\leq\frac{\pi^{\frac{s}{2}}}{\left(\frac{s}{2}\right)!}\cdot\frac{\left(1+a^2\right)^{\frac{s}{2}}}{(a-1)^s}=\frac{\pi^{\frac{s}{2}}}{\left(\frac{s}{2}\right)!}\cdot\left(1+2N^{-\frac{1}{s}}+2N^{-\frac{2}{s}}\right)^{\frac{s}{2}},$$

где $(-b_s)$ есть наибольший по модулю отрицательный биномиальный коэффициент в разложении $(a-1)^s$ по степеням a: $b_2=2,b_3=3,b_4=4,b_5=10,b_6=20,b_7=35,b_8=56,b_9=126,b_{10}=252,b_{11}=462,b_{12}=792,b_{13}=1716,b_{14}=3432,b_{15}=6435,\dots$ и т. д.

Доказательство теоремы 2 начнем с оценки сверху дляпроизвольных $s\geq 3$ (см. также лемму 1):

$$\nu_s^2(a,N;N=(a-1)^s)\leq g_s^2(0,1,0,\dots,0)=1+a^2=N^{\frac{2}{s}}\left(1+2N^{-\frac{1}{s}}+2N^{-\frac{2}{s}}\right).$$

Доказательство оценки снизу проведем для двух значений s, равных четному 6 и нечетному 3, откуда будет ясен случай произвольных s.

Оценка снизу при $s=3,(a-1)^3=N$,

$$g_3^2(u_1,u_2,u_3)\equiv g_3^2(u_1,u_2,u_3;a,N)=\left(Nu_1-au_2-a^2u_3\right)+u_2^2+u_3^2.$$

Пусть сначала $u_1\neq 0$. Положим $|u_3|\leq a-l_3,|u_2|\leq a-l_2$. В этих условиях имеем ($|sgnu_1|=1$)

$$\left|Nu_1-au_2-a^2u_3\right|=|sgnu_1|\cdot\left|Nu_1-au_2-a^2u_3\right|=\left|N|u_1|-a^2\cdot u_3\cdot sgnu_1-a\cdot u_2\cdot sgnu_1\right|\geq$$

$$\geq N|u_1| - a^2|u_3| - a|u_2| \geq (a-1)^3 - a^2(a-l_3) - a(a-l_2) =$$
$$= a^3 - 3a^2 + 3a - 1 - a^3 + a^2 l_3 - a^2 + al_2 = a^2(-3 + l_3 - 1) + a(3 + l_2) - 1 =$$
$$= \|l_3 = 4, l_2 = 0\| = 3a - 1 \geq 2$$

при $a \geq 1$.

Поэтому в условиях $a \geq 4, |u_2| \leq a, |u_3| \leq a-4$ получаем $g_3^2(u_1,u_2,u_3) \geq (3a-1)^2 \geq 4$, откуда

$$g_3(u_1,u_2,u_3) \geq 3a - 1.$$

Если $|u_2| > a \Leftrightarrow |u_2| \geq a+1$, то при любом u_3 имеем

$$g_3^2(u_1,u_2,u_3) \geq u_2^2 \geq (a+1)^2 = a^2 + 1 + 2a > a^2 + 1 = g_3^2(0,1,0).$$

Если $a \geq 4$ и $|u_3| > a-4 \Leftrightarrow |u_3| \geq a-3 \geq 4-3 = 1$, то при любом u_2

$$g_3(u_1,u_2,u_3) \geq |u_3| \geq a - 3 \geq 1.$$

Далее, неравенство $1 + a^2 > (a-3)^2 = a^2 + 9 - 6a$ эквивалентно неравенству $6a > 8$, которое верно при $a \geq 4$, поэтому само тоже выполнено.

Таким образом, при $a \geq 4, u_1 \neq 0, u_2, u_3$ - произвольных

$$\sqrt{1+a^2} > a - 3, g_3(u_1,u_2,u_3) \geq a - 3 \left(u_1 \neq 0, (u_2,u_3) \in Z^2\right). \tag{3.1}$$

Теперь обратимся к случаю $u_1 = 0$. Начнем с подслучая $a \geq l \geq 0, u_1 = 0, u_3 \neq 0, |u_2| \leq a - l$, тогда

$$\left|au_2 + a^2 u_3\right| \geq a^2|u_3| - a|u_2| \geq a^2 - a(a-l) = a \cdot l,$$

стало быть,

$$g(0,u_2,u_3) \geq |au_2 + au_3| \geq a \cdot l.$$

Следующий случай, $a \geq l$, $u_1 = 0, u_3$? любое, $|u_2| > a - l \geq 0 \Leftrightarrow \Leftrightarrow |u_2| \geq a - l + 1 \geq 1$, и потому

$$g_3(0,u_2,u_3) \geq |u_2| \geq a - l + 1.$$

И, наконец, $u_1 = 0, u_3 = 0, u_2 \neq 0$

$$g_3(0,u_2,0) \geq \sqrt{1+a^2} = g_3(0,1,0).$$

Таким образом, при $u_1 = 0$ и произвольных u_2, u_3 $(|u_2| + |u_3| \geq 1)$ выполнено

$$g(0,u_2,u_3) \geq \min\left\{al; a - l + 1; \sqrt{1+a^2}\right\}.$$

Займемся нахождением этого min при $l = 4$. Тогда

$$4a > a - l + 1 = a - 3,$$

что вместе с первой частью (3.1) приводит к выводу:

если $a \geq 4$, то при $u_1 = 0$ и при произвольных u_2 и u_3

$$g_3(0,u_2,u_3) \geq a - 3.$$

Отсюда, вместе со второй частью (3.1), для любых $(u_1,u_2,u_3) \in Z_0^3$ получаем неравенство

$$g_3(u_1,u_2,u_3) \geq \min\left\{a-3, \sqrt{a^2+1}\right\} = a - 3 = N^{\frac{1}{3}} - 2,$$

стало быть,

$$\nu_3(a,N;(a-1)^3 = N) \geq a - 3 = (a-1) - 2 = N^{\frac{1}{3}} - 2 = N^{\frac{1}{3}}(1 - 2N^{-\frac{1}{3}}). \tag{3.2}$$

Перейдем к случаю $s = 6, (a-1)^6 = N$,

$$g_6^2 \equiv g_6^2(u_1,...,u_6) \equiv g_6^2(u_1,...,u_6;a,N) = \left(Nu_1 - au_2 - a^2u_3 - \cdots - a^5u_6\right)^2 + u_2^2 + \cdots + u_6^2.$$

Начнем со случая $u_1 \neq 0, u_2, u_3, u_4, u_5, u_6$ - любые, которые имеют подслучаи и подподслучаи.

Пусть

$$|u_j| \leq a - l_j \, (j = 2,...,6), \tag{3.3}$$

где целые числа l_j подберем позже.

Как и в случае $s=3$, вписывая $|sgnu_1|=1$ во внутрь модуля $\left|Nu_1-au_2-\cdots-a^5u_6\right|$, будем иметь

$$\left|Nu_1-a^5u_6-a^4u_5-a^3u_4-a^2u_3-au_2\right|\geq N|u_1|-a^5|u_6|-a^4|u_5|-a^3|u_4|-a^2|u_3|-a|u_2|=$$

$$=(a-1)^6|u_1|-a^5|u_6|-a^4|u_5|-a^3|u_4|-a^2|u_3|-a|u_2|\geq a^6-6a^5+15a^4-20a^3+15a^2-6a+1-$$

$$-a^5(a-l_6)-a^4(a-l_5)-a^3(a-l_4)-a^2(a-l_3)-a(a-l_2)=$$

$$=a^6-a^6+a^5(-6+l_6-1)+a^4(15+l_5-1)+a^3(-20+l_4-1)+a^2(15+l_3-1)+a(-6+l_2)+1.$$

Теперь целые $l_2,...,l_6$ выберем такими, чтобы последняя сумма была равна $a+1$, тогда

$$l_6=7,l_5=-14,l_4=21,l_3=-14,l_2=7. \tag{3.4}$$

Отсюда, в условиях (3.3)–(3.4) получаем

$$g_6^2\equiv g_6^2(u_1,u_2,u_3,u_4,u_5,u_6)\geq(a+1)^2, \tag{3.5}$$

после чего остаются 5 случаев

$$u_1\neq0,|u_j|\geq a-l_j+1\,(j=2,...,6), \tag{3.6}$$

каждое из которых соответственно влечет выполнение неравенства

$$g_6=g_6(u_1,u_2,u_3,u_4,u_5,u_6)\geq|u_j|\geq a-l_j+1. \tag{3.7}$$

При $j=2,3,4,5,6$, согласно (3.4), неравенства (3.6)–(3.7) соответственно следующие

$$g_6\geq|u_2|\geq a-6,$$

$$g_6\geq|u_3|\geq a+15,$$

$$g_6\geq|u_4|\geq a-20,$$

$$g_6\geq|u_5|\geq a+15,$$

$$g_6\geq|u_6|\geq a-6.$$

Оставляя здесь наименьшую в правой части величину, а именно $(a-20)$ и потому полагая $a\geq21$, отсюда, из неравенств $\sqrt{1+a^2}>a>a-20$ и (3.5) выводим, что при всех $u_1\neq0,u_2,u_3,u_4,u_5,u_6$ справедливо неравенство

$$a\geq21,g_6(u_1,u_2,u_3,u_4,u_5,u_6)\geq a-20\left(u_1\neq0,(u_2,...,u_6)\in Z^5\right). \tag{3.8}$$

В случае $u_1=0$ при произвольных u_2,u_3,u_4,u_5,u_6 имеем

$$g_6^2(0,u_2,u_3,u_4,u_5,u_6)=\left(a^5u_6+a^4u_5+a^3u_4+a^2u_3+au_2\right)^2+u_6^2+u_5^2+u_4^2+u_3^2+u_2^2. \tag{3.9}$$

Опять же, полагая

$$a\geq l_j,u_6\neq0,|u_j|\leq a-l_j\,(j=2,...,5)$$

и внося $sgnu_6\neq0$ под корень квадратный из первого слагаемого в (3.9), будем иметь

$$g_6(0,u_2,u_3,u_4,u_5,u_6)\geq a^5|u_6|-a^4|u_5|-a^3|u_4|-a^2|u_3|-a|u_2|\geq$$

$$\geq a^5-a^4(a-l_5)-a^3(a-l_4)-a^2(a-l_3)-$$

$$-a(a-l_2)=a^5-a^5-a^4(-l_5+1)-a^3(-l_4+1)-a^2(-l_3+1)+al_2=a,$$

которое выполняется тогда и только тогда, когда $l_5=l_4=l_3=l_2=1$.

Если же хотя бы при одном $j=2,3,4,5$ выполнено $|u_j|>a-1$, откуда $|u_j|\geq a$, то из (3.9) выводим

$$g_6(0,u_2,u_3,u_4,u_5,u_6)\geq a.$$

Таким образом, при $a\geq1,u_6\neq0$ ивсех (u_2,u_3,u_4,u_5) выполнено неравенство

$$a\geq1,g_6(0,u_2,u_3,u_4,u_5,u_6)\geq a\left(u_6\neq0,(u_2,u_3,u_4,u_5)\in Z^4\right). \tag{3.10}$$

Следующий случай заключается в том, что если $u_6=0$ и u_5,u_4,u_3,u_2 ? произвольные целые числа не равные нулю одновременно, то требуется оценить снизу нижнюю грань функции

$$g_6^2(0,u_2,u_3,u_4,u_5,0)=\left(a^4u_5+a^3u_4+a^2u_3+au_2\right)^2+u_2^2+u_3^2+u_4^2+u_5^2.$$

Пусть u_k есть не равное нулю первое из чисел u_5, u_4, u_3, u_2 (в силу условия $|u_5|+|u_4|+|u_3|+|u_2| \geq 1$ такое $k, 5 \geq k \geq 2$ существует).

Тогда

$$g_6^2(0, u_2, u_3, u_4, u_5, 0) = g_6^2(0, u_2, ..., u_k, 0, ..., 0) = \left(a^{k-1}u_k + \cdots + au_2\right)^2 + u_k^2 + \cdots + u_2^2. \quad (3.11)$$

Если $|u_{k-1}| \leq a-1, ..., |u_2| \leq a-1$, то $(u_k \neq 0)$

$$g_6(0, u_2, ..., u_k, 0, ..., 0) \geq a^{k-1}|u_k| - a^{k-2}|u_{k-1}| - \cdots - a^2|u_3| - a|u_2| \geq$$

$$\geq a^{k-1} - a^{k-2}(a-1) - \cdots - a^2(a-1) - a(a-1) = a^{k-1} - a^{k-1} + a^{k-2} - \cdots - a^3 + a^2 - a^2 + a = a.$$

Если же хотя бы одно из чисел $|u_{k-1}|, ..., |u_2|$ больше $a-1$, стало быть, больше или равно a, то из (3.11) следует, что

$$g_6(0, u_2, ..., u_k, 0, ..., 0) \geq \sqrt{u_{k-1}^2 + \cdots + u_2^2} \geq a.$$

Поэтому, в случае $u_6 = 0$ при произвольных одновременно не равных нулю $u_2, ..., u_5$ имеет место неравенство

$$a \geq 1, g_6(0, u_2, ..., u_5, 0, ..., 0) \geq a\left(u_6 = 0, (u_2, ..., u_5) \in Z_0^4\right).$$

Отсюда и из (3.10) следует, что при $a \geq 1$ и всех $u_2, ..., u_6$ $(|u_2| + \cdots + |u_6| \geq 1)$

$$a \geq 1, g_6(0, u_2, ..., u_6) \geq a.\left(u_1 = 0, (u_2, ..., u_6) \in Z_0^5\right).$$

Это же соотношение вместе с (3.8) приводит к утверждению: при $a \geq 21$ и всех $(u_1, ..., u_6) \in Z_0^6$

$$g_6(u_1, u_2, u_3, u_4, u_5, u_6) \geq a - 20 = (a-1) - 19 = N^{\frac{1}{6}} - 19 = N^{\frac{1}{6}}\left(1 - 19N^{-\frac{1}{6}}\right).$$

Заметим, что при доказательстве случая $u_1 = 0$ попутно установлено, что если $k \geq 2$, то при всех $(u_k, ..., u_2) \in Z_0^{k-1}$ выполнено неравенство

$$\left(a^{k-1}u_k + \cdots + a^2u_3 + au_2\right)^2 + u_2^2 + \cdots + u_k^2 \geq a^2. \quad (1)$$

Тем самым, при $s = 3$ (см. (3.2)))

$$N^{\frac{1}{3}}\left(1 - 2N^{-\frac{1}{3}}\right) = (a-1) - 2 = a - 3 \leq \nu_3\left(a, N; N = (a-1)^3\right) \leq N^{\frac{1}{3}}\sqrt{1 + 2N^{-\frac{1}{3}} + 2N^{-\frac{2}{3}}}$$

и при $s = 6$

$$N^{\frac{1}{6}}\left(1 - 19N^{-\frac{1}{6}}\right) = (a-1) - 19 = a - 20 \leq \nu_6\left(a, N; N = (a-1)^6\right) \leq N^{\frac{1}{6}}\sqrt{1 + 2N^{-\frac{1}{6}} + 2N^{-\frac{2}{6}}}.$$

Как это видно из доказанных случаев, в оценках снизу коэффициенты (-2) и (-19) при $N^{-\frac{1}{s}}$ есть наибольшие по модулю с отрицательным знаком коэффициенты в разложениях

$$(a-1)^3 = 1 - 3a^2 + 3a - 1 \; u \; (a-1)^6 = 1 - 6a + 15a^2 - 20a^3 + 15a^2 - 6a + 1$$

соответственно, к которым прибавлен $+1$.

Всё это имеет место в случае произвольных $s \geq 3$:

$$\nu_s(a, N; N = (a-1)^s) \geq a - b_s,$$

где b_s означает абсолютную величину наибольшего по модулю отрицательного коэффициента при степени a в разложении $(a-1)^s$ по степеням a.

Действительно, в общем случае s переменных повторяя рассуждения при $s = 3$ и $s = 6$ получаем, что из всех неравенств вида $|u_j| \geq a - l_j + 1$, наименьшая оценка снизу достигается при $a - l_j + 1 = a - b_s$, т. е. при $l_j = b_s + 1$, поэтому при условии $a \geq b_s + 1$ для всех не равных одновременно нулю $u_1, ..., u_s$ будет выполняться неравенство

$$g_s(u_1, ..., u_s; a, N = (a-1)^s) \geq a - b_s \geq 1\left((u_1, ..., u_s) \in Z_0^s\right), \quad (3.13)$$

откуда, в силу определения v_s^2 и леммы 1 при $l = b_s$, приходим к неравенству

$$\nu_s(a, N; (a-1)^s = N) \geq a - b_s = (a-1) - (b_s - 1) = N^{\frac{1}{s}} - (b_s - 1) = N^{\frac{1}{s}}\left(1 - (b_s - 1)N^{-\frac{1}{s}}\right).$$

Теорема 2 полностью доказана.

Из доказательства Теоремы 2 выделим следующие леммы, имеющие самостоятельное значение.

Лемма 2. *(см. (3.13)). При заданных* $s \geq 2$ *и* $a \geq b_s + 1$ *для всякого* $(\vartheta_1, \ldots, \vartheta_s)$ *из* Z_0^s *имеет место неравенство*

$$\left((a-1)^s \vartheta_1 - a\vartheta_2 - \ldots - a^{s-1}\vartheta_s\right)^2 + \vartheta_2^2 + \vartheta_3^2 + \ldots + \vartheta_s^2 \geq (a - b_s)^2 .$$

Лемма 3. *При фиксированных* $(a-1)^\tau = N\lambda$ *для* $\nu_s \equiv \nu_s(a, N; (a-1)^\tau = N\lambda)$ *имеет место следующая цепочка неравенств*

$$\nu_2(a, N) \geq \nu_3(a, N) \geq \cdots \geq \nu_s(a, N) \geq \nu_{s+1}(a, N) \geq \cdots .$$

Доказательство следует из возможности «наращивания» количества переменных от s до τ, $2 \leq s < \tau$:

$$\nu_s^2(a, N; (a-1)^\tau = N\lambda) = \inf_{(u_1,\ldots,u_s)\in Z_0^s} \left(Nu_1 - a\cdot u_2 - \cdots - a^{s-1}u_s\right)^2 + u_2^2 + \cdots + u_s^2 =$$

$$= \inf_{(u_1,\ldots,u_\tau)=(u_1,\ldots,u_s,0,\ldots,0)\in Z_0^\tau} \left(Nu_1 - a\cdot u_2 - \cdots - a^{s-1}u_s - a^s u_{s+1} - \cdots - a^{\tau-1}u_\tau\right) + u_2^2 + \cdots + u_\tau^2 \geq$$

$$\geq \inf_{(u_1,\ldots,u_\tau)\in Z_0^\tau} \left(Nu_1 - a\cdot u_2 - \cdots - a^{\tau-1}u_\tau\right)^2 + u_2^2 + \cdots + u_\tau^2 = \nu_\tau^2(a, N; (a-1)^\tau = N\lambda) .$$

Отсюда, $\nu_2^2(a, N; (a-1)^\tau = N\lambda) \geq \nu_3(a, N; (a-1)^\tau = N\lambda) \geq \cdots$.

Лемма 3 доказана.

Лемма 4. *Если* $\lambda | (a-1)$, *то для* $l_{k+1} = (-1)^{(s-1)-k}\binom{s-1}{k}$ $(k = 1, ..., s-1)$ *выполнено равенство*

$$g_s^2(1, \frac{a-1}{\lambda}l_2, ..., \frac{a-l}{\lambda}l_s) = \left(\frac{a-1}{\lambda}\right)^2 \sum_{k=0}^{s-1} \left(\binom{s-1}{k}\right)^2 .$$

Замечание. Применяемая техника:

1. Значения функции $g_s(u_1, ..., u_s)$ вычисляются в точках $\bar{u}_j = \frac{a-1}{\lambda}l_j$ $(j = 2, ..., s)$.
2. Оценка снизу $g_s(u_1, ..., u_s)$ производится при $|u_j| \leq a - l_j$, где l_j любого знака.

Доказательство. При $s = 3$ функция g_3 есть

$$g_3^2(u_1, u_2, u_3) = \left(Nu_1 - au_2 - a^2u_3\right)^2 + u_2^2 + u_3^2.$$

При $N = \frac{(a-1)^3}{\lambda}$, $u_1' = 1$, $u_2' = \frac{a-1}{\lambda}l_2$, $u_3' = \frac{a-1}{\lambda}l_3$ имеем

$$\frac{(a-1)^3}{\lambda} - a\frac{a-1}{\lambda}l_2 - a^2\frac{a-1}{\lambda}l_3 = \frac{(a-1)}{\lambda}\left((a-1)^2 - al_2 - a^2l_3\right) =$$

$$= \frac{(a-1)}{\lambda}\left(a^2 - 2a + 1 - al_2 - a^2l_3\right) = \frac{(a-1)}{\lambda}\left(a^2(1-l_3) + a(-2-l_2) + 1\right) = \frac{a-1}{\lambda}$$

при $l_2 = -2$, $l_3 = 1$.

Отсюда, полагая $\overline{u_1} = 1, \overline{u_2} = -2\frac{a-1}{\lambda}, \overline{u_3} = \frac{a-1}{\lambda}$, получаем

$$g_3^2(\bar{u}) = \left(\frac{a-1}{\lambda}\right)^2 + 4\left(\frac{a-1}{\lambda}\right)^2 + \left(\frac{a-1}{\lambda}\right)^2 = \left(\frac{a-1}{\lambda}\right)^2 (1^2 + 2^2 + 1^2) =$$

$$= \left(\frac{a-1}{\lambda}\right)^2 6 = \left(\frac{a-1}{\lambda}\right)^2 \left(\binom{2}{0}^2 + \binom{2}{1}^2 + \binom{2}{2}^2\right).$$

Таким образом, лемма при $s = 3$ доказана.

Пусть теперь $s = 6$. Опять же, для

$$u_1' = 1,\ u_2' = \frac{a-1}{\lambda}l_2,\ u_3' = \frac{a-1}{\lambda}l_3,\ u_4' = \frac{a-1}{\lambda}l_4,\ u_5' = \frac{a-1}{\lambda}l_5,\ u_6' = \frac{a-1}{\lambda}l_6$$

будем иметь

$$\frac{(a-1)^6}{\lambda} - a\frac{a-1}{\lambda}l_2 - a^2\frac{a-1}{\lambda}l_3 - ... - a^5\frac{a-1}{\lambda}l_6 =$$

$$= \frac{a-1}{\lambda}\left((a-1)^5 - al_2 - a^2l_3 - \cdots - a^5l_6\right).$$

Далее,

$$\begin{array}{ccccccccccc}
 & & & & & 1 & & & & & \\
 & & & & 1 & & 1 & & & & \\
 & & & 1 & & 2 & & 1 & & & \\
 & & 1 & & 3 & & 3 & & 1 & & \\
 & 1 & & 4 & & 6 & & 4 & & 1 & \\
1 & & 5 & & 10 & & 10 & & 5 & & 1 \\
+ & & - & & + & & - & & + & & - \\
\binom{5}{0} & & \binom{5}{1} & & \binom{5}{2} & & \binom{5}{3} & & \binom{5}{4} & & \binom{5}{5}
\end{array}$$

$$(a-1)^5 - al_2 - a^2l_3 - \cdots - a^5l_6 = a^5 - 5a^4 + 10a^3 - 10a^2 + 5a - 1 - al_2 -$$
$$-a^2l_3 - a^3l_4 - a^4l_5 - a^5l_6 = a^5(1-l_6) + a^4(-5-l_5) + a^3(10-l_4) +$$
$$+a^2(-10-l_3) + a(5-l_2) - 1 = -1$$

при $l_2 = 5,\ l_3 = -10,\ l_4 = 10,\ l_5 = -5,\ l_6 = 1$, т. е. при $l_{k+1} = (-1)^{5-k}\binom{5}{k}\ (k = 1, ..., 5)$.

Отсюда, полагая

$$\bar{u}_1 = 1,\ \bar{u}_2 = 5\frac{a-1}{\lambda},\ \bar{u}_3 = -10\frac{a-1}{\lambda},\ \bar{u}_4 = 10\frac{a-1}{\lambda},\ \bar{u}_5 = -5\frac{a-1}{\lambda},\ \bar{u}_6 = 1$$

будем иметь

$$g_6^2(\bar{u}) = \left(\frac{a-1}{\lambda}\right)^2\left(1 + 5^2 + (-10)^2 + 10^2 + (-5)^2 + 1\right) = \left(\frac{a-1}{\lambda}\right)^2(2 + 50 + 200) =$$

$$= \left(\frac{a-1}{\lambda}\right)^2 252 = \left(\frac{a-1}{\lambda}\right)^2 \sum_{k=0}^{5}\binom{5}{k}^2,$$

поскольку $\binom{5}{0} = 1$.

Итак, утверждение леммы доказано при $s = 3$ и $s = 6$. Общий случай проводится по той же схеме.

Именно,

$$\left(\frac{(a-1)^s}{\lambda} - \frac{a(a-1)}{\lambda}l_2 - \cdots - \frac{a^s(a-1)}{\lambda}l_s\right) = \left(\frac{a-1}{\lambda}\right)\left((a-1)^{s-1} - al_2 - \cdots - a^{s-1}l_s\right) =$$

$$= \left(\frac{a-1}{\lambda}\right)\left(\sum_{k=0}^{s-1}(-1)^{(s-1)-k}\binom{s-1}{k}a^k - \sum_{k=1}^{s-1}a^k l_{k+1}\right) = \left(\frac{a-1}{\lambda}\right) \times$$

$$\times\left((-1)^{s-1} + \sum_{k=1}^{s-1}a^k\left((-1)^{(s-1)-k}\binom{s-1}{k} - l_{k+1}\right)\right) = \left(\frac{a-1}{\lambda}\right)(-1)^{s-1},$$

где $l_{k+1} = (-1)^{(s-1)-k}\binom{s-1}{k}\ (k = 1, ..., s-1)$. Отсюда, при

$$\bar{u}_1 = 1, \bar{u}_{k+1} = \left(\frac{a-1}{\lambda}\right)l_{k+1} = \left(\frac{a-1}{\lambda}\right)(-1)^{(s-1)-k}\binom{s-1}{k}\ (k = 1, ..., s-1),$$

получаем

$$g^2(\bar{u}_1, ..., \bar{u}_s) = \left(\frac{a-1}{\lambda}\right)^2\left[\left((-1)^{s-1}\right)^2 + \sum_{k=1}^{s-1}\left(\binom{s-1}{k}\right)^2\right] = \left(\frac{a-1}{\lambda}\right)^2\sum_{k=0}^{s-1}\left(\binom{s-1}{k}\right)^2,$$

что доказывает лемму в общем случае.

Лемма 5. *Если* $k \geq 2$ *и* $(u_2, ..., u_k) \in Z_0^{k-1}$, *то*

$$(a^{k-1}u_k + \cdots + au_2)^2 + u_2^2 + \cdots + u_k^2 \geq a^2.$$

Доказательство было дано при доказательстве Теоремы 2 (см. (1)).

Лемма 6. *Если* $a \geq b_s + 1, u_1 \neq 0$ *и* $|u_j| \leq a - l_j$ *для всех* $j, j = 2, ..., s$, *то*

$$(a-1)^s |u_1| - a|u_2| - \cdots - a^{s-1}|u_s| \geq a + (-1)^s \geq a - 1 \, (a \geq 2),$$

где $l_2 = 1 + (-1)^s s$ *и* $l_{j+1} = (-1)^{s-j-1} \binom{s}{j} + 1$ *при* $j = 2, ..., s-1$.

Доказательство. Временно полагая $a \geq l_j, |u_j| \leq a - l_j \, (j = 2, ..., s)$, будем иметь:

$$(a-1)^s |u_1| - a|u_2| - \cdots - a^{s-1}|u_s| \geq (a-1)^s - \sum_{j=2}^{s} a^{j-1}(a - l_j) = \sum_{j=0}^{s} (-1)^{s-j} \binom{s}{j} a^j - \sum_{j=2}^{s} a^j + \sum_{j=1}^{s-1} a^j l_{j+1} =$$

$$= \left(a^s + \sum_{j=2}^{s-1} (-1)^{s-j} \binom{s}{j} a^j + (-1)^{s-1} \binom{s}{1} a + (-1)^s \right) - \left(a^s + \sum_{j=2}^{s-1} a^j \right) + \sum_{j=2}^{s-1} a^j l_{j+1} + a l_2 =$$

$$= \sum_{j=2}^{s-1} a^j \left((-1)^{s-j} \binom{s}{j} - 1 + l_{j+1} \right) + \left((-1)^{s-1} \binom{s}{1} + l_2 \right) a + (-1)^s = a + (-1)^s ,$$

если только для всех $j = 2, ..., s-1$

$$l_{j+1} = (-1)^{s-j-1} \binom{s}{j} + 1$$

и

$$(-1)^{s-1} \binom{s}{1} + l_2 = 1 \Leftrightarrow l_2 = 1 - (-1)^{s-1} \binom{s}{1} = 1 + (-1)^1 \cdot (-1)^{s-1} \binom{s}{1} = 1 + (-1)^s s.$$

Лемма 6 доказана.

Теорема 3 ($s = \tau = 2, \lambda \geq 2$). *Пусть параметры* a *и* N *связаны равенством* $(a-1)^2 = N\lambda$, *где целое* $\lambda \geq 2$. *Тогда*

$$\sqrt{\frac{N}{\lambda}} \times \sqrt{1 - 2\frac{\sqrt{N\lambda} - 1}{N\lambda}} = \frac{\sqrt{1 + (a-2)^2}}{\lambda} \leq \nu_2 \left(a, N; (a-1)^2 = N\lambda, \lambda \geq 2 \right) \overset{\lambda | (a-1)}{\leq}$$

$$\overset{\lambda | (a-1)}{\leq} \frac{\sqrt{2}}{\lambda} (a-1) = \sqrt{\frac{2}{\lambda}} \cdot \sqrt{N},$$

где в оценке сверху требуется условие $\lambda | (a-1) \Leftrightarrow (a-1) | N$.

Доказательство теоремы 3. Оценка сверху. По условию $\overline{u}_2 = \frac{a-1}{\lambda}$ есть число целое. Поэтому $(\overline{u}_1 = 1)$

$$g_2^2 (\overline{u}_1, \overline{u}_2) = (N\overline{u}_1 - a\overline{u}_2)^2 + \overline{u}_2^2 = \left(\frac{(a-1)^2}{\lambda} - \frac{a(a-1)}{\lambda} \right)^2 + \left(\frac{a-1}{\lambda} \right)^2 =$$

$$= \left(\frac{a-1}{\lambda} \right)^2 (a - 1 - a)^2 + \left(\frac{a-1}{\lambda} \right)^2 = 2 \left(\frac{a-1}{\lambda} \right)^2 .$$

Стало быть,

$$\nu_2 \left(a, N; (a-1)^2 = N\lambda, \lambda \geq 2 \right) \leq g_2 (\bar{u}_1, \bar{u}_2) = \sqrt{2} \left(\frac{a-1}{\lambda} \right) = \sqrt{2} \frac{(N\lambda)^{\frac{1}{2}}}{\lambda} = \sqrt{\frac{2}{\lambda}} \cdot \sqrt{N}.$$

С другой стороны, применяя Теорему 1 при $N = (a-1)^2$, для всякого ненулевого вектора (u_1, u_2) из Z^2 будем иметь

$$g^2 (u_1, u_2) = (Nu_1 - au_2)^2 + u_2^2 = \left(\frac{(a-1)^2}{\lambda} u_1 - au_2 \right)^2 + u_2^2 = \left(\frac{1}{\lambda^2} \right) \left[\left((a-1)^2 u_1 - a\lambda u_2 \right)^2 + \right.$$

$$\left. + (\lambda u_2)^2 \right] \geq \frac{1}{\lambda^2} \inf_{(\vartheta, \vartheta_2) \in Z_0^2} \left[\left((a-1)^2 \vartheta_1 - a\vartheta_2 \right)^2 + \vartheta_2^2 \right] \overset{-1}{=} \frac{1 + (a-2)^2}{\lambda^2},$$

откуда в силу определения ν_2^2 и Леммы 1

$$\nu_2\left(a,N;(a-1)^2=N\lambda,\lambda\geq 2\right)\geq\frac{(a-2)^2+1}{\lambda^2}=\frac{(a-1)^2-2(a-1)+2}{\lambda^2}=\frac{(a-1)^2}{\lambda^2}\left(1-2\frac{(a-1)-1}{(a-1)^2}\right)=$$

$$=\frac{N\lambda}{\lambda^2}\left(1-2\frac{\sqrt{N\lambda}-1}{N\lambda}\right)=\frac{N}{\lambda}\cdot\left(1-2\frac{\sqrt{N\lambda}-1}{N\lambda}\right).$$

Теорема 3 доказана.

Теорема 4 ($\tau>s=2,(a-1)^\tau=N$). *Пусть даны числа* $\tau>s=2$, $a\geq b_\tau+1$ *и* $N>a$ *такие, что* $N=(a-1)^\tau$. *Тогда*

$$N^{\frac{1}{\tau}}\left(1-(b_\tau-1)N^{-\frac{1}{\tau}}\right)=a-b_\tau\leq\nu_2(a,N;(a-1)^\tau=N)\leq\sqrt{1+a^2}=N^{\frac{1}{\tau}}\sqrt{1+2N^{-\frac{1}{\tau}}+2N^{-\frac{2}{\tau}}},$$

$$\pi N^{\frac{2}{\tau}-1}\left(1-(b_\tau-1)N^{-\frac{1}{\tau}}\right)^2=\pi\frac{(a-b_\tau)^2}{(a-1)^\tau}\leq\mu_2(a,N;(a-1)^\tau=N)\leq$$

$$\leq\pi\frac{\left(1+a^2\right)}{(a-1)^\tau}=\pi N^{\frac{2}{\tau}-1}\left(1+2N^{-\frac{1}{\tau}}+2N^{-\frac{2}{\tau}}\right).$$

Доказательство теоремы 4. В силу леммы 3 и Теоремы 2 имеем

$$\nu_2(a,N;(a-1)^\tau=N)\geq\nu_\tau(a,N;(a-1)^\tau=N)\geq a-b_\tau=(a-1)-(b_\tau-1)=N^{\frac{1}{\tau}}-(b_\tau-1)=$$

$$=N^{\frac{1}{\tau}}\left(1-(b_\tau-1)N^{-\frac{1}{\tau}}\right).$$

С другой стороны, в силу леммы 1 имеем

$$g_2^2(0,1)=1+a^2=N^{\frac{2}{\tau}}\left(1+2N^{-\frac{1}{\tau}}+2N^{-\frac{2}{\tau}}\right)\geq\nu_2^2(a,N;(a-1)^\tau=N).$$

Теорема 4 доказана.

Теорема 5 ($\tau=s\geq 2$, $(a-1)^s=N\lambda$, $\lambda\geq 1$). *Пусть числа* $a\geq b_s+1, N>a, s\geq 2$ *и* $\lambda\geq 2$ *таковы, что* $(a-1)^s=N\lambda$. *Тогда*

$$\frac{N^{\frac{1}{s}}}{\lambda^{1-\frac{1}{s}}}\sqrt{\sum_{k=0}^{s-1}\left(\binom{s-1}{k}\right)^2}=\frac{a-1}{\lambda}\sqrt{\sum_{k=0}^{s-1}\left(\binom{s-1}{k}\right)^2}\overset{\lambda|(a-1)}{\geq}\nu_s(a,N;(a-1)^s=N\lambda)\geq$$

$$\geq\frac{a-b_s}{\lambda}=\frac{N^{\frac{1}{s}}}{\lambda^{1-\frac{1}{s}}}\left(1-(b_s-1)(N\lambda)^{-\frac{1}{s}}\right),$$

где в оценке сверху предполагается выполнение условия $\lambda|(a-1)\Leftrightarrow(a-1)^{\tau-1}|N$.

Доказательство теоремы 5. Доказательство оценки снизу: для всех $(u_1,...,u_s)\in Z_0^s$ в силу Леммы 2 и условия $(a-1)^s=N$ имеем

$$g_s^2(u_1,...,u_s)\overset{(a-1)^s=N\lambda}{=}\left(\frac{(a-1)^s}{\lambda}u_1-au_2-\cdots-a^{s-1}u_s\right)^2+u_2^2+\cdots+u_s^2=$$

$$=\frac{1}{\lambda^2}\left[((a-1)^su_1-a(\lambda u_2)-\cdots-a^{s-1}(\lambda u_s))^2+(\lambda u_2)^2+\cdots+(\lambda u_s)^2\right]\geq$$

$$\geq\frac{1}{\lambda^2}\inf_{(\vartheta_1,...,\vartheta_s)\in Z_0^s}\left[\left((a-1)^s\vartheta_1-a\vartheta_2-\cdots-a^{s-1}\vartheta_s^2\right)^2+\vartheta_2^2+\cdots+\vartheta_s^2\right]\overset{\text{Лемма 2}}{\geq}\frac{1}{\lambda^2}(a-b_s)^2.$$

Отсюда в силу определения ν_s и равенства $(a-1)^s=N\lambda$ имеем

$$\nu_s(a,N;(a-1)^s=N\lambda)\geq\frac{a-b_s}{\lambda}=\frac{(a-1)-(b_s-1)}{\lambda}=\frac{(N\lambda)^{\frac{1}{s}}-(b_s-1)}{\lambda}=$$

$$=\frac{(N\lambda)^{\frac{1}{s}}}{\lambda}\left(1-(b_s-1)(N\lambda)^{-\frac{1}{s}}\right),$$

т. е. оценка снизу доказана.

Оценка сверху следует из Леммы 4 в условиях $(a-1)^s = N\lambda, \lambda \mid (a-1)$

$$\frac{a-1}{\lambda}\sqrt{\sum_{k=0}^{s-1}\left(\binom{s-1}{k}\right)^2} = g_s\left(1, \frac{a-1}{\lambda}l_2, ..., \frac{a-1}{\lambda}l_s\right) \geq \nu_s(a, N; (a-1)^s = N\lambda),$$

где

$$\frac{a-1}{\lambda} = \frac{(N\lambda)^{\frac{1}{s}}}{\lambda} = \frac{N^{\frac{1}{s}}}{\lambda^{1-\frac{1}{s}}}.$$

Теорема 5 доказана.

Теорема 6 ($2 \leq s < \tau, (a-1)^\tau = N\lambda, 1 \leq \lambda \leq (a-1)^{\tau-s}$). *Если* a, N, s, τ *и* λ *связаны равенством* $(a-1)^\tau = N\lambda$ *и неравенствами* $a \geq b_s + 1, 2 \leq s < \tau, 1 \leq \lambda \leq (a-1)^{\tau-s}$, *то*

$$(N\lambda)^{\frac{1}{\tau}}\left(1 - (b_s - 1)(N\lambda)^{-\frac{1}{\tau}}\right) = a - b_s \leq \nu_s(a, N; (a-1)^\tau = N\lambda) \leq \sqrt{1+a^2} =$$

$$= (N\lambda)^{\frac{1}{\tau}}\sqrt{1 + 2(N\lambda)^{-\frac{1}{\tau}} + 2(N\lambda)^{-\frac{2}{\tau}}},$$

$$\frac{\pi^{\frac{s}{2}}}{\left(\frac{s}{2}\right)!}\frac{\left((N\lambda)^{\frac{1}{\tau}}\left(1 - (b_s-1)(N\lambda)^{-\frac{1}{\tau}}\right)\right)^s}{N} = \frac{\pi^{\frac{s}{2}}}{\left(\frac{s}{2}\right)!}\frac{(a-b_s)^s \times \lambda}{(a-1)^\tau} \leq \mu_s(a, N; (a-1)^\tau = N\lambda) \leq$$

$$\leq \frac{\pi^{\frac{s}{2}}}{\left(\frac{s}{2}\right)!}\frac{\left(1+a^2\right)^{\frac{s}{2}} \times \lambda}{(a-1)^\tau} = \frac{\pi^{\frac{s}{2}}}{\left(\frac{s}{2}\right)!}\frac{\left((N\lambda)^{\frac{1}{\tau}}\sqrt{1 + 2(N\lambda)^{-\frac{1}{\tau}} + 2(N\lambda)^{-\frac{2}{\tau}}}\right)^s}{N}.$$

Доказательство теоремы 6. Пусть сначала $u_1 \neq 0$. Тогда для всех $(u_1, ..., u_s)$ имеем

$$\begin{aligned} g_s^2(u_1, ..., u_s) &= \left(\frac{(a-1)^\tau}{\lambda}u_1 - au_2 - \cdots - a^{s-1}u_s\right)^2 + u_2^2 + \cdots + u_s^2 = \\ &= \left(\frac{(a-1)^\tau}{\lambda}|u_1| - au_2\, sgn\, u_1 - \cdots - a^{s-1}u_s\, sgn\, u_1\right)^2 + \left|u_2^2\right| + \cdots + \left|u_s^2\right|. \end{aligned} \tag{3.14}$$

Возможны два случая

а) $u_1 \neq 0$ и $|u_j| \leq a + (-1)^{s-j}\binom{s}{j}$ $(j = 2, ..., s)$

и

в) $|u_{j_0}| > a + (-1)^{s-j_0}\binom{s}{j_0}$ для некоторого j_0 из чисел $2, ..., s$.

В случае а) из условия $\frac{(a-1)^{\tau-s}}{\lambda} \geq 1$, равенства (3.14) и Леммы 6 имеем

$$\begin{aligned} &\frac{(a-1)^\tau}{\lambda}|u_1| - au_2\, sgn\, u_1 - \cdots - a^{s-1}u_s\, sgn\, u_1 \geq \\ &\frac{(a-1)^{\tau-s}}{\lambda}(a-1)^s|u_1| - a|u_2| - \cdots - a^{s-1}|u_s| \geq \\ &\geq (a-1)^s|u_1| - a|u_2| - \cdots - a^{s-1}|u_s| \overset{\text{Лемма 6}}{\geq} a - 1. \end{aligned} \tag{3.15}$$

В случае в) из определения g_s следует (даже без условия $u_1 \neq 0$)

$$g_s(u_1, ..., u_s) \geq |u_{j_0}| \geq a - (-1)^{s-j_0}\binom{s}{j_0} + 1 \geq a - b_s. \tag{3.16}$$

В случае $u_1 = 0$ для всех $(u_2, ..., u_s) \in Z_0^{s-1}$ по Лемме 8 получаем

$$g_s(0, u_2, ..., u_s) \geq a. \tag{3.17}$$

Из (3.15)–(3.17) следует что для всех $(u_1, ..., u_s) \in Z_0^s$ выполнено

$$g_s(u_1, ..., u_s; a, (a-1)^\tau = N\lambda) \geq a - b_s.$$

Отсюда, и из Леммы 1 при $N\lambda = (a-1)^\tau$ получаем

$$\nu_s\left(a, N; (a-1)^\tau = N\lambda, 1 \leq \lambda \leq (a-1)^{\tau-s}\right) \geq a - b_s = (N\lambda)^{\frac{1}{\tau}}\left(1 - (b_s-1)(N\lambda)^{-\frac{1}{\tau}}\right).$$

Оценка сверху следует из равенств $N\lambda = (a-1)^\tau$, $g_s(0,1,0,...,0;a,N) = \sqrt{1+a^2}$ и Леммы 1. Теорема 6 доказана.

Теорема 7 ($2 \le \tau < s$, $(a-1)^\tau = N\lambda$, $\lambda \ge 1$). *Пусть даны числа* $a, N > a, s, \tau$ *и* λ *такие, что* $(a-1)^\tau = N\lambda$, $2 \le \tau < s, \lambda \ge 1$. *Тогда*

$$\nu_s(a,N;(a-1)^\tau = N\lambda) \le \sqrt{\sum_{k=0}^{\tau}\left(\binom{\tau}{k}\right)^2}.$$

Доказательство теоремы 7. Идею доказательства поясним на примере $\tau = 2$ и $s = 3$. При $\overline{u}_1 = \lambda, \overline{u}_2 = -2, \overline{u}_3 = 1$ имеет место равенство

$$\frac{(a-1)^2}{\lambda}\overline{u_1} - a\overline{u_2} - a^2\overline{u_3} = (a-1)^2 + 2a - a^2 = 1,$$

и потому

$$g_3^2(\overline{u_1},\overline{u_2},\overline{u_3}) = \left(\frac{(a-1)^2}{\lambda}\overline{u_1} - a\overline{u_2} - a^2\overline{u_3}\right)^2 + \overline{u}_2^2 + \overline{u}_3^2 = 1+4+1 = 6,$$

стало быть, $\nu_3(a,N;(a-1)^2 = N\lambda) \le \sqrt{6}$.

В общем случае, пользуясь условием $\tau < s$, полагаем $\overline{u}_1 = \lambda$, а $\overline{u}_2, ..., \overline{u}_{\tau+1}$ выбираем из условия

$$\sum_{k=1}^{\tau}(-1)^{\tau-k}\binom{\tau}{k}a^k = a^\tau\bar{u}_{\tau+1} + a^{\tau-1}\bar{u}_\tau + \cdots + a\bar{u}_2 = \sum_{k=1}^{\tau}\bar{u}_{k+1}a^k,$$

т. е. равными

$$\bar{u}_{k+1} = (-1)^{\tau-k}\binom{\tau}{k} \ (k = 1, ..., \tau),$$

оставшиеся же $\bar{u}_j$ из $\bar{u}_1, ..., \bar{u}_s$ приравниваем к нулю. Тогда

$$g_s^2(\bar{u}_1,...,\bar{u}_s) = \left(\sum_{k=0}^{\tau}(-1)^{\tau-k}\binom{\tau}{k}a^k - \sum_{k=1}^{\tau}a^k\bar{u}_{k+1}\right)^2 + \sum_{k=1}^{\tau}\left((-1)^{\tau-k}\binom{\tau}{k}\right)^2 =$$

$$= \left((-1)^\tau\binom{\tau}{0}\right)^2 + \sum_{k=1}^{\tau}\left(\binom{\tau}{k}\right)^2 = \sum_{k=0}^{\tau}\left(\binom{\tau}{k}\right)^2 \ge \nu_s^2(a,N;(a-1)^\tau = N\lambda).$$

Заметим, что в условиях $(a-1)^\tau = N\lambda$ величина λ меняется в пределах $1 \le \lambda < (a-1)^{\tau-1}$ поскольку $N > a > a-1$, стало быть, $(a-1)^\tau = N\lambda > (a-1)\cdot\lambda$.

В этих условиях справедлива

Лемма 7. *Пусть даны числа* $a, N, a < N$, $2 \le s < \tau$ *и* $(a-1)^\tau = N\lambda$. *Тогда для* $\lambda_t = (a-1)^t$ $(\tau - s + 1 \le t \le \tau - 2)$ *выполнено*

$$\nu_s(a,N;(a-1)^\tau = N\lambda_t) \le \sqrt{\sum_{k=0}^{\tau-t}\left(\binom{\tau-t}{k}\right)^2} \le \sqrt{\sum_{k=0}^{s-1}\left(\binom{s-1}{k}\right)^2}.$$

Доказательство. Для $\lambda_t = (a-1)^t$ $(\tau - s + 1 \le t \le \tau - 2)$ имеем

$$N = \frac{(a-1)^\tau}{\lambda_t} = (a-1)^{\tau-t},$$

где $-\tau + s - 1 \ge -t \ge -\tau + 2 \Leftrightarrow s - 1 \ge \tau - t \ge 2$.

В этих условиях применение теоремы 7 приводит к неравенствам

$$\nu_s(a,N;(a-1)^\tau = N\lambda_t) = \nu_s\left(a,N;(a-1)^{\tau-t} = N\right) \le \sqrt{\sum_{k=0}^{\tau-t}\left(\binom{\tau-t}{k}\right)^2},$$

из которых следует утверждение леммы.

Тем самым, Теорема 6 доказана полностью.

Лемма 8. *Для любых целых чисел* N *и* $a, N > a > 2$ *в условиях теоремы A существует, причем единственное* $\tau = \tau(a, N)$ *такое, что*

$$(a-1)^{\tau} \equiv 0 \,(\mathrm{mod} N) \text{ и } (a-1)^{\tau-1} \not\equiv 0 \,(\mathrm{mod} N) \tag{3.18}$$

Доказательство. Сразу же покажем, что из условия $N > a \geq 2$ следует $\tau \geq 2$, ибо $1 \leq a-1 < N$ и потому $(a-1)$ делить N не может, стало быть, случай $\tau = 1, (a-1)^{\tau} \equiv 0 \,(\mathrm{mod} N)$ невозможен.

Сначала убедимся в том, что величина $\tau = \tau(a, N)$ со свойствами (3.18) единственна.

Пусть имеется еще $\tau_1 \neq \tau$ с теми же свойствами:

$$N \mid (a-1)^{\tau_1} \text{ и } N \nmid (a-1)^{\tau_1 - 1}. \tag{3.19}$$

Тогда $\tau_1 > \tau$ или же $\tau_1 < \tau$.

Если $\tau_1 > \tau$, то $\tau_1 - 1 \geq \tau$ и потому из $N \mid (a-1)^{\tau}$ следует $N \mid (a-1)^{\tau_1 - 1}$, что противоречит второму условию из (3.19).

Если $\tau_1 < \tau$, то $\tau_1 \leq \tau - 1$ и потому из $N \nmid (a-1)^{\tau-1}$ следует $N \nmid (a-1)^{\tau_1}$, что противоречит первому условию из (3.19).

Тем самым, потенциал $\tau(a, N)$ из (3.18) единственен.

Итак, если $\tau \geq 2$ со свойством (3.18) существует, то такое τ единственное.

Теперь докажем что, τ со свойствами из (3.18) существует.

Доказательство леммы основано на том, что степень p^{α} делит степень p^{β} тогда и только тогда, когда $\beta \geq \alpha$ и что деление разложенных на простые множители целых чисел сводится к делению степеней каждого простого числа из этих разложений.

Если модуль $N = 4^{\aleph_0} p_1^{\aleph_1} \cdots p_t^{\aleph_t}$ (целые $\aleph_j \geq 1$ при $j = 1, ..., t$ и $\aleph_0 \geq 0$), то, согласно теореме A, множитель a будет вида $a = d 4^{r_0} p_1^{r_1} ... p_t^{r_t} + 1$ где $r_j \geq 1 \, (j = 1, ..., t)$ и $r_0 \geq 0$. Если целое число $\tau \geq 2$ достаточно большое, что $\tau r_j \geq \aleph_j$ для всех $j = 0, 1, ..., t$, то $N \mid (a-1)^{\tau}$. Тем самым, одно τ, для которого первое свойство из (3.18) выполнено, найдено. Далее, если в этом будет необходимость, то уменьшая до $\tau \geq 2$, убеждаемся в существовании наименьшого $\tau \geq 2$ со вторым свойством (3.18).

Лемма 8 доказана.

В заключение условимся об записях N и a в применениях.

Вводя, в случае необходимости, множитель $p = 2$ можно N и a записать в виде $N = p_1^{\aleph_1} \cdots p_t^{\aleph_t}$ и $a = 1 + d \times p_1^{r_1} ... p_t^{r_t}$.

При этом, освобождая, в случае наличия, d от простых множителей $p_1, ..., p_t$ можно считать, что d и N взаимно простые.

Тогда искомый потенциал записывается в виде $\tau = \max \left\{ \left\lceil \frac{\aleph_1}{r_1} \right\rceil, ..., \left\lceil \frac{\aleph_t}{r_t} \right\rceil \right\}$, где $\lceil x \rceil$ обозначает целую часть положительного числа x как не превосходящее x наибольшее целое число (см. об этом [1, стр. 40, Упр. 5] и [2, стр. 45, Упр. 5]).

§4. Комментарии и выводы

В этом параграфе уточним некоторые положения, в общем виде затронутых в §1 и обратимся к ряду других в свете полученных здесь результатов. Сразу же отметим, что нет жесткой привязки к параметрам генераторов случайных чисел a, N, $1 \leq a < N$, которым в допустимых для каждого случая применения пределах разрешено меняться (в том смысле, что если намеченная точность в $1/10^9$ оказалась недостаточной, то никто не будет следующую назначать в $1/\left(10^9 + 07022011\right)$ или $1/\left(10^9 + 22072013\right)$).

Отсюда приходим к следующим рекомендациям (нумерации которых продолжают нумерацию в §1).

11°. В теоремах 1–7 при фиксированном $s, s \geq 2$ определялось асимптотическое поведение $\nu_s(a, N)$ в зависимости от соотношений $\tau = s \geq 2, \tau > s$ и $2 \leq \tau < s$, где τ есть потенциал генератора $\langle \mathrm{X}_n(a, N) \rangle$, связывающий множитель a и максимальный период N в равенстве $(a-1)^{\tau} = N\lambda$.

Однако, в применениях, по результатам теорем 1–7, как это было показано в §1, роли τ и s меняются – генератор случайных чисел $\langle \mathrm{X}_n(a, N) \rangle_{n=0}^{N-1}$ задаётся через τ, a её спектральное

тестирование проводится по значениям величины $\nu_s(a,N;(a-1)^\tau = N\lambda)$ при переменной $s \geq 2$, асимптотически точные порядки которых заранее найдены в тех же теоремах 1–7.

12°. Теоремы 1–7 приводят к общему выводу: множитель $a, a \approx \nu_s(a,N)$ отвечает за s-точность, а потенциал τ - за величину максимального периода $N\lambda = (a-1)^\tau$ и за эффективные пределы s, $2 \leq s \leq \tau$.

13°. В открытых применениях при заданных множителе $a-1 = d \times p_1^{r_1} \cdots p_t^{r_t}$ и потенциале $\tau \geq 2$ можно ограничиться случаем $N = (a-1)^\tau = p_1^{\tau r_1} \cdots p_t^{\tau r_t}$, в то время как для обеспечения практически неограниченной конфиденциальности максимальный период $N = p_1^{\aleph_1} \cdots p_t^{\aleph_t}$, в сочетании с $\lambda = d \times p_1^{\tau r_1 - \aleph_1} \cdots p_t^{\tau r_t - \aleph_t}$ надлежит выбирать в ST-пределах с оценками

14°. В применениях надо не упускать из виду разницу между асимптотически точными формулами и конкретными вычислениями по ним.

В теоремах 1–7 оценки имеют вид $N^{\frac{1}{s}}\overline{\overline{\gamma}}_N \leq \nu_s(a,N) \leq N^{\frac{1}{s}}\overline{\gamma}_N$, которые носят асимптотический характер с явной записью величин $\overline{\gamma}_N$ и $\overline{\overline{\gamma}}_N$.

Абсолютно точные при неограниченном возрастании N, в конкретных вычислениях с обычно небольшими значениями N, погрешности могут быть ощутимыми.

В связи с чем заметим, что в ST-методе множители $\overline{\overline{\gamma}}_N = \left(1 - (b_\tau - 1)\, N^{-\frac{1}{\tau}}\right)$ и $\overline{\gamma}_N = \sqrt{1 + 2N^{-\frac{1}{\tau}} + 2N^{-\frac{2}{\tau}}}$ при $N^{\frac{1}{\tau}}$ являются лишь гарантирующими близость к наилучшему значению s-точности $\nu_s \equiv \nu_s(a,N;(a-1)^\tau = N)$ случайной последовательности $\langle X_n(a,N=(a-1)^\tau\rangle_{n=0}^{N-1}$, поэтому в применениях хотя и пишется $... \leq \nu_s$, действительность же может намного превосходить эти гарантии.

15°. Выбор максимального периода $N = (a-1)^\tau = p_1^{\aleph_1} \cdots p_t^{\aleph_t}$ произволен в силу произвольности выбора простых $1 < p_1 < p_2 < ... < p_t$ и положительных $\aleph_1, ..., \aleph_t$, произвольности выбора множителя $a = d \times p_1^{r_1} \cdots p_t^{r_t} + 1$ с произвольными положительными $r_1, ..., r_t$ и произвольности выбора потенциала $\tau \geq 2$, но связанных неравенствами $\aleph_j \leq r_j\tau$ для всех $j = 1, \ldots, s$ и $(\tau - 1)\, r_{j_0} < \aleph_{j_0}$ для некоторого j_0, что вполне соответствует требованиям в [2, стр. 118]: *«... когда для приложений нужен генератор случайных чисел, обеспечивающий получение последовательности, очень близкой к случайной, простые конгруэнтные генераторы для этого не подходят. Вместо них нужно использовать генератор с длинным периодом, даже если на самом деле необходимо генерировать только малую часть периода».*

Именно, при фиксированном множителе $a = d \times p_1^{r_1} \cdots p_t^{r_t} + 1$ увеличением потенциала τ можно добиться сколь угодно большого значения максимального периода $N = p_1^{\tau r_1} \cdots p_t^{\tau r_t}$. И не только «большого», но и с одновременным обеспечением контролируемого качества случайной последовательности $\langle X_n(a,(a-1)^\tau = N\lambda\rangle_{n=0}^{N-1}$ в виде независимости s-мерных векторов $(X_n, X_{n+1}, ..., X_{n+(s-1)})$ при всех $2 \leq s \leq \tau$ с двусторонними оценками асимптотического типа $\nu_s(a,N;(a-1)^\tau = N\lambda) \approx N^{\frac{1}{\tau(a,N)}}$ и $\mu_s(a,N;(a-1)^\tau = N\lambda) \approx \pi^{\frac{\tau(a,N)}{2}} \left(\frac{\tau(a,N)}{2}\right)!$. При этом здесь показатели предельно точны.

16°. Выбор множителя a с учетом особенностей ЭВМ, на котором проводятся вычисления, обсуждается в [2, 3.2.1.3. Потенциал, стр. 43]: *«В предыдущем разделе было показано, что максимальный период может быть достигнут, когда $a-1$ кратно каждому простому делителю N, и $a-1$ должно быть также кратно 4, если N кратно 4. Если b – основание системы счисления машины ($b = 2$ для бинарного компьютера и $b = 10$ для десятичного компьютера), N – длина слова в компьютере b^t, томножитель $a = b^k + 1$, $2 \leq k < t$ удовлетворяет этим условиям. По теореме A можно брать $c = 1$. Рекурентное соотношение теперь имеет вид*

$$X_{n+1} = \left(\left(b^k + 1\right) X_n + 1\right) \bmod b^t$$

и это уравнение означает, что можно избежать умножения; просто достаточно перемещения и суммирования».

Тогда, согласно соотношениям ST, при $N = b^t$ получаем $(a-1)^\tau = b^{k\tau} = b^t = N$ для всех τ, которые делят t, с двусторонней оценкой

$$a - b_\tau \le \nu_s(a, N; (a-1)^\tau = N) \le \sqrt{1+a^2}$$

для всех $2 \le s \le \tau$.

Далее, в [2, стр. 43-44] сообщается *«Например, пусть $a = B^2 + 1$, где B – размер байта компьютера MIX. Программа*

LDAX; SLA 2; ADDX; INCA 1

может использоваться вместо программы, приведенной в разделе 3.2.1.1, и время выполнения программы уменьшается от 16u до 7u.

По этой причине, множители, имеющие вид $a = b^k + 1$ широко обсуждались в литературе. Они действительно рекомендованы многими авторами. Однако первые несколько лет экспериментирования с этим методом убедительно показали, что множителей, имеющих простой вид $a = b^k + 1$, следует избегать. Сгенерированные числа просто недостаточно случайны».

Можно предположить, что точные, взамен экспериментальных, ST-соотношения в каждом конкретном случае приведут к правильным (адекватным) выводам.

17°. Произвольный выбор потенциала τ, поддерживающего при всех s, $2 \le s \le \tau$ независимость s-последовательных значений линейной конгруэнтной последовательности $\{X_n\}$ обеспечивается двусторонней асимптотически точной оценкой $\asymp N^{\frac{1}{\tau}}$ по ST-формулам, которые снимают все ограничения, связанные с *«доступными по [1-2]»* случаями $s = 2, 3, 4, 5, 6$ (см. [1 и 2, Раздел 3.3.4]).

18°. Приращение c, согласно теореме A, должно быть меньше значения максимального периода N и взаимно простым с ним. Возможность использования c в определении $X_{n+1} = (X_n a + c) \bmod N$ при заданных a и N с целью взаимного уничтожения по формуле (2.2) коэффициентов Фурье с отрицательным выводом обсуждалась в [1, стр. 123, Упражнение 11].

19°. Проверка выполнения условий (1.3)–(1.4) для заданных a и N является нетривиальной задачей. Так, в [1, стр. 33-40] и [2, стр. 40-45] вводятся специальные определения, в которых наименьшее решение τ сравнения $a^x \equiv 1 (\mathrm{mod} N)$ называют *порядком множителя a по модулю N*, а любое такое значение a, которое имеет *максимальный* возможный порядок по модулю N *-первообразным элементом* по модулю N.

По-видимому, теоремы 1-7, как это показано в 5°–16°, снимают необходимость в таких исследованиях, разве лишь в случаях, продиктованных другими соображениями.

20°. Не исключено, что методы создания новых генераторов комбинацией известных (см. [1, стр. 46] и [2, стр. 132-133]) с использованием построенных здесь, могут быть перспективными.

Отдельно изучим производную характеристику случайности $\mu_s(a, N)$.

21°. *Мера эффективности* $\mu_s(a, N) := \frac{\pi^{\frac{s}{2}}}{\left(\frac{s}{2}\right)!} \cdot \frac{\nu_s^s(a,N)}{N}$ *множителя a для заданного максимального периода N* как *«относительно независимое от N»* правило определения качества генератора случайных чисел N *изменяется в следующих пределах:*

ST-1 $\left(s = \tau = 2, (a-1)^2 = N\right)$:

$$\mu_2\left(a; N; N = (a-1)^2\right) = \pi\left(1 - 2\frac{a-2}{(a-1)^2}\right) = \pi\left(1 - 2\frac{\sqrt{N}-1}{N}\right),$$

ST-2 $(s \ge 3, a \ge b_s + 1, (a-1)^s = N)$:

$$\frac{\pi^{\frac{s}{2}}}{\left(\frac{s}{2}\right)!}\left(1 - (b_s - 1)N^{-\frac{1}{s}}\right)^s = \frac{\pi^{\frac{s}{2}}}{\left(\frac{s}{2}\right)!}\left(\frac{a-b_s}{a-1}\right)^s \le \mu_s(a, N; N = (a-1)^s) \le$$

$$\le \frac{\pi^{\frac{s}{2}}}{\left(\frac{s}{2}\right)!} \cdot \frac{\left(1+a^2\right)^{\frac{s}{2}}}{(a-1)^s} = \frac{\pi^{\frac{s}{2}}}{\left(\frac{s}{2}\right)!} \cdot \left(1 + 2N^{-\frac{1}{s}} + 2N^{-\frac{2}{s}}\right)^{\frac{s}{2}},$$

ST-3 $\left(s=\tau=2,\,(a-1)^2=N\lambda,\lambda\geq 2\right)$:

$$\frac{\pi}{\lambda}\cdot\left(1-2\cdot\frac{\sqrt{N\lambda}-1}{N\lambda}\right)=\frac{\pi}{\lambda}\cdot\left(\frac{1+(a-2)^2}{(a-1)^2}\right)\leq\mu_2\left(a,N:(a-1)^2=N\lambda,\lambda\geq 2\right)\overset{\lambda|(a-1)}{\leq}\frac{2\pi}{\lambda},$$

ST-4 $(\tau>s=2,(a-1)^\tau=N)$:

$$\pi N^{\frac{2}{\tau}-1}\left(1-(b_\tau-1)\,N^{-\frac{1}{\tau}}\right)^2=\pi\frac{(a-b_\tau)^2}{(a-1)^\tau}\leq\mu_2\left(a,N;(a-1)^\tau=N\right)\leq\pi\frac{\left(1+a^2\right)}{(a-1)^\tau}=$$

$$=\pi N^{\frac{2}{\tau}-1}\left(1+2N^{-\frac{1}{\tau}}+2N^{-\frac{2}{\tau}}\right),$$

ST-5 $(\tau=s\geq 2,\,(a-1)^s=N\lambda,\ \lambda\geq 1)$:

$$\frac{\pi^{\frac{s}{2}}}{\left(\frac{s}{2}\right)!}\frac{1}{\lambda^{s-1}}\left(\sum_{k=0}^{s-1}\left(\binom{s-1}{k}\right)^2\right)^{\frac{s}{2}}\overset{\lambda|(a-1)}{\geq}\mu_s\left(a,N;(a-1)^s=N\lambda\right)\geq$$

$$\geq\frac{\pi^{\frac{s}{2}}}{\left(\frac{s}{2}\right)!}\cdot\frac{1}{\lambda^{s-1}}\cdot\frac{(a-b_s)^s}{(a-1)^s}=\frac{\pi^{\frac{s}{2}}}{\left(\frac{s}{2}\right)!}\cdot\frac{1}{\lambda^{s-1}}\left(1-(b_s-1)\,(N\lambda)^{-\frac{1}{s}}\right)^s,$$

ST-6 $\left(2\leq s<\tau,(a-1)^\tau=N\lambda,1\leq\lambda\leq(a-1)^{\tau-s}\right)$:

$$\frac{\pi^{\frac{s}{2}}}{\left(\frac{s}{2}\right)!}\cdot\frac{\left((N\lambda)^{\frac{1}{\tau}}\left(1-(b_s-1)\,(N\lambda)^{-\frac{1}{\tau}}\right)\right)^s}{N}=\frac{\pi^{\frac{s}{2}}}{\left(\frac{s}{2}\right)!}\frac{(a-b_s)^s\times\lambda}{(a-1)^\tau}\leq$$

$$\leq\mu_s(a,N;(a-1)^\tau=N\lambda)\leq\frac{\pi^{\frac{s}{2}}}{\left(\frac{s}{2}\right)!}\frac{\left(1+a^2\right)^{\frac{s}{2}}\times\lambda}{(a-1)^\tau}=\frac{\pi^{\frac{s}{2}}}{\left(\frac{s}{2}\right)!}\frac{\left((N\lambda)^{\frac{1}{\tau}}\sqrt{1+2\,(N\lambda)^{-\frac{1}{\tau}}+2\,(N\lambda)^{-\frac{2}{\tau}}}\right)^s}{N},$$

ST-7 $\left(2\leq s<\tau,(a-1)^\tau=N\lambda,\lambda=(a-1)^{\tau-s+1},...,(a-1)^{\tau-2}\right)$:

$$\mu_s(a,N;(a-1)^\tau=N\lambda,\lambda=(a-1)^{\tau-s+1},...,(a-1)^{\tau-2})\leq$$

$$\leq\frac{\pi^{\frac{s}{2}}}{\left(\frac{s}{2}\right)!}\cdot\left(\sum_{k=0}^{s-1}\left(\binom{s-1}{k}\right)^2\right)^{\frac{s}{2}}\cdot\frac{1}{N}=\frac{\pi^{\frac{s}{2}}}{\left(\frac{s}{2}\right)!}\cdot\left(\sum_{k=0}^{s-1}\left(\binom{s-1}{k}\right)^2\right)^{\frac{s}{2}}\cdot\frac{\lambda}{(a-1)^\tau},$$

ST-8 $(2\leq\tau<s,\,(a-1)^\tau=N\lambda,\,\lambda\geq 1)$:

$$\mu_s\left(a,N;(a-1)^\tau=N\lambda\right)\leq\frac{\pi^{\frac{s}{2}}}{\left(\frac{s}{2}\right)!}\cdot\left(\sum_{k=0}^{\tau}\left(\binom{\tau}{k}\right)^2\right)^{\frac{s}{2}}\cdot\frac{1}{N},$$

где $(-b_m)$ *есть наибольший по модулю отрицательный биномиальный коэффициент в разложении* $(a-1)^m$ *по степеням* a*:* $b_2=2,b_3=3,b_4=4,b_5=10,b_6=20,b_7=35,b_8=56,b_9=126,b_{10}=252,b_{11}=462,b_{12}=792,b_{13}=1716,b_{14}=3432,b_{15}=6435,...$ *и т. д.*

Отметим, что здесь $\frac{\pi^{\frac{s}{2}}}{\left(\frac{s}{2}\right)!}\to 0\ (s\to\infty)$: согласно формуле Стирлинга при четных $s=2m$ имеем $(\theta(m)\to 0)$

$$\frac{\pi^{\frac{s}{2}}}{\left(\frac{s}{2}\right)!}=\frac{\pi^m}{m!}=\frac{\pi^m\cdot e^m}{\sqrt{2\pi m}\cdot m^m\cdot e^{\theta(m)}}=\frac{1}{\sqrt{2\pi m}\cdot e^{\theta(m)}}\cdot\left(\frac{\pi e}{m}\right)^m\to 0\ (s\to\infty),$$

то же при нечетных $s=2m+1$

$$\frac{\pi^{\frac{s}{2}}}{\left(\frac{s}{2}\right)!}=\frac{\pi^{m+\frac{1}{2}}}{\left(\frac{2m+1}{2}\right)\left(\frac{2m-1}{2}\right)\left(\frac{2m-3}{2}\right)...\left(\frac{2m-(2m-5)}{2}\right)\left(\frac{3}{2}\right)\left(\frac{1}{2}\right)}\eqsim$$

$$\eqsim\frac{\pi^{m+\frac{1}{2}}\cdot 2^{2m+1}\cdot 2^m\cdot(m!)}{(2m+1)!}\eqsim\frac{\pi^{m+\frac{1}{2}}\cdot 2^{3m+1}\sqrt{2\pi m}\cdot m^m\cdot e^{2m+1}}{\sqrt{2\pi\,(2m+1)}\cdot(2m+1)^{2m+1}\cdot e^m}\approx\frac{\pi^{\frac{1}{2}}\cdot e}{\sqrt{2}\cdot m}\cdot\left(\frac{2\pi e}{m}\right)^m\to 0\ (s\to\infty).$$

В принятых определениях и обозначениях сравним ST-результаты с известными [1-2] (при $\lambda=1$).

В полном согласии с $\nu_s^s\left(a,N;N=(a-1)^{\tau(a,N)}\right)\asymp N^{\frac{1}{\tau(a,N)}}$ мера эффективности 0 и N возрастает при возрастании s от 2 до $\tau\,(a,N)$:

$$\mu_s\left(a,N;N=(a-1)^{\tau(a,N)}\right)=\frac{\pi^{\frac{s}{2}}\nu_s^s\left(a,N;N=(a-1)^{\tau(a,N)}\right)}{\left(\frac{s}{2}\right)!N}\asymp$$
$$\asymp\frac{\pi^{\frac{s}{2}}}{\left(\frac{s}{2}\right)!}\cdot\frac{1}{N^{1-\frac{s}{\tau(a,N)}}}\,(2\le s\le\tau(a,N))\,, \tag{4.1}$$

причем возрастает до максимального $\frac{\pi^{\frac{\tau(a,N)}{2}}}{\left(\frac{\tau(a,N)}{2}\right)!}$, затем, при переходе s через $\tau\,(a,N)$ становится *«ужасно малым»*

$$\mu_s\,(a,N)\le\frac{\pi^{\frac{s}{2}}\cdot\left(\sum_{k=0}^{\tau}\left(\binom{\tau(a,N)}{k}\right)^2\right)^{\frac{s}{2}}}{\left(\frac{s}{2}\right)!}\cdot\frac{1}{N}(s>\tau(a,N)). \tag{4.2}$$

Эти выводы также подтверждаются экспериментальными данными из [2, стр. 131]

Строка	a	N	μ_2	μ_3	μ_4	μ_5	μ_6	$e=\frac{1}{10}$
2	2^7+1	2^{35}	$2e^6$	$3e^4$	0. 04	4. 66	$2e^3$	

Действительно, в согласии с (4.1)–(4.2) при $\tau=5$ происходит рост $\mu_2=\frac{2}{10^6}<\mu_3=\frac{3}{10^4}<\mu_4=\frac{4}{10^2}$ с пиковым $\mu_5=4.66$ и резким падением $\mu_6=\frac{2}{10^3}$.

Числовые данные, полученные по оценкам (4.1)–(4.2) подтверждаютили опровергают (тогда, по-видимому, надо провести пересчет) эти показатели:

$a=2^7+1$	$N=2^{35}$	$1.47471e^6\le\mu_2$ $\le 1.52161e^6$	$2.4386551e^4\le\mu_3$ $\le 2.6172608e^4$	$3.506387856e^2\le\mu_4$ $\le 3.977690029e^2$	$3.65580844757\le\mu_5$ ≤ 5.47346593181	$\mu_6\le 2.40685602e^3$

То же происходит с $\mu_s(a,N)$ и при $\lambda>1$

$$\mu_s(a,N;\ (a-1)^s=N\lambda,\lambda|\,(a-1))\asymp\frac{\pi^{\frac{s}{2}}}{\left(\frac{s}{2}\right)!}\cdot\frac{1}{\lambda^{s-1}},$$

в котором асимптотически точное при $\lambda=1$ равенство $\asymp\pi^{\frac{s}{2}}\Big/\left(\frac{s}{2}\right)!$ ухудшается на множитель $1\big/\lambda^{s-1}$.

Как это показывают теоремы 1–7, оценка сверху через $\gamma_N\cdot N^{\frac{1}{s}}$ для $\nu_s\,(a,N)$ в теореме B достижима, поэтому естественно было бы определить $\mu_s\,(a,N)$ как отношение $\frac{\nu_s^s(a,N)}{N}$, без множителя $\pi^{\frac{s}{2}}/\left(\frac{s}{2}\right)!$.

Это предложение основывается на том обстоятельстве, что данная величина, о чем сообщалось выше при цитировании причин введения в теорию спектрального тестирования меры эффективности $\mu_s\,(a,N)$, появилась из вероятностных соображений в виде объёма эллипсоида в s-мерном пространстве, но, которое, как показывает проведенное здесь исследование, прямого отношения к обсуждаемой тематике не имеет.

В определении $\overline{\mu_s}\,(a,N):=\frac{\nu_s^s(a,N)}{N}=\frac{\left(\frac{s}{2}\right)!}{\pi^{\frac{s}{2}}}\cdot\mu_s(a,N)$ (без зависящего только от s множителя $\frac{\pi^{\frac{s}{2}}}{\left(\frac{s}{2}\right)!}$, искажающем соотношения между $\nu_s(a,N)$ и N) меры эффективности множителя a для максимального периода N результаты по спектральному тестированию (ST) переписываются в виде

ST-1 $(s=\tau=2,\lambda=1)$**:** $\overline{\mu_2}\left(a;N;N=(a-1)^2\right)\asymp 1$

ST-2 $(\tau=s\ge 3,N=(a-1)^s,\lambda=1)$**:** $\overline{\mu_s}\,(a,N;N=(a-1)^s)\asymp 1$

ST-3 $(s=\tau=2,\lambda\ge 2)$**:** $\overline{\mu_2}\left(a,N:(a-1)^2=N\lambda,\lambda\ge 2\right)\asymp\frac{1}{\lambda}$

ST-4 $(\tau>s=2,\lambda=1)$**:** $\overline{\mu_2}\,(a,N;(a-1)^\tau=N)\asymp\frac{1}{N^{1-\frac{2}{\tau}}}$

ST-5 $(\tau=s\ge 2,\ (a-1)^s=N\lambda,\ \lambda\ge 1,\ \lambda|\,(a-1))$**:** $\overline{\mu_s}\,(a,N;(a-1)^s=N\lambda)\asymp\frac{1}{\lambda^{\tau-1}}$

ST-6 $\left(2\le s<\tau,(a-1)^\tau=N\lambda,1\le\lambda\le(a-1)^{\tau-s}\right)$**:** $\overline{\mu_s}(a,N;(a-1)^\tau=N\lambda)\asymp\frac{\lambda^{\frac{1}{\tau}}}{N^{1-\frac{1}{\tau}}}$

ST-7 $\left(2 \le s < \tau, (a-1)^{\tau} = N\lambda, \lambda = (a-1)^{\tau-s+1}, ..., (a-1)^{\tau-2}\right)$**:** $\overline{\mu_s}(a, N; (a-1)^{\tau} = N\lambda, \lambda = (a-1)^{\tau-s+1}, ..., (a-1)^{\tau-2}) \ll \frac{1}{N}$

ST-8 $(2 \le \tau < s,\ (a-1)^{\tau} = N\lambda,\ \lambda \ge 1)$**:** $\overline{\mu_s}\,(a, N; (a-1)^{\tau} = N\lambda) \ll \frac{1}{N}$.

В свете выписанных асимптотических и порядковых равенств для $\mu_s(a, N)$ и $\overline{\mu_s}(a, N)$ вновь обратимся к мотивам их назначения «*В некоторых случаях хорошо бы иметь правила для определения, удовлетворяет ли датчик критерию, относительно независимое от* N *чтобы можно было сказать, что некоторый множитель* a *хорош либо плох по отношению к другим множителям для заданного* N *, не проверяя остальных* (см. [2, стр. 128])».

Во всех случаях при $2 \le s \le \tau$ величина $\overline{\mu_s}(a, N; (a-1)^{\tau} = \lambda N)$ асимптотически или порядково зависит только N, λ и τ при связанном с ними равенством $(a-1)^{\tau} = \lambda N$ множителе a, обращающем Генератор Лехмера в оптимальный, поэтому вопрос «*некоторый множитель* a *хорош либо плох по отношению к другим множителям для заданного* N *, не проверяя остальных*» отпадает.

И, наконец, $\mu_s\,(a, N) = \frac{\left(\frac{s}{2}\right)!}{\pi^{\frac{s}{2}}} \cdot \overline{\mu_s}\,(a, N)$, т. е. вносится ещё зависимость от s, никак не связанная с выбором a при фиксированном N, что вкупе с другими вышеизложенными аргументами вызывает сомнение в её информативности как *меры эффективности множителя* a .

22 °. От неосязаемой напрямую асимптотической оценки $\nu_s(a, N)$ обратимся к геометрически наглядной составляющей случайности в виде «*частотности*», в котором числа $0, 1, \ldots N-1$ надлежит переставить в другом порядке $X_0, \ldots,\ X_{N-1}$ как биективное отображение на себя таким образом, чтобы для любого сегмента $[\alpha, \beta]$ из $[0, 1]$ количество чисел $\frac{X_n}{N}$ попавших в $[\alpha, \beta]$ должно быть близко $(\beta - \alpha)$.

Конечно, здесь приведено только интуитивное описание частотности в изучаемом конкретном случае. Представление о фундаментальном значении частотности можно получить по следующему высказыванию А. Н. Колмогорова в статье «О таблицах случайных чисел» (см. [17]): «*Основой применимости математической теории вероятностей к случайным явлениям реального мира является частотный подход к вероятности в той или иной форме, неизбежность обращения к которому горячо отстаивал фон Мизес*».

Во всех задачах, в которых требуется построить равномерно распределенную на $[0, 1]$ последовательность

$$U_n = \frac{X_n}{N} \quad (n = 0, ..., N-1)$$

с обеспечением s-случайности в смысле независимости s следующих друг за другом наборов чисел $\left(U_n, U_{n+1},\ ..., U_{n+(s-1)}\right)$ на полном периоде из N членов и если можно ограничиться точностью $\frac{1}{\nu_s(a, N=(a-1)^s)}$, когда первые $\lg \nu_s\left(a, N = (a-1)^{\,s}\right)$ разрядов в двоичном представлении чисел можно считать случайными, то в качестве $\langle X_n \rangle$, согласно S–T-результатам, надо принять $\langle X_n\,(a, N = (a-1)^s, c = 1, X_0 = 0) \rangle_{n=0}^{N-1}$.

Проведем вычислительный эксперимент на «частотность» с Генератором случайных чисел Лехмера, построенного по $a = 26, \tau = 2$ и $N = 625$:

$$X_{n+1} = (X_n \cdot 26 + 1) \bmod 625\,(n = 0, ..., 624; X_0 = 0)\,.$$

Полученная последовательность $\langle U_n \rangle_{n=0}^{N-1}$ случайных чисел вынесена в Таблицу 3:

Таблица 3 – Случайные числа.

0,0016; 0,0432; 0,1248; 0,2464; 0,408; 0,6096; 0,8512; 0,1328; 0,4544; 0,816; 0,2176; 0,6592; 0,1408; 0,6624; 0,224; 0,8256; 0,4672; 0,1488; 0,8704; 0,632; 0,4336; 0,2752; 0,1568; 0,0784; 0,04; 0,0416; 0,0832; 0,1648; 0,2864; 0,448; 0,6496; 0,8912; 0,1728; 0,4944; 0,856; 0,2576; 0,6992; 0,1808; 0,7024; 0,264; 0,8656; 0,5072; 0,1888; 0,9104; 0,672; 0,4736; 0,3152; 0,1968; 0,1184; 0,08; 0,0816; 0,1232; 0,2048; 0,3264; 0,488; 0,6896; 0,9312; 0,2128; 0,5344; 0,896; 0,2976; 0,7392; 0,2208; 0,7424; 0,304; 0,9056; 0,5472; 0,2288; 0,9504; 0,712; 0,5136; 0,3552; 0,2368; 0,1584; 0,12; 0,1216; 0,1632; 0,2448; 0,3664; 0,528; 0,7296; 0,9712; 0,2528; 0,5744; 0,936; 0,3376; 0,7792; 0,2608;

0,7824; 0,344; 0,9456; 0,5872; 0,2688; 0,9904; 0,752; 0,5536; 0,3952; 0,2768; 0,1984; 0,16; 0,1616; 0,2032; 0,2848; 0,4064; 0,568; 0,7696; 0,0112; 0,2928; 0,6144; 0,976; 0,3776; 0,8192; 0,3008; 0,8224; 0,384; 0,9856; 0,6272; 0,3088; 0,0304; 0,792; 0,5936; 0,4352; 0,3168; 0,2384; 0,2; 0,2016; 0,2432; 0,3248; 0,4464; 0,608; 0,8096; 0,0512; 0,3328; 0,6544; 0,016; 0,4176; 0,8592; 0,3408; 0,8624; 0,424; 0,0256; 0,6672; 0,3488; 0,0704; 0,832; 0,6336; 0,4752; 0,3568; 0,2784; 0,24; 0,2416; 0,2832; 0,3648; 0,4864; 0,648; 0,8496; 0,0912; 0,3728; 0,6944; 0,056; 0,4576; 0,8992; 0,3808; 0,9024; 0,464; 0,0656; 0,7072; 0,3888; 0,1104; 0,872; 0,6736; 0,5152; 0,3968; 0,3184; 0,28; 0,2816; 0,3232; 0,4048; 0,5264; 0,688; 0,8896; 0,1312; 0,4128; 0,7344; 0,096; 0,4976; 0,9392; 0,4208; 0,9424; 0,504; 0,1056; 0,7472; 0,4288; 0,1504; 0,912; 0,7136; 0,5552; 0,4368; 0,3584; 0,32; 0,3216; 0,3632; 0,4448; 0,5664; 0,728; 0,9296; 0,1712; 0,4528; 0,7744; 0,136; 0,5376; 0,9792; 0,4608; 0,9824; 0,544; 0,1456; 0,7872; 0,4688; 0,1904; 0,952; 0,7536; 0,5952; 0,4768; 0,3984; 0,36; 0,3616; 0,4032; 0,4848; 0,6064; 0,768; 0,9696; 0,2112; 0,4928; 0,8144; 0,176; 0,5776; 0,0192; 0,5008; 0,0224; 0,584; 0,1856; 0,8272; 0,5088; 0,2304; 0,992; 0,7936; 0,6352; 0,5168; 0,4384; 0,4; 0,4016; 0,4432; 0,5248; 0,6464; 0,808; 0,0096; 0,2512; 0,5328; 0,8544; 0,216; 0,6176; 0,0592; 0,5408; 0,0624; 0,624; 0,2256; 0,8672; 0,5488; 0,2704; 0,032; 0,8336; 0,6752; 0,5568; 0,4784; 0,44; 0,4416; 0,4832; 0,5648; 0,6864; 0,848; 0,0496; 0,2912; 0,5728; 0,8944; 0,256; 0,6576; 0,0992; 0,5808; 0,1024; 0,664; 0,2656; 0,9072; 0,5888; 0,3104; 0,072; 0,8736; 0,7152; 0,5968; 0,5184; 0,48; 0,4816; 0,5232; 0,6048; 0,7264; 0,888; 0,0896; 0,3312; 0,6128; 0,9344; 0,296; 0,6976; 0,1392; 0,6208; 0,1424; 0,704; 0,3056; 0,9472; 0,6288; 0,3504; 0,112; 0,9136; 0,7552; 0,6368; 0,5584; 0,52; 0,5216; 0,5632; 0,6448; 0,7664; 0,928; 0,1296; 0,3712; 0,6528; 0,9744; 0,336; 0,7376; 0,1792; 0,6608; 0,1824; 0,744; 0,3456; 0,9872; 0,6688; 0,3904; 0,152; 0,9536; 0,7952; 0,6768; 0,5984; 0,56; 0,5616; 0,6032; 0,6848; 0,8064; 0,968; 0,1696; 0,4112; 0,6928; 0,0144; 0,376; 0,7776; 0,2192; 0,7008; 0,2224; 0,784; 0,3856; 0,0272; 0,7088; 0,4304; 0,192; 0,9936; 0,8352; 0,7168; 0,6384; 0,6; 0,6016; 0,6432; 0,7248; 0,8464; 0,008; 0,2096; 0,4512; 0,7328; 0,0544; 0,416; 0,8176; 0,2592; 0,7408; 0,2624; 0,824; 0,4256; 0,0672; 0,7488; 0,4704; 0,232; 0,0336; 0,8752; 0,7568; 0,6784; 0,64; 0,6416; 0,6832; 0,7648; 0,8864; 0,048; 0,2496; 0,4912; 0,7728; 0,0944; 0,456; 0,8576; 0,2992; 0,7808; 0,3024; 0,864; 0,4656; 0,1072; 0,7888; 0,5104; 0,272; 0,0736; 0,9152; 0,7968; 0,7184; 0,68; 0,6816; 0,7232; 0,8048; 0,9264; 0,088; 0,2896; 0,5312; 0,8128; 0,1344; 0,496; 0,8976; 0,3392; 0,8208; 0,3424; 0,904; 0,5056; 0,1472; 0,8288; 0,5504; 0,312; 0,1136; 0,9552; 0,8368; 0,7584; 0,72; 0,7216; 0,7632; 0,8448; 0,9664; 0,128; 0,3296; 0,5712; 0,8528; 0,1744; 0,536; 0,9376; 0,3792; 0,8608; 0,3824; 0,944; 0,5456; 0,1872; 0,8688; 0,5904; 0,352; 0,1536; 0,9952; 0,8768; 0,7984; 0,76; 0,7616; 0,8032; 0,8848; 0,0064; 0,168; 0,3696; 0,6112; 0,8928; 0,2144; 0,576; 0,9776; 0,4192; 0,9008; 0,4224; 0,984; 0,5856; 0,2272; 0,9088; 0,6304; 0,392; 0,1936; 0,0352; 0,9168; 0,8384; 0,8; 0,8016; 0,8432; 0,9248; 0,0464; 0,208; 0,4096; 0,6512; 0,9328; 0,2544; 0,616; 0,0176; 0,4592; 0,9408; 0,4624; 0,024; 0,6256; 0,2672; 0,9488; 0,6704; 0,432; 0,2336; 0,0752; 0,9568; 0,8784; 0,84; 0,8416; 0,8832; 0,9648; 0,0864; 0,248; 0,4496; 0,6912; 0,9728; 0,2944; 0,656; 0,0576; 0,4992; 0,9808; 0,5024; 0,064; 0,6656; 0,3072; 0,9888; 0,7104; 0,472; 0,2736; 0,1152; 0,9968; 0,9184; 0,88; 0,8816; 0,9232; 0,0048; 0,1264; 0,288; 0,4896; 0,7312; 0,0128; 0,3344; 0,696; 0,0976; 0,5392; 0,0208; 0,5424; 0,104; 0,7056; 0,3472; 0,0288; 0,7504; 0,512; 0,3136; 0,1552; 0,0368; 0,9584; 0,92; 0,9216; 0,9632; 0,0448; 0,1664; 0,328; 0,5296; 0,7712; 0,0528; 0,3744; 0,736; 0,1376; 0,5792; 0,0608; 0,5824; 0,144; 0,7456; 0,3872; 0,0688; 0,7904; 0,552; 0,3536; 0,1952; 0,0768; 0,9984; 0,96; 0,9616; 0,0032; 0,0848; 0,2064; 0,368; 0,5696; 0,8112; 0,0928; 0,4144; 0,776; 0,1776; 0,6192; 0,1008; 0,6224; 0,184; 0,7856; 0,4272; 0,1088; 0,8304; 0,592; 0,3936; 0,2352; 0,1168; 0,0384; 0

Для данного отрезка $[\alpha,\beta]$ $(0 \le \alpha < \beta \le 1)$ обозначим через $m \equiv m(\alpha,\beta)$ количество случайных чисел U_n, попавших в отрезок $[\alpha,\beta]$ и, соответственно, частоту $\frac{m}{N} = \frac{m(\alpha,\beta)}{N}$ попадания $\langle U_n \rangle$ в отрезок $[\alpha,\beta]$. Тогда величина $\Delta \equiv \Delta(\alpha,\beta) = \left|\frac{m(\alpha,\beta)}{N} - (\beta-\alpha)\right|$

принимается за меру равномерной распределенности – чем меньше, тем лучше. Будем руководствоваться следующими примерами выбора отрезков: [*год, месяц, день рождения матери; год, месяц, день рождения студента*], $\left[\frac{1}{\pi^2}, 1-\frac{1}{e}\right]$, с концами из членов полученной последовательности и еще несколько "случайных" сегментов.

Таблица 4 – Результаты проверки случайных чисел из Таблицы 3 на равномерную распределенность.

	α	β	m	m/N	$\beta-\alpha$	Δ
$\langle X_n\,(a=26; N=625)\rangle_{n=0}^{624}$ $\nu_2 \approx 24.02$	0.580815	0.850411	168	0.2688	0.2696	0.000796
	$1/\pi^2$	$1-1/e$	332	0.5312	0.530799	0.0004
	0.15	0.32	107	0.17	0.1712	0.0012
	0.1	0.9	500	0.8	0.8	0
	0	0.9872	616	0.9872	0.9856	0.0016
	0.2	0.9	437	0.6992	0.7	0.0008
	0.100922291	0.620622291	324	0.5184	0.5197	0.0013

Тем самым, конкретный генератор $X_{n+1} = (X_n \cdot 26 + 1) \bmod 625\,(n = 0, ..., 624; X_0 = 0)$ выдержал выборочную проверку на равномерную рапределенность: Δ с двумя нулями после запятой при относительно небольшом $N = 625$ с $\nu_2(26, 625) = \sqrt{577}$.

Как оказалось, свойством равномерной распределенности обладают все Генераторы случайных чисел Лехмера с максимальным периодом (за указание на это автор благодарен Н.Ж. Наурызбаеву): последовательность $\frac{X_0}{N}, \frac{X_1}{N}, \ldots, \frac{X_{N-1}}{N}$ есть записанная в порядке $X_0, X_1, \ldots, X_{N-1}$ равномерная сетка $\frac{0}{N}, \frac{1}{N}, \ldots, \frac{N-1}{N}$, делящая отрезок $[0, 1]$ на N равных частей, и поэтому при всех $0 \le \alpha < \beta \le 1$ и некоторых целых k_α и k_β выполнены неравенства

$$\frac{k_\alpha}{N} \le \alpha \le \frac{k_\alpha + 1}{N} \le \frac{k_\beta}{N} \le \beta \le \frac{k_\beta + 1}{N},$$

откуда следует

$$\Delta_{\alpha,\beta} \le \frac{1}{N},$$

в частности, при $N = 625, \Delta_{\alpha,\beta} \le \frac{1}{625} = 0,0016$.

В итоге, приходим к выводу: вся проблема случайности последовательности Лехмера в смысле спектрального теста Ковэю и Макферсона заключена в величине $\nu_s(a, N)$, а равномерная распределенность есть прямое следствие Теоремы А – Критерия максимального периода.

Относительно испытаний на независимость заранее можно считать, что любой S"-генератор случайных чисел, включая, конечно, и рассматриваемый, уже прошел проверку критерием серий [2, стр. 133, ***F. Связь с критерием серий***]: *«В ряде значительных работ, опубликованных в 70-е годы, Гаральд Нидеррейтер (Harald Niederreiter) показал, как проводить исследования s-мерных векторов* $\{(U_n, ..., U_{n+s-1}) : 0 \le \mathrm{n} < \mathrm{N}\}$ *с помощью экспоненциальных сумм. Одним из основных результатов его теории было следующее: он показал, что* ***генератор случайных чисел проходит проверку с помощью критерия серий для нескольких измерений, если этот генератор выдерживает проверку спектральным критерием, даже*** *когда вместо полного периода рассматривается большая его часть».*

Замечание. Перспективы количественного изучения «частотности» выражены К. Ротом в [18]: *«Грубо говоря, наука об* ***«иррегулярностях распределения»*** *изучает в каких пределах конечный набор точечных масс в K-мерном кубе может (в различных геометрических смыслах) послужить приближением к равномерному распределению массы по всему кубу. … Я ожидаю, что в будущем вся эта тематика в целом будет расширяться, ее значение будет расти и обнаружатся интересные взаимосвязи между ее различными частями».*

В связи с чем отметим, что статьи [7–12] посвящены этой проблематике.

23°. В связисо многими вычислительными экспериментами в [1–2], среди которых *«Метод средин квадратов фон Неймана, как было показано, фактически является сравнительно бедным источником случайных чисел. Опасность состоит в том, что последовательность*

стремится войти в привычную колею, т. е. короткий цикл повторяющихся элементов. Например, каждое появление нуля как числа последовательности приведет к тому, что все последующие числа также будут нулями.

Некоторые ученые экспериментировали с методом средин квадратов в начале 1950-х годов. Работая с четырехзначными числами вместо десятизначных, Дж. Э. Форсайт (G. E. Forsythe) испытал 16 различных начальных значений и обнаружил, что 12 из них приводят к циклическим последовательностям, заканчивающимся циклом 6100, 2100, 4100, 8100, 6100,..., в то время как две из них приводят к последовательностям, вырождающимся в 0. Более интенсивные исследования, главным образом в двоичной системе счисления, провел Н. К. Метрополис (N. C. Metropolis). Он показал, что если использовать 20-разрядное число, то последовательность случайных чисел, полученная методом средин квадратов, вырождается в 13 различных циклов, причем длина самого большого периода равна 142.

Используя 38-разрядные числа, Метрополис получил невырожденную последовательность, содержащую около 750 000 чисел (прежде чем произошло вырождение), и полученные 750 000 × 38 бит удовлетворительно прошли статистический тест на случайность. [Symp. on Monte Carlo Methods (Wiley, 1956), 29-36.] Эти опыты показали, что метод средин квадратов может давать удовлетворительные результаты, но ему опасно доверять, пока не выполнены тщательные вычисления», с выводом: ***«Мораль этой истории в том, что случайные числа не следует генерировать методом, выбранным наудачу. Нужна какая-нибудь теория.*** *В следующих разделах будут рассмотрены генераторы случайных чисел более высокого уровня, чем метод средин квадратов»* [1, стр. 18; 2, стр. 25].

Эту ситуацию с центральным для Компьютерных наук выводом Жиль Земор в [15, Пункт 3.2] описывает в следующих словах: *«Возникает искушение заняться составлением супернепредсказуемых псевдослучайных генераторов, выбирая функцию f, которая действует нестолько произвольно. Кнут цитирует фон Неймана, предложившего функцию $f : [0, 10^m] \to [0, 10^m]$, представляющую собой возведение целого числа X в квадрат, за которым следует извлечение из середины десятичной записи числа X^2 некоторых m цифр. А затем он рассказывает, каково же было удивление, когда, запрограммировав этот генератор, он обнаружил очень быструю сходимость к неподвижной точке, то есть к такому X, для которого $f(X) = X$. Мораль этого опыта в том, что, как ни парадоксально, но псевдослучайный генератор, выбранный случайным образом, плох. Эту кажущуюся загадку можно объяснить, если изучить период генераторов. Заметим, что любой псевдослучайный генератор f типа $f : E \to E$ периодичен, потому что N равное мощности E конечно, и мы неизбежно получим $f(X_n) = f(X_k)$ для какого-то $k < n$. И тогда мы увидим, что функция будет бесконечно воспроизводить цикл $(X_k,\ X_{k+1}, \ldots,\ X_n)$. Очевидно, хочется, чтобы псевдослучайный генератор имел длинный период, хотя он, конечно, будет ограничен числом N ».*

В связи с чем отметим, что найденные чисто методами математического анализа ST-утверждения, в теоретическом плане фактически закрывающие тему, в практическом аспекте могут существенно сократить компьютерные поиски.

24°. По-видимому, переход от прямого исследования (1.10) к более общему случаю квадратических форм (см. [1, стр. 113] и [2, стр. 121] *«Мы доказали, что*

$$\nu_t^2 = \min_{(u_1,\ldots,u_t)\neq(0,\ldots,0)} \left\{u_1^2 + \cdots + u_t^2 | u_1 + au_2 + \cdots + a^{t-1}u_t \equiv 0 \,(\text{по модулю}\, N)\right\} =$$

$$= \min_{(x_1,\ldots,x_t)\neq(0,\ldots,0)} \left\{\left(Nx_1^2 - ax_2 - a^2x_3 - \cdots - a^{t-1}x_t\right)^2 + x_2^2 + x_3^2 + \cdots + x_t^2\right\}. \qquad (16)$$

С. Обоснование вычислительныхметодов. *Сведем спектральный критерий к задаче нахождения минимального значения (16). Но как можно найти минимальное значение за разумный отрезок времени? Грубое силовое исследование не входит в наши планы, так как N - очень большое в случаях, представляющих практический интерес.*

Будет интересно и, возможно, более полезно разработать вычислительные методы решений даже более общей проблемы: найти минимальное значение величины

$$f(x_1, ..., x_t) = (u_{11}x_1 + \cdots + u_{t1}x_t)^2 + \cdots + (u_{1t}x_1 + \cdots + u_{tt}x_t)^2 \quad (17)$$

по всем ненулевым целым вектором $(x_1, ..., x_t)$ *для любой невырожденной матрицы с коэффициентами* $U = (u_{ij})$. *Выражение (17) назовем положительно определенной квадратичной формой от* t *переменных.»*, составил методологический просчет (по крайней мере до издания [2], где результатов данной статьи нет).

25°. Основной результат данной статьи составляют двусторонние предельно точные оценки s-мерной точности генератора случайных чисел – меры эффективности множителя a для заданного максимального периода $N, N\lambda = (a-1)^\tau$ во всех случаях из (1.12).

Тем самым, в условиях наличия явных ST-формул, быть может за некоторыми исключениями, какие-то алгоритмические вычисления ν_s теряют смысл, в связи с чем приведем «[2, стр. 121] ***D. Как выполнить спектральный критерий.*** *В этом разделе будет приведена эффективная вычислительная процедура.*

Алгоритм S (Спектральный критерий). Этот алгоритм определяет значение

$$\nu_s = \min\left\{\sqrt{x_1^2 + \ldots + x_s^2} | x_1 + ax_2 + \ldots + a^{s-1}x_s \equiv 0 \quad (\text{по модулю } N)\right\}$$

для $2 \le s \le T$, *заданных* a, N *и* T, *где* $0 < a < N$ *и* a *и* N *- взаимно простые числа. (Минимум взят по всем ненулевым целочисленным векторам* $(x_1, \ldots, x_s)$, *а число* v_s *является* s*-мерной точностью генератора случайных чисел, как обсуждалось выше.) Вся арифметика в пределах алгоритма дана в целых числах, размеры которых редко либо никогда не превышают* N^2, *исключая шаг S7. К тому же почти все целые переменные будут меньше* N *по абсолютной величине на протяжении вычислений».*

§5. Примеры генераторов случайных чисел с максимальным периодом в контексте известных и популярных

Вынесенную в название параграфа тему, которой посвящена Таблица 1 в [2, стр. 129-135], где в 29-ти примерах с подробными комментариями собраны результаты теоретических исследований и компьютерных поисков в разные годы различных авторов, начнем со следующего примера в ключе *«ST-формулы любой множитель делают эффективным»*.

26°. *«Генератор строки 15 предложен Дж. Марсальи (G. Marsaglia)в качестве «кандидата на наилучший множитель», после компьютерных исследований для почти кубических решеток размерностью от 2 до 5. Это предложение было сделано, в частности, потому, что множитель можно легко запомнить (см. книгу под редакцией С. К. Зарембы [Applications of Number Theory to Numerical Analysis, edited by S. K. Zaremba (New York: Academic Press, 1972), 275]».*

Данный генератор $\langle X_n \left(a = 69069, N = 2^{32}\right)\rangle$ по критерию А имеет максимальным периодом число $N = 2^{32}$, поскольку единственный простой множитель в нем содержится и в $a - 1 = d \cdot 2^2 = 17267 \times 2^2$, причем d и N взаимно просты, и потому потенциал равен $\tau = \frac{32}{2} = 16$ (см. [2, стр. 45, Упр. 5]).

Для ориентации в обсуждаемом вопросе, сразу же определимся, что согласно теореме 2

$$\nu_s^2(a, N) \le a^2 + 1 = 4770526762, \tag{5.1}$$

для всех $s \ge 2$. Вместе с тем, данные строки 15 Таблицы 1, начиная с $s = 3$, намного меньше

$$\nu_3^2 = 2072544, \nu_4^2 = 52804, \nu_5^2 = 6990, \nu_6^2 = 242. \tag{5.2}$$

Применения ST-формул к множителю Дж. Марсальи $a = 69069$ приводят к следующим результатам.

При $s = 2$ Теорема 1 дает следующее точное равенство

$$\nu_2^2\left(a = 69069, N = (69068)^2 = 4770388624\right) = (a-2)^2 + 1 = (69067)^2 + 1 = 4770250489,$$

что на величину 527040633 больше значения $\nu_2^2 = 4243209856$ из Таблицы 1 [2, стр. 130-131], вычисленного для $N = 2^{32} = 4294967296$.

При всех $s, s > 2$ действует Теорема 7

$$\nu_s^2\left(a = 69069, N = (69068)^2 = 4770388624\right) \le \sum_{k=0}^{2}\left(\binom{2}{k}\right)^2 = 6.$$

Таким образом для множителя Марсальи получаем наилучше возможное значение ν_2^2 с максимальным периодом $N = 4770388624$.

Для сравнения возможностей ST-формул с данными (5.2), для $\tau = 6$ применим теоремы 5–6, которые при всех $s, 2 \le s \le 6$ приводят к следующим оценкам снизу

$$4767626304 \le v_s^2(69069; N = (69068)^6). \tag{5.3}$$

Тем самым, построен генератор случайных чисел $\langle X_n \left(69069; N = (69068)^6\right)\rangle_{n=0}^{(69068)^6-1}$ с множителем Марсалья, в котором с большим максимальным периодом $N = (69068)^6 \approx 2^{192}$ против $N = 2^{32}$ и одновременно большие, где-то с предельно большим (5.1), ν_s^2 при $s = 3, 4, 5, 6$ в (5.3) против (5.2), получается, как говорят, «Сплошной праздник!».

Разумеется, здесь не были использованы какие-то индивидуальные свойства множителя Марсальи, –ST-формулы к таким результатам приводят любое целое положительное число a.

27°. *«Похожий, но не менее выдающийся множитель* $16807 = 7^5$ *в строке 19 стал более часто использоватьсяа для этого модуля, после того как его предложили Левис, Гудман и Миллер (см. работу Lewis, Goodman, and Millerв IBM SystemsJ. 8 (1969), 136-146). Генератор с этим множителем является основным с 1971 года в популярной библиотеке программ IMSL. Основная причина продолжительного использования* $a = 16807$ *состоит в том, что* a^2 *меньше модуля* N, *поэтому операция* $ax \bmod N$ *может быть выполнена с высокой эффективностью на языках высокого уровня, использующих технику из упр. 3.2.1.1-9. Однако такие малые множители имеют известные дефекты. »*[2, стр. 131-133].

Применение теорем 1–7, при любом $m \ge 2$ (в частности, при $m = 2$ как рассматриваемом примере) $a - 1 = p_1^{r_1} \cdots p_t^{r_t}$ и $(a-1)^m < (a-1)^{m+t} = N\,(t \ge 1)$, например, при $a - 1 = 7^r, N = 7^{mr+t}\,(t \ge 1)$, обеспечат выполнение $a^m < N$, причем с произвольно большим a.

28°. Все 29 множителей из Таблицы 1 ([2, стр. 130-131]), как *«выдающиеся»*, *«эффективно применяемые»* и просто *«хорошие»*, так и *«утратившие популярность»* и *«достаточные для того, чтобы вызвать испуг в глазах и спазмы в желудке у многих ученых, специализирующиеся на компьютерах»*, все без исключения по ST-формулам могут порождать $\langle X_n\,(a, N)\rangle_{n=1}^{N}$ генераторы с предельно высокими ν_s-качествами.

При этом, сам вид

$$X_{n+1} = (X_n\,(a-1) + X_n + c) \bmod (a-1)^\tau\,(n = 1, ..., (a-1)^\tau - 1)$$

попадает под процитированное выше свойство *«избежать умножения, просто достаточно перемещения и суммирования»*.

29°. Поскольку в [2, стр. 130] рассматривались примеры 0 и N, не удовлетворяющих теореме А, это 1-ая строка Таблицы с $a - 1 = 22 = 2 \cdot 11$, в то время как $N = 10^8 + 1 = 100000001 = 2 \cdot \left(5 \cdot 10^7 + \frac{1}{2}\right) = 11 \times 909,181818182$, стало быть, такое N не является максимальным периодом для последовательности $\langle X_n\,(a, N)\rangle$, тем не менее, для них вычислены $\nu_2^2 = \nu_3^2 = \nu_4^2 = \nu_5^2 = 530$ и $\nu_6^2 = 447$.

В связи с чем, возникает вопрос, насколько корректно пользоваться показателем $\nu_s\,(a, N; (a-1)^\tau = N\lambda)$ качества случайности генератора $\{X_n\,(a, N, c, X_0)\}$ при 0 и N, не удовлетворяющим теореме А.

Здесь проблема в том, что формула (8) в [1, стр. 107-109], на основе которой дано определение (12), выведена при условии *«Мы предположили, что последовательность имеет максимальный период».*

Причем, только это предположение выводит на сравнение $m_1 + am_2 + \ldots + a^{s-1}m_s \equiv 0\,(\mathrm{mod}\,N)$, составляющего определение $\nu_s\,(a, N)$ (см. об этом также §2).

Вместе с тем, по-видимому, все такие генераторы случайных чисел выдвигались по каким-то, в каждом случае по своим, причинам.

Разумеется, теоремы 1–7 отдельно для $a = p_1^{r_1} \cdots p_t^{r_t}$, но со своим $N = (a-1)^\tau = p_1^{\tau r_1} \cdots p_t^{\tau r_t}$ и отдельно для $N = p_1^{\aleph_1} \cdots p_t^{\aleph_t}$ со своим $a = d \times p_1^{r_1} \cdots p_t^{r_t} + 1$ спотенциалом $\tau = \max\left\{\left\lceil \frac{\aleph_1}{r_1} \right\rceil, ..., \left\lceil \frac{\aleph_t}{r_t} \right\rceil\right\}$ (в условиях Упр. 5 из [2, стр. 45]), порождают хорошие генераторы,

но здесь речь о начальном совместном соотношении между a и N, не удовлетворяющих условиям Теоремы А.

30°. Как это отмечалось и использовалось в 21°, прохождение генератором случайных чисел спектрального тестирования обеспечивает выполнение для него критерия серий. Быть может будет небезынтересно изучение таких взаимоотношений с другими теоретическими и эмпирическими тестами (см. [1, стр. 52-105] и [2, стр. 62-116]).

31°. В [2, стр. 19-20] приведен ряд применений случайных чисел:

«Числа, которые выбираются случайным образом, находят множество полезных применений.

1. *Моделирование. При использовании компьютера для моделирования естественных явлений случайные числа нужны для того, чтобы сделать эти модели похожими на реальные явления. Моделирование применяется во многих областях, начиная от исследований в ядерной физике (где частицы испытывают случайные столкновения) и заканчивая исследованием операций (где люди прибывают, например, в аэропорт через случайные промежутки времени).*
2. *Выборочный метод. Часто невозможно исследовать все варианты, но случайная выборка обеспечивает понимание того, что можно назвать "типичным" поведением.*
3. *Численный анализ. Для решения сложных задач численного анализа была разработана остроумная техника, использующая случайные числа. Об этом написано несколько книг.*
4. *Компьютерное программирование. Случайные величины являются хорошим источником данных для тестирования эффективности компьютерных алгоритмов. Более важно то, что они играют решающую роль при использовании рандомизированных алгоритмов, которые часто намного превосходят своих детерминированных двойников. В этой серии книг нас, в первую очередь, интересует именно такое применение случайных чисел. Этим объясняется то, что случайные числа рассматриваются уже здесь, в главе 3, прежде чем появится большинство других компьютерных алгоритмов.*
5. *Принятие решений. Говорят, что многие администраторы принимают решения, бросая монету, игральную кость либо каким-нибудь другим подобным способом. Сплетничают, что некоторые профессора в колледжах ставят оценки, используя тот же метод. Иногда важно принять полностью "беспристрастное" решение. Случайность является также важной частью оптимальных стратегий в теории матричных игр.*
6. *Эстетика. Небольшая добавка случайности оживляет музыку и компьютерную графику. Например, рисунок в определенном смысле выглядит привлекательнее чем* [См. D. E. Knuth, Bull. Amer. Math. Soc. 1 (1979), 369.]
7. *Развлечения. Многие считают, что они замечательно проводят время, бросая игральную кость, тасуя колоду карт, вращая колесо рулетки и т. п. Такие традиционные способы использования случайных чисел получили название метод Монте-Карло. Это общее название всех алгоритмов, использующих случайные числа».*

Не исключено, что построенные в этой статье генераторы случайных чисел существенно расширят границы применений.

32°. В статье Пламстеда [14] (см. также [15, §3. 10]) предложен метод решения задачи полного восстановления Генератора Лехмера $X_{n+1} = (aX_n + c) \bmod N$ при определенном количестве последовательных известных членов, но не его модуля.

В контексте политики журнала [19] «Подготовка Казахстана к Четвертой промышленной революции и исполнение программы «Цифровой Казахстан»» данная статья выполнена, надеемся, в ключе *«Решение полное и окончательное известных респектабельных проблем»*.

В последующих номерах данного журнала предполагается продолжение такого же наполнения объявленной политики статьями по линиям *«Постановки новых задач с иллюстративными решениями»*, *«Новые методы исследования»*, *«Новые формулы прямого применения»*, *«Новые моменты в разработанных методах»* и по другим, по крайней

мере, вынесенным в [19] в виде фундаментальных и значимых результатов (разумеется, постановки задач, результаты, методы и формулы оттуда закрепляются за авторами и в каких-то дополнительных разъяснениях не нуждаются, речь идет о государственных интересах Казахстана в науке и образовании).

Список литературы

1 Кнут Д. Э. Искусство программирования для ЭВМ, том 2. Получисленные алгоритмы. – М.: Издательство «Мир», 1977. – 784 с. (Пер. с англ. Г. П. Бабенко, Э. Г. Белаги и Л. В. Майорова, под ред. К. И. Бабенко: Knuth D. The art of computer programming, Volume 2: Semi numerical Algorithms, Publisher: Addison-Wesley, 1969).

2 Кнут Д. Э. Искусство программирования, том 2. Получисленные алгоритмы. –М.: Издательскийдом «Вильямс», 2001. – 832 с. (Пер. с англ. под общей редакцией Ю. В. Козаченко: Knuth D. The art of computer programming, Volume 2: Seminumerical Algorithms, 3^{rd} Edition, Publisher: Addison-Wesley, 1998).

3 Ильин А. М., Данилин А. Р. Асимптотические методы в анализе, –М.: ФИЗМАТЛИТ, 2009, – 248 с.

4 Coveyou R.R., MacPherson R.D. Fourier Analysis of Uniform Random Number Generators, Journal of the ACM (JACM). –1967. –Vol. 14 Issue 1, Jan., –P. 100-119.

5 Коробов Н. М. Теоретико-числовые методы в приближенном анализе. –М.: Физматгиз. 1963.

6 Dung D., Temlyakov V., Ullrich T. Hyperbolic Cross Approximation. http://arxiv.org/abs/1601.03978.

7 Воронин С. М. , Темиргалиев Н. , О квадратурных формулах, связанных с дивизорами поля гауссовых чисел // Матем. заметки. –1989. –Т. 46. –№ 2. –С. 34-41

8 Темиргалиев Н. Применение теории дивизоров к численному интегрированию периодических функций многих переменных // Матем. сб. –1990. –Т.181. –№ 4. –С. 490-505

9 Темиргалиев Н., Баилов Е. А., ЖубанышеваА. Ж. Об общем алгоритме численного интегрирования периодических функций многих переменных // Докл. РАН. –2007. –Т. 416. –№ 2. –С. 169-173.

10 Жубанышева А.Ж., Темиргалиев Н., Темиргалиева Ж.Н., Применение теории дивизоров к построению таблиц оптимальных коэффициентов квадратурных формул // Ж. вычисл. матем. и матем. физ. – 2009. –Т. 49, –№ 1. –С. 14-25.

11 Баилов Е.А., Сихов М.Б., Темиргалиев Н. Об общем алгоритме численного интегрирования функций многих переменных // Ж. вычисл. матем. и матем. физ. –2014. –Т. 54. –№7. –С. 1059-1077.

12 Шерниязов К., Приближенное восстановление функций и решений уравнения теплопроводности с функциями распределения начальных температур из классов E, SW и B // Кандидатская диссертация по спец. 01.01.01 – Математический анализ. –Алматы, –1998.

13 Рудин У. Функциональный анализ. –М.: Издательство «Мир», –1975, –443 с.

14 Plumstead J., Inferring a sequence generated by a linear congruence// in 23^{rd} IEEE FOGS. –1982, –P. 153-159.

15 Земор Ж. , Курс криптографии. –М. -Ижевск: НИЦ «Регулярная и хаотическая динамика»; Институт компьютерных исследований, –2006. –256с.

16 Минеев М. П. , Чубариков В. Н. , Лекции по арифметическим вопросам криптографии. – М. : Издательство «Попечительский совет Механико-математического факультета МГУ им. М. В. Ломоносова», 2010. – 186 с.

17 Колмогоров А. Н. Избранные труды: в 6 т. /Т. 3: Теория информации и теория алгоритмов. –2005. –263 с.

18 Рот К. Ограничения для регулярности // Математика: границы и перспективы, –М.: ФАЗИС, 2005. – С. 375-394.

19 Темиргалиев Н. Предисловие Главного редактора журнала «Вестник Евразийского национального университета имени Л. Н. Гумилева. Серия Математика. Информатика. Механика» о целях издания и путях их реализации// Вестник Евразийского национального университета имени Л. Н. Гумилева. Серия Математика. Информатика. Механика. –2018. –Т. 122. –№1. –С. 8-67.

Н. Темірғалиев
Теориялық математика және ғылыми есептеулер институты
Л.Н. Гумилев атындағы Еуразия ұлттық университеті, Астана, Қазақстан

Ковэю мен Макферсонның спектралды тесті кездейсоқтық талаптарын қандай мөлшерде қанағаттандырса, сондай дәрежеде кездейсоқ болатын Лехмердің сызықты конгруэнтті тізбегінің элементарлы құрылуы

Аннотация: Бір қарағанда өз-өзінен түсінікті болып көрінетін кездейсоқ сан мен кездейсоқ тізбек ұғымдарының – не қиындығы бар, бірі бірінен кейін ойға келген сандарды тізіп жаза берсе болмай ма – дәл есептелінетін анықтамалары берілмей келеді. Осы жағдайда іс-жүзінде әртүрлі кездейсоқ сандарды қатын ережелер – Генераторлар ұсынылады да, соларды кездейсоқтыққа тексеретін (тестілейтін) әдістер жасалады. Мұндай «емтиханнан» өткен тізбектер *кездейсоқ тізбек* деп, ал оның әрбір мүшесі *кездейсоқ сан* деп жарияланады, нәтижесінде қаншама тексеру тесті бар болса, соншама кездейсоқтық түрі бар болып шығады.

Мақалада қойылымы және оның зерттеу тарихы Компьютерлік ғылымдарының жоғары сатыларынан табылатын десе де болатын мәселе зерттеліп, ғылыми тақырып ретінде толығымен жабылған. Бұл қойылымда қарастырылатын ең танымалыларының бірі, тіпті ең танымаласы да болуы мүмкін - 1949 жылғы *Лехмер генераторы* және *«қолданыстағы тестілердің ең нәтижелісі»* болып табылатын 1965 жылы берілген *Ковею мен Макферсонның спектралдық тесті.* Осылардың өзара байланыста 1969 жылдан бастап бүгінгі күнге дейін толықтырылып отырылған зерттеу жолы Дональд Эрвин Кнуттың «*Программалау өнері*» атты монографиясының барлық басылымдарында кеңінен ашылған. Демек, бұл тақырып әрдайым ізденіс үстінде болып келеді.

Міне, 50 жылдық тарихы бар уақыт өлшемінде үнемі жетілу жолында болып келсе және де осы уақытқа дейінгі белгілі жетістік, ν_s кездейсотықтың негізгі сандық сипаттамасына жасалған айтарлықтай мәлімет бермейтін біржақты жоғарыдан бағалауы ғана. Мақалада пессимистік « $s \geq 10$ *болғанда* ν_s *дәлдігін есептеу өте қиын*» деген болжамға қарамастан күтілмеген асимптотикалық теңдік алынған. Бұл мәселенің дұрыс қойылымы мен оның әрі қарай зерттеуді қажет етпейтін шешімін құрайды.

Максималды периодты *Лехмердің кездейсоқ сандарының генераторы* немесе *сызықтық конгруэнтті тізбек* деп бүтін теріс емес $\langle X_n \rangle$ сандардың

$$X_{n+1} = (aX_n + c) \bmod N, n \geq 0, \tag{0.1}$$

рекуррентті тізбегі аталады. Мұндағы

$$N - \textit{модуль}\, 0 < N, a - \textit{көбейткіш}\, 0 \leq a < N,$$
$$c - \textit{өсімше}\, 0 \leq A < N,\, X_0 - \textit{бастапқы мән}\, 0 \leq X_0 < N.$$

Және де (0.1) рекуррентті тізбегіне оны *максималды периодты* ететін келесі шартар қойылады:
$a > 1$, $N > a$, $\tau(a, N) \geq 2$ және $1 \leq \lambda(a, N) \equiv \frac{(a-1)^{\tau(a,N)}}{N} < (a-1)^{\tau(a,N)-1})$ бүтін сандары $(a-1)^{\tau(a,N)} \equiv 0 \,(\mathrm{mod} N)$ және $(a-1)^{\tau(a,N)-1} \not\equiv 0 \,\,(\mathrm{mod} N)$ салыстыруларымен өзара байланысқан.

Әдеттегідей, бұл жағдайда да, мәселе толығымен дәл қойылған математикалық есепке келтіріледі (барлық түсіндірмелер мен талқылаулар мақала мәтінінде келтірілген): берілген $s \geq 2$ және $\tau \geq 2$ сандары мен өспелі N үшін (барлық параметрлер – оң бүтін сандар)

$$\nu_s(a,\, N) = \inf\left\{\sqrt{m_1^2 + ... + m_s^2} : m = (m_1, ..., m_s) \in Z^s, m \neq 0,\, \sum_{j=0}^{s} m_j a^{j-1} \equiv 0 \,(\mathrm{mod} N)\right\}$$

болғандағы

$$\sup\left\{\nu_s(a, N) : 2 \leq a < N, (a-1)^{\tau} \equiv 0(\mathrm{mod} N), (a-1)^{\tau-1} \not\equiv 0(\mathrm{mod} N)\right\} \tag{0.2}$$

шамасының асимтотикасын табу.

Сонымен, мәселе барлық a, N және s үшін $\nu_s(a, N) \leq \gamma(s) N^{\frac{1}{s}}$ теңсіздігі-ақ белгілі болғанда, $\nu_s(a, N)$ шамасының мәні неғұрлым үлкен болатындай $a = a(N)$ санын табу болып табылады. Әрине, кез келген жоғарғы баға сияқты бұл да аса көтеріңкі болуы мүмкін, сол себепті мәселені шешпейді.

Осы жұмыста барлық мүмкіндерді қамтып, сондықтан да зерттелудегі мәселенің толық шешімімен қамтамасыз ететін s, τ және λ параметрлерінің қатынастарына тәуелді асимптотикалық сипаттағы спектралді тестілеу (ST) бойынша жаңа және оны толығымен жабатын нәтижелер алынды:

$$\mathbf{ST} : \nu_2\left(a, N; (a-1)^2 = N\right) = (a-1)\sqrt{1 - 2\frac{a-2}{(a-1)^2}} = \sqrt{N}\sqrt{1 - 2\frac{\sqrt{N}-1}{N}},$$
$$\mathbf{ST}\,(2 \leq s = \tau) : N^{\frac{1}{s}}\left(1 - (b_s - 1)\, N^{-\frac{1}{s}}\right) = a - b_s \leq \nu_s(a, N; (a-1)^s = N) \leq$$
$$\leq \sqrt{a^2+1} = N^{\frac{1}{s}}\sqrt{1 + 2N^{-\frac{1}{s}} + 2N^{-\frac{2}{s}}},$$
$$\mathbf{ST}\,(2 \leq s < \tau, \lambda \geq 1) : (N\lambda)^{\frac{1}{\tau}}\left(1 - (b_s - 1)\,(N\lambda)^{-\frac{1}{\tau}}\right) = (a - b_\tau) \leq$$
$$\leq \nu_s\left(a, N; (a-1)^{\tau} = N\lambda, 1 \leq \lambda \leq (a-1)^{\tau-s}\right) \leq \sqrt{a^2+1} = (N\lambda)^{\frac{1}{\tau}}\sqrt{1 + 2\,(N\lambda)^{-\frac{1}{\tau}} + 2\,(N\lambda)^{-\frac{2}{\tau}}},$$
$$\mathbf{ST}\,(s > \tau \geq 2, \lambda \geq 1) : \nu_s(a, N; (a-1)^{\tau} = N\lambda, \lambda \geq 1) \leq \sqrt{\sum_{k=0}^{\tau}\left(\binom{\tau}{k}\right)^2},$$

мұндағы $(-b_m)$ *оң бүтін саны* a *-ның дәреже*лері бойынша жіктелген $(a-1)^m$ *көпмүшелігінің теріс мәнді биноминалдық коэффициенттерінің абсолютті шамаларының ең үлкені:* $b_2 = 2, b_3 = 3, b_4 = 4, b_5 = 10, b_6 = 20, b_7 = 35$, $b_8 = 56, b_9 = 126, b_{10} = 252, b_{11} = 462, b_{12} = 792, b_{13} = 1716, b_{14} = 3432, b_{15} = 6435$ *және т.с.с.*

Д. Кнуттың «Программалау өнері» атты монографиясындағы осы тақырып бойынша берілген барлық құрылымдар жартылай эмпирикалық сипатта – онда теориялық қағидалар ұсынылады да, соның негізінде статистикалық эксперименттер жүргізіледі. Сонымен қатар, Д.Кнут кездейсоқ тізбек құрудың фон Нейманның *«орта квадраттар»* әдісіндегі параметрлерді кездейсоқ түрде таңдаудың күмән тудыратын көрінісіне сүйеніп, күллі эксперименттік іздеулердің сенімді емес екендігін және кандай да болсын теория әрдайым қажет екендігі туралы қорытындыға келген.

Біз таза теориялық зерттеулер жүргіздік.

Барлық ST-тұжырымдарында төменгі бағалаулары N өскен сайын 1 санына ұмтылатын айқын түрде (практикалық қолданыста шешуші мағынаға ие) жазылатын $\overline{\gamma_N}$ көбейткіші үшін $\overline{\gamma_N}\cdot N^{\frac{1}{s}} \le \nu_s(a,N)$ түрінде болады.

Бұл қатарымен екі мәселені шешеді (жалғыз ғана кедергі - компьютерлік техниканың есептеу мүмкіндіктері)

a) кездейсоқ сандардың саны N таңдауымызша үлкен болуы міндетті және мүмкін де;
b) кездейсоқтықтың негізгі сипаттамасы $\nu_s(a,N)$ барлық $s \ge 2$ үшін қалауымызша үлкен болуы міндетті және мүмкін.

$\langle X_n\rangle$ генераторының s өлшемді ν_s дәлдігінің *«өлшем қарғысы»* ретінде белгілі $N^{\frac{1}{s}}$ негізгі бөлігі $1/s$ көрсеткішінің кішілігіне байланысты N-нен оған кері s -ке сай N^s дәрежесі үлкен болуын талап етеді (осымен сандық интегралдаудағы бірқалыпты торлы және бірдей салмақты квадратуралық формулаларымен жуықтау жылдамдығының шамасы қайталанылады).

Бұның бәрінен жаңа мәселе туындайды: (0.1)-(0.2) кездейсоқ сандар генераторы қолданылатын әр жағдай үшін *« N және $\nu_s(a,N)$ қаншалықты үлкен болуы керектігін анықтау қажет»*. Әрине, бұл тіпті тривиалды болмауы да мүмкін, өз алдына жеке мәселе.

$\nu_s(a,N) \le \overline{\overline{\gamma_N}}\cdot N^{\frac{1}{s}}$ $\left(\overline{\overline{\gamma_N}} \to 1\right)$ түріндегі асимптотикалық дәл жоғарғы баға N мен $\nu_s(a,N)$ шамаларын жүзеге асыру кезінде орасан артық жұмыстарды қоса алып жүретін қисынсыз үлкен етіп алмауға кепіл болады.

$s=2$ жағдайынан басқа барлық ST- тұжырымдар дәл емес, асимптотикалық қана. Бірақ бұл жәйт қолданысты еш шектемейді - N мен $\nu_s(a,N)$-тің дәл мәндері емес, қажетті шекарадан шықпайтын жуық мәндері қажет етіледі.

Егер кездейсоқтық әсері тікелей сезілмейтін $\nu_s(a,N)$-тің бағасынан кездейсоқтықты «жиілік» арқылы тексеруге көшсек (бұл қасиет *бірқалыпты таралым* деп аталады, кездейсоқтықтан әлде көп шарттар талап етіледі), $0,1,\ldots,N-1$ сандарын $[0,1]$ сегментінен алынған кез келген $[\alpha,\beta]$ сегменті үшін онда жататын $\frac{X_n}{N}$ сандарының саны $(\beta-\alpha)$-ға жуық болатындай етіп, өз-өзіне биективті бейнелеу арқылы басқа $X_0,\ldots,X_{N-1}$ ретімен берілуі қажет болады, яғни кез келген максимал периодты Лехмер тізбегінің әуел басынан-ақ $\frac{1}{N}$ жақсартылмайтын ауытқу ретімен бірқалыпты таралатындығы аңғарылады. Бұл қасиетті осы тізбектің тамаша қасиеттерінің біріне жатқызуға болады. Сөйтіп, мәселенің тек $\nu_s(a,N)$ кездейсоқтық көрсеткішінде болатындығы туралы қорытындыға келеміз.

Түйін сөздер: Кездейсоқ сандар генераторы, Ковэю және Макферсон спектралды тесті, максималды период, сызықты конгруэнтті тізбек, асимптотикалық теңдік, кездейсоқ сандар генераторының көпөлшемді дәлдігі.

N. Temirgaliyev

Institute of Theoretical Mathematics and Scientific Computations
L.N. Gumilyov Eurasian National University, Astana, Kazakhstan

Elementary construction of the linear congruent Lehmer sequence with the degree of randomness that is required by the spectral test of Coveyou and MacPherson

Abstract: The ideas of a random number and a random sequence can not be completely formalized. Instead, for whatever reason, arrays of random number generators are proposed, they are used to create methods for testing them for randomness. Sequences that pass such an examination are declared random, and each of its elements is a random number, as a result there are various types of randomness, as many many tests.

The article is devoted to the complete solution of the posed problems, objects and a long, respectable history of research with instructive conclusions, in the aggregate, we hope, in the higher echelons of Computer Sciences: Lehmer's Generator (1949) is one of the most popular if not the most popular sensor and the spectral test of 1965 by Coveyou and MacPherson as *"the most perfect test available"*, both in conjunction with the 50-year history, in the development detailed in all editions of the monograph *"The Art of Programming"* by Donald Erwin Knuth from 1969 to the present, has become being in constant development. Namely, a little that clarifies the one-sided estimate from above of the main numerical characteristic of randomness ν_s with a pessimistic forecast *"it would be very difficult to calculate the accuracy* ν_s *, when* $s \ge 10$ *"* is replaced by an unexpected asymptotic for all $s \ge 2$ - what the problem consisted in ideally, and this is its solution.

The generator of random numbers of Lehmer or the *Linear congruential sequence* of the maximal period is, by definition, the recurrence sequence $\langle X_n\rangle$ of nonnegative integers

$$X_{n+1} = (aX_n + c) \bmod N, n \ge 0, \tag{0.1}$$

where

$$N - module\, 0 < N, a - multiplier\, 0 \le a < N,$$
$$c - increment\, 0 \le A < N,\ X_0 - initialvalue\ 0 \le X_0 < N,$$

whole numbers $a > 1, N > a, \tau(a,N) \ge 2$ and $1 \le \lambda(a,N) \equiv \frac{(a-1)^{\tau(a,N)}}{N} < (a-1)^{\tau(a,N)-1}$ are related by comparisons $(a-1)^{\tau(a,N)} \equiv 0 \,(\mathrm{mod} N)$ and $(a-1)^{\tau(a,N)-1} \not\equiv 0 \ (\mathrm{mod} N)$.

As it often occurs, in this case too, the whole problem is reduced to a clearly formulated mathematical problem (all motivations and details are given in the text of the article): for given $s \ge 2$ and $\tau \ge 2$ and increasing N find the asymptotic value (all parameters are positive integers)

$$\sup\left\{\nu_s(a,N) : 2 \le a < N, (a-1)^{\tau} \equiv 0(\mathrm{mod} N), (a-1)^{\tau-1} \not\equiv 0(\mathrm{mod} N)\right\}, \tag{0.2}$$

where

$$\nu_s(a,N)=\inf\left\{\sqrt{m_1^2+\cdots+m_s^2}:m=(m_1,...,m_s)\in Z^s,m\neq 0,\sum_{j=1}^{s}m_ja^{j-1}\equiv 0\,(\mathrm{mod}N)\right\}.$$

Thus, the problem consists in indicating the number $a=a(N)$ with as large a value as possible $\nu_s(a,N)$, while for all the a,N and s only ones we know only the inequalities $\nu_s(a,N)\leq\gamma(s)N^{\frac{1}{s}}$. As with any upper bound, this inequality can be greatly overestimated, so the problem has no solution.

In this paper, new and final results are obtained on spectral testing (ST), which are asymptotic in nature, depending on all possibilities and, therefore, providing a complete solution of the problem under study, the relations between the parameters s, τ and λ:

$$\mathbf{ST}:\nu_2\left(a,N;(a-1)^2=N\right)=(a-1)\sqrt{1-2\frac{a-2}{(a-1)^2}}=\sqrt{N}\sqrt{1-2\frac{\sqrt{N}-1}{N}},$$

$$\mathbf{ST}\,(2\leq s=\tau):N^{\frac{1}{s}}\left(1-(b_s-1)N^{-\frac{1}{s}}\right)=a-b_s\leq\nu_s\left(a,N;(a-1)^s=N\right)\leq$$

$$\leq\sqrt{a^2+1}=N^{\frac{1}{s}}\sqrt{1+2N^{-\frac{1}{s}}+2N^{-\frac{2}{s}}},$$

$$\mathbf{ST}\,(2\leq s<\tau,\lambda\geq 1):(N\lambda)^{\frac{1}{\tau}}\left(1-(b_s-1)(N\lambda)^{-\frac{1}{\tau}}\right)=(a-b_\tau)\leq$$

$$\leq\nu_s\left(a,N;(a-1)^\tau=N\lambda,1\leq\lambda\leq(a-1)^{\tau-s}\right)\leq\sqrt{a^2+1}=$$

$$=(N\lambda)^{\frac{1}{\tau}}\sqrt{1+2(N\lambda)^{-\frac{1}{\tau}}+2(N\lambda)^{-\frac{2}{\tau}}},$$

$$\mathbf{ST}\,(s>\tau\geq 2,\lambda\geq 1):\nu_s\left(a,N;(a-1)^\tau=N\lambda,\lambda\geq 1\right)\leq\sqrt{\sum_{k=0}^{\tau}\left(\binom{\tau}{k}\right)^2},$$

where $(-b_m)$ *is the largest modulo negative binomial coefficient in the expansion of* $(a-1)^m$ *in powers of* $a:b_2=2,b_3=3$, $b_4=4,b_5=10,b_6=20,b_7=35,b_8=56,b_9=126,b_{10}=252,b_{11}=462,b_{12}=792,b_{13}=1716,b_{14}=3432,b_{15}=6435,...$ *etc.*

All the constructions on this subject in D. Knuth's monograph "The Art of Programming" are semi-empirical in nature - theoretical positions are put forward on the basis of which statistical experiments are conducted. In addition, D. Knuth, using the example of seemingly undoubtedly random selection of parameters in the *"mid-squares"* method, von Neumann, comes to the conclusion that purely experimental searches are unreliable and that some kind of theory is always needed.

We conducted a purely theoretical study.

As follows from the lower bounds in all ST-statements, all of them with an accuracy tending to 1 with increasing N explicitly written out (which is crucial in practical applications) of the factor $\overline{\gamma_N}$ have the form $\overline{\gamma_N}\cdot N^{\frac{1}{s}}\leq\nu_s(a,N)$.

This means that simultaneously solved two problems (with a single limitation - the computing capabilities of computer technology)

a) *The number of random numbers* N *must and can be arbitrarily large,*

b) *The basic characteristic of the randomness of* $\nu_s(a,N)$ *must and can be so large as ever for all* $s\geq 2$.

In this case, the main part $N^{\frac{1}{s}}$ of the s-dimensional accuracy of the generator $\langle X_n\rangle$ due to the small exponent $1/s$, known as the *"curse of dimension",* requires N in its inverse to s to be large (this repeats the velocity from a uniform grid in numerical integration).

A new problem arises: *"In each concrete case of using the random number generator (0.1)–(0.2) find out how big* N *and* $\nu_s(a,N)$ *should be?".* Of course, this is a separate problem, perhaps even non-trivial.

The asymptotically exact upper bounds $\nu_s(a,N)\leq\overline{\overline{\gamma_N}}\cdot N^{\frac{1}{s}}\left(\overline{\overline{\gamma_N}}\to 1\right)$ act as guarantors not to take N and $\nu_s(a,N)$ unjustifiably large with accompanying high implementation costs.

With the exception of the case $s=2$, all the ST-statements are not exact, but asymptotic, which does not restrict applications in any way-it does not require exact values of N and $\nu_s(a,N)$ but only approximate boundaries in the contexts required by the context.

If we pass from the intangible estimate of $\nu_s(a,N)$ directly to the randomness check through the *"frequency"* (this property is also called *the uniform distribution*, from randomness it takes a lot more), where the difficulty, even the extra difficulty of the posed problem, in which the numbers $0,1,...,N-1$ must be rearranged in another order $X_0,\ldots,X_{N-1}$ as a bijective map onto itself in such a way that for any segment $[\alpha,\beta]$ of $[0,1]$ the number of $\frac{X_n}{N}$ numbers $[\alpha,\beta]$ should be close $(\beta-\alpha)$, then it is appeared that any Lehmer sequence with maximal period initially uniformly distributed with unimprovable rate of deviation $\frac{1}{N}$, which can be attributed for remarkable property. Thereby, the problem is connected whith indicator of randomness of $\nu_s(a,N)$.

Keywords: Lechmer random number generator, spectral test of Coveyou and MacPherson, linear congruent sequence, maximal period, asymptotic equality, multidimensional accuracy of random number generator.

References

1 Knuth D. Iskusstvo programmirovaniya dlya EHVM. Poluchislennye algoritmy. 2nd vol.(Izdatel'stvo "'Mir"', Moscow, 1977, 784 p) [in Russian] (Translated from english G.P. Babenko, E.G. Belagi, L.V. Maiorov, In edition K.I. Babenko: Knuth D. The art of computer programming, Volume 2: Semi numerical Algorithms, Publisher: Addison-Wesley, 1969).

2 Knuth D. Iskusstvo programmirovaniya dlya EHVM. Poluchislennye algoritmy. 3rd vol.(Izdatel'skij dom "'Vil'yams"', Moscow, 2001, 832 p.) [in Russian] (Translated in edition YU.V. Kozachenko: Knuth D. The art of computer programming, Volume 2: Seminumerical Algorithms, 3^{rd} Edition, Publisher: Addison-Wesley, 1998).
3 Ilin A.M., Danilin A.M. Asimptoticheskie metody v analize [Asymptotic methods in analysis] (FIZMATLIT, Moscow, 2009, 248 p.). [in Russian]
4 Coveyou R.R., MacPherson R.D. Fourier Analysis of Uniform Random Number Generators, Journal of the ACM (JACM), **14**(1), 100-119 (1967).
5 Korobov N.M. Teoretiko-chislovye metody v priblizhennom analize[Theoretic-Numerical Methods in Approximate Analysis] (Fizmatgiz, Moscow, 1963) [in Russian].
6 Dung D., Temlyakov V., Ullrich T. Hyperbolic Cross Approximation. http://arxiv.org/abs/1601.03978.
7 Voronin S.M., Temirgaliev N. Quadrature formulas associated with divisors of the field of Gaussian numbers, Mat. zametki, **46**(2), 597-602 (1989).
8 Temirgaliev N. Application of divisor theory to the numerical integration of periodic functions of several variables, Matem. sbornik, **69**(2), 527-542 (1990).
9 Temirgaliev N., Bailov E. A., Zhubanysheva A. Zh. General algorithm for the numerical integration of Periodic function of several variables, Dockland Mathematics, 681-685 (2007).
10 Zhubanysheva A. Zh., Temirgaliev N., Temirgalieva Zh. N. Application of divisor theory to the construction of tables of optimal coefficients for quadrature formulas, Computational mathematics and mathematical physics, **49**(1), 12-22(2009).
11 Bailov E.A., Sikhov M.B., Temirgaliev N. General Algorithm for the Numerical Integration of Functions of Several Variables, Computational Mathematics and Mathematical Physics, **54**(7), 1061–1078(2014).
12 Sherniyazov K. Approximate Reconstruction of Functions and Solutions of the Heat Equation with Distribution Functions of Initial Temperatures in the Classes E, SW, and B, Candidate's Dissertation in Mathematics and Physics (Almaty, 1998).
13 Rudin U. Funkcional'nyj analiz [Functional analysis](Izdatel'stvo "'Mir"', Moscow, 1975, 443 p.).
14 Plumstead J. Inferring a sequence generated by a linear congruence in 23^{rd} IEEE FOGS. 1982, P. 153-159.
15 Zemor Zh. Kurs kriptografii [Cryptography course] (NIC "Regulyarnaya i haoticheskaya dinamika", institut komp'yuternyh issledovanij, Izhevsk, 2006, 256 p.).
16 Mineev M.P., Chubarikov V.N. Lectures on arithmetic questions of cryptography [Lekcii po arifmeticheskim voprosam kriptografii] (Publishing house "Board of Trustees of the Faculty of Mechanics and Mathematics of Moscow State University named after MV Lomonosov", Moscow, 2010, 186).
17 Kolmogorov A.N. Izbrannye trudy [Selected Works]: in 6 vol. /Vol. 3: Teoriya informacii i teoriya algoritmov[Information Theory and Theory of Algorithms]. –2005. –263 c.
18 Roth K.F., Ogranicheniya dlya regulyarnosti // Matematika: granitsy i perspektivy, (FAZIS, Moscow, 2005, P. 375–394) [in Russian](Translated from english: Roth K.F. On irregularities of distribution. Mathematika 1, 1954. P. 73-79)
19 Temirgaliyev N. Introdaction of the Editor-in-chief of the journal "The Bulletin of the L.N. Gumilyov Eurasian National University. Mathematics. Computer Science. Mechanics series" about the issue purposes and the ways of its implementation, Bulletin of the L.N. Gumilyov Eurasian National University. Mathematics. Computer Science. Mechanics series, **122**(1), 8-67 (2018).

Сведения об авторах:

Темиргалиев Н. - Директор Института теоретической математики и научных вычислений, Евразийский национальный университет им. Л. Н. Гумилева, ул. Сатпаева, 2, Астана, Казахстан.

Temirgaliyev N. - Director of the Institute of Theoretical Mathematics and Scientific Computations, L. N. Gumilyov Eurasian National University, 2 Satpayev str., Astana, Kazakhstan, e-mail.

Поступила в редакцию 19.05.2018

«Л.Н. Гумилев атындағы Еуразия ұлттық университетінің хабаршысы. Математика. Информатика. Механика сериясы» журналына жіберілетін жұмыстарға қойылатын талаптар

Журнал редакциясы авторларға осы нұсқаулықпен толық танысып, журналға мақала әзірлеу мен дайын мақаланы журналға жіберу кезінде басшылыққа алуды ұсынады. Бұл нұсқаулық талаптарының орындалмауы сіздің мақалаңыздың жариялануын кідіртеді.

1. Автордың қолжазбаны редакцияға жіберуі мақала авторының басып шығарушы, Л.Н. Гумилев атындағы Еуразия ұлттық университетіне мақаласын басуға келісімін және кез келген шетел тіліне аударылып қайта басылуына келісімін білдіреді.

2. Баспаға (барлық жариялаушы авторлардың қол қойылған қағаз нұсқасы және электронды нұсқасында) журналдың түпнұсқалы стильдік файлының міндетті қолданысымен LaTeX баспа жүйесінде дайындалған Tex-пен Pdf-файлындағы жұмыстар ұсынылады. Стильдік файлды ***bulmathmc.enu.kz*** журнал сайтынан жүктеп алуға болады.

3. Мақаланың көлемі 6 беттен кем және 18 беттен артық болмауы тиіс. Талап деңгейінен асқан жұмыстар редакциялық алқа отырысында қаралып, баспаға ерекше жағдайда ғана рұқсат етіледі.

4. Жұмыстың мәтіні ХҒТАР (Халықаралық ғылыми-техникалық ақпарат рубрикаторы) кодының көрсеткішімен басталып, кейін автор(лар)дың аты және тегі, жұмыс орнының толық атауы, қаласы, мемлекеті, E-mail-ы, мақаланың толық атауы, аннотациясы көрсетіледі. Аннотация 150-200 сөз көлемінде болуы тиіс, сонымен қатар мәтінде күрделі есептік формулалар болмауы, мақаланың толық аты қайталанбауы, жұмыстың мәтіні мен әдебиеттер тізімінде көрсетілетін сілтемелер болмауы керек. Аннотация мақаланың ерекшеліктерін көрсететін және оның құрылымын (кіріспе, есептің қойылымы, мақсаты, тарихы, зерттеу әдістері, нәтижелер және олардың талқылаулары, қорытынды) сақтайтын мақаланың қысқаша мазмұны болуы тиіс.

5. Жұмыстың мәтінінде кездесетін таблицалар мәтіннің ішінде жеке нөмірленіп, мәтін көлемінде сілтемелер түрінде көрсетілуі керек. Суреттер мен графиктер PS, PDF, TIFF, GIF, JPEG, BMP, PCX форматындағы стандарттарға сай болуы керек. Нүктелік суреттер кеңейтілімі 600 dpi кем болмауы қажет. Суреттердің барлығы да айқын әрі нақты болуы керек.

6. Жұмыста қолданылған әдебиеттер тек жұмыста сілтеме жасалған түпнұсқалық көрсеткішке сай (сілтеме беру тәртібінде немесе ағылшын әліпбиі тәртібі негізінде толтырылады) болуы керек. Баспадан шықпаған жұмыстарға сілтеме жасауға тиым салынады.

Сілтемені беруде автор қолданған әдебиеттің бетінің нөмірін көрсетпей, келесі нұсқаға сүйеніңіз дұрыс: тараудың номері, бөлімнің номері, тармақтың номері, теораманың номері (лемма, ескерту, формуланың және т.б.) номері көрсетіледі. Мысалы: «... қараңыз . [3; § 7, лемма 6]», «...қараңыз [2; 5 теорамадағы ескерту]». Бұл талап орындалмаған жағдайда мақаланы ағылшын тіліне аударғанда сілтемелерде қателіктер туындауы мүмкін.

Қолданылаған әдебиеттер тізімін рәсімдеу мысалдары

1 Воронин С. М., Карацуба А. А. Дзета-функция Римана. –М: Физматлит, –1994, –376 стр. – **кітап**

2 Баилов Е. А., Сихов М. Б., Темиргалиев Н. Об общем алгоритме численного интегрирования функций многих переменных // Журнал вычислительной математики и математической физики –2014. –Т.54. № 7. –С. 1059-1077. - **мақала**

3 Жубанышева А.Ж., Абикенова Ш. О нормах производных функций с нулевыми значениями заданного набора линейных функционалов и их применения к поперечниковым задачам // Функциональные пространства и теория приближения функций: Тезисы докладов Международной конференции, посвященной 110-летию со дня рождения академика С.М.Никольского, Москва, Россия, 2015. – Москва, 2015. –С.141-142. – **конференция еңбектері**

4 Нуртазина К. Рыцарь математики и информатики. –Астана: Каз.правда, 2017. 19 апреля. –С.7. – **газеттік мақала**

5 Кыров В.А., Михайличенко Г.Г. Аналитический метод вложения симплектической геометрии // Сибирские электронные математические известия –2017. –Т.14. –С.657-672. doi: 10.17377/semi.2017.14.057. – URL: http://semr.math.nsc.ru/v14/p657-672.pdf. (дата обращения: 08.01.2017). - **электронды журнал**

7. Әдебиеттер тізімінен соң автор өзінің библиографикалық мәліметтерін орыс және ағылшын тілінде (егер мақала қазақ тілінде орындалса), қазақ және ағылшын тілінде (егер мақала орыс тілінде орындалса), орыс және қазақ тілінде (егер мақала ағылшын тілінде орындалса) жазу қажет. Соңынан транслиттік аударма мен ағылшын тілінде берілген әдебиеттер тізімінен соң әр автордың жеке мәліметтері (қазақ, орыс, ағылшын тілдерінде – ғылыми атағы, қызметтік мекенжайы, телефоны, e-mail-ы) беріледі.

8. *Редакцияның мекенжайы*: 010008, Қазақстан, Астана қаласы, Қ.Сәтпаев көшесі, 2, Л.Н. Гумилев атындағы Еуразия ұлттық университеті, Бас ғимарат, 408-кабинет. Телефоны: (7172) 709-500 (ішкі 31-428). E-mail: *vest_ math@enu.kz*. Сайт: *bulmathmc.enu.kz*.

Provision on articles submitted to the journal
"Bulletin of L.N. Gumilyov Eurasian National University. Mathematics. Computer Science. Mechanics Series"

The journal editorial board asks the authors to read the rules and adhere to them when preparing the articles, sent to the journal. Deviation from the established rules delays the publication of the article.

1. Submission of articles to the scientific publication office means the authors' consent to the right of the Publisher, L.N. Gumilyov Eurasian National University, to publish articles in the journal and the re-publication of it in any foreign language.

2. The scientific publication office accepts the article (in electronic and printed, signed by the author) in Tex- and Pdf-files, prepared in the LaTeX publishing system with mandatory use of the original style log file. The style log file can be downloaded from the journal website ***bulmathmc.enu.kz***.

3. The volume of the article should not exceed 18 pages(from 6 pages). The article, exceeding this volume is accepted for publication in exceptional cases by a special decision of the journal Editorial Board.

4. The text of the article begins with the IRSTI (International Rubricator of Scientific and Technical Information), then followed by the Initials and Surname of the author (s); full name of organization, city, country; E-mail of the author (s); the article title; abstract. Abstract should consist of 150-250 words, it should not contain cumbersome formulas, the content should not repeat the article title, abstract should not contain references to the text of the article and the list of literature), abstract should be a brief summary of the article content, reflecting its features and preserving the article structure - introduction, problem statement, goals, history, research methods, results with its discussion, conclusion.

5. Tables are included directly in the text of the article; it must be numbered and accompanied by a reference to them in the text of the article. Figures, graphics should be presented in one of the standard formats: PS, PDF, TIFF, GIF, JPEG, BMP, PCX. Bitmaps should be presented with a resolution of 600 dpi. All details must be clearly shown in the figures.

6. The list of literature should contain only those sources (numbered in the order of quoting or in the order of the English alphabet), which are referenced in the text of the article. References to unpublished issues, the results of which are used in evidence, are not allowed. Authors are recommended to exclude the reference to pages when referring to the links and guided by the following template: chapter number, section number, paragraph number, theorem number (lemmas, statements, remarks to the theorem, etc.), number of the formula. For example, "..., see [3, § 7, Lemma 6]"; "..., see [2], a remark to Theorem 5". Otherwise, incorrect references may appear when preparing an English version of the article.

Template

1 Воронин С. М., Карацуба А. А. Дзета-функция Римана. -М: Физматлит, -1994, -376 стр.-**book**

2 Баилов Е. А., Сихов М. Б., Темиргалиев Н. Об общем алгоритме численного интегрирования функций многих переменных // Журнал вычислительной математики и математической физики -2014. -Т.54. № 7. -С. 1059-1077. - **journal article**

3 Жубанышева А.Ж., Абикенова Ш. О нормах производных функций с нулевыми значениями заданного набора линейных функционалов и их применения к поперечниковым задачам // Функциональные пространства и теория приближения функций: Тезисы докладов Международной конференции, посвященная 110-летию со дня рождения академика С.М.Никольского, Москва, Россия, 2015. - Москва, 2015. -С.141-142. - - **Conferences proceedings**

4 Нуртазина К. Рыцарь математики и информатики. -Астана: Каз.правда, 2017. 19 апреля. -С.7. **newspaper articles**

5 Кыров В.А., Михайличенко Г.Г. Аналитический метод вложения симплектической геометрии // Сибирские электронные математические известия -2017. -Т.14. -С.657-672. doi: 10.17377/semi.2017.14.057. - URL: http://semr.math.nsc.ru/v14/p657-672.pdf. (дата обращения: 08.01.2017). - **Internet resources**

7. At the end of the article, after the list of references, it is necessary to indicate bibliographic data in Russian and English (if the article is in Kazakh), in Kazakh and English (if the article is in Russian) and in Russian and Kazakh languages (if the article is English language). Then a combination of the English-language and transliterated parts of the references list and information about authors (scientific degree, office address, telephone, e-mail - in Kazakh, Russian and English) is given.

8. *Address:* 010008, Republic of Kazakhstan, Astana, Satpayev St., 2., L.N. Gumilyov Eurasian National University, Main Building, room 408). E-mail: *vest_ math@enu.kz.* Сайт: *bulmathmc.enu.kz.*

Правила представления работ в журнал
"Вестник Евразийского национального университета имени Л.Н.Гумилева. Серия Математика. Информатика. Механика"

Редакция журнала просит авторов ознакомиться с правилами и придерживаться их при подготовке работ, направляемых в журнал. Отклонение от установленных правил задерживает публикацию статьи.

1. Отправление статьи в редакцию означает согласие автора (авторов) на право Издателя, Евразийского национального университета имени Л.Н. Гумилева, издания статьи в журнале и переиздания их на любом иностранном языке.

2. В редакцию (в бумажном виде, подписанном всеми авторами и в электронном виде) представляются Tex- и Pdf-файлы работы, подготовленные в издательской системе LaTeX, с обязательным использованием оригинального стилевого файла журнала. Стилевой файл можно скачать со сайта журнала *bulmathmc.enu.kz*.

3. Объем статьи не должен превышать 18 страниц (от 6 страниц). Работы, превышающие указанный объем, принимаются к публикации в исключительных случаях по особому решению Редколлегии журнала.

4. Текст работы начинается с рубрикатора МРНТИ (Международный рубрикатор научно-технической информации), затем следуют инициалы и фамилия автора(ов), полное наименование организации, город, страна, E-mail автора(ов), заглавие статьи, аннотация. Аннотация должна состоять из 150-250 слов, не должна содержать громоздкие формулы, по содержанию не должна повторять название статьи, не должна содержать ссылки на текст работы и список литературы, должна быть кратким изложением содержания статьи, отражая её особенности и сохранять структуру статьи - введение, постановка задачи, цели, история, методы исследования, результаты с их обсуждением, заключение, выводы.

5. Таблицы включаются непосредственно в текст работы, они должны быть пронумерованы и сопровождаться ссылкой на них в тексте работы. Рисунки, графики должны быть представлены в одном из стандартных форматов: PS, PDF, TIFF, GIF, JPEG, BMP, PCX. Точечные рисунки необходимо выполнять с разрешением 600 dpi. На рисунках должны быть ясно переданы все детали.

6. Список литературы должен содержать только те источники (пронумерованные в порядке цитирования или в порядке английского алфавита), на которые имеются ссылки в тексте работы. Ссылки на неопубликованные работы, результаты которых используются в доказательствах, не допускаются.

Авторам рекомендуется при оформлении ссылок исключить упоминание страниц и руководствоваться следующим шаблоном: номер главы, номер параграфа, номер пункта, номер теоремы (леммы, утверждения, замечания к теореме и т.п.), номер формулы. Например, "..., см. [3; § 7, лемма 6]"; "..., см. [2; замечание к теореме 5]". В противном случае при подготовке англоязычной версии статьи могут возникнуть неверные ссылки.

Примеры оформления списка литературы

1 Воронин С. М., Карацуба А. А. Дзета-функция Римана. -М: Физматлит, -1994, -376 стр. - **книга**

2 Баилов Е. А., Сихов М. Б., Темиргалиев Н. Об общем алгоритме численного интегрирования функций многих переменных // Журнал вычислительной математики и математической физики -2014. -Т.54. № 7. -С. 1059-1077. - **статья**

3 Жубанышева А.Ж., Абикенова Ш. О нормах производных функций с нулевыми значениями заданного набора линейных функционалов и их применения к поперечниковым задачам // Функциональные пространства и теория приближения функций: Тезисы докладов Международной конференции, посвященной 110-летию со дня рождения академика С.М.Никольского, Москва, Россия, 2015. - Москва, 2015. -С.141-142. - **труды конференции**

4 Нуртазина К. Рыцарь математики и информатики. -Астана: Каз.правда, 2017. 19 апреля. -С.7. - **газетная статья**

5 Кыров В.А., Михайличенко Г.Г. Аналитический метод вложения симплектической геометрии // Сибирские электронные математические известия -2017. -Т.14. -С.657-672. doi: 10.17377/semi.2017.14.057. - URL: http://semr.math.nsc.ru/v14/p657-672.pdf. (дата обращения: 08.01.2017). - **электронный журнал**

7. После списка литературы, необходимо указать библиографические данные на русском и английском языках (если статья оформлена на казахском языке), на казахском и английском языках (если статья оформлена на русском языке) и на русском и казахском языках (если статья оформлена на английском языке). Затем приводится комбинация англоязычной и транслитерированной частей списка литературы и сведения по каждому из авторов (научное звание, служебный адрес, телефон, e-mail - на казахском, русском и английском языках).

8. *Адрес редакции:* 010008, Казахстан, г. Астана, ул. Сатпаева, 2, Евразийский национальный университет имени Л.Н.Гумилева, учебно-административный корпус, каб. 408. Тел: (7172) 709-500 (вн. 31-428). E-mail: *vest_ math@enu.kz*. Сайт: *bulmathmc.enu.kz*.