

ЧЕБЫШЕВСКИЙ СБОРНИК

Том 14 Выпуск 1 (2013)

УДК 511.34

О ПРЕДСТАВЛЕНИЯХ НАТУРАЛЬНЫХ ЧИСЕЛ

В. Г. Чирский, В. Ю. Матвеев (г. Москва)

Аннотация

Задача представления натуральных чисел в виде сумм слагаемых определенного вида актуальна в теории чисел и ее приложениях. Интерес представляют среднее значение длины таких разложений и необходимое количество вспомогательных вычислений. В статье рассмотрены разложения с двойной базой, цепи с двойной базой, полиадическое (факториальное) разложения натуральных чисел.

ON REPRESENTATIONS OF POSITIVE INTEGERS

V. G. Chirskii, V. Y. Matveev

Abstract

The problem of representing integers as sums of terms of a certain type is actual in number theory and its applications.

We are interested in the average length of these expansions and the required number of auxiliary calculations. The paper deals with DBNS, chains and the polyadic (factorial) expansions of positive integers.

1. Введение

Задача представления натуральных чисел в виде сумм слагаемых определенного вида актуальна в теории чисел и ее приложениях [1], [5], [6], [7], [8]. Интерес представляют среднее значение длины таких разложений и необходимое количество вспомогательных вычислений. В работе проводится сравнение следующих способов представления натуральных чисел.

Во-первых, это разложение чисел с использованием двух оснований, т.е. представление чисел в виде суммы слагаемых вида $2^a 3^b$, a, b — неотрицательные целые числа, которое принято называть разложением DBNS.

Во-вторых, это представление чисел с помощью цепи с двойным основанием, т.е. представление числа N в виде

$$\begin{aligned} N &= \sum_{i=1}^m s_i 2^{a_i} 3^{b_i}, \text{ где } s_i \in \{-1; 1\}, \\ a_1 &\geq a_2 \geq \dots \geq a_m \geq 0, \\ b_1 &\geq b_2 \geq \dots \geq b_m \geq 0. \end{aligned} \quad (1)$$

Третье рассматриваемое представление назовем полиадическим или (факториальным) представлением числа N в виде

$$\begin{aligned} N &= \sum_{n=1}^r a_n \cdot n!, \\ a_n &\in \{0; 1; 2; \dots; n\} \end{aligned}$$

Термин полиадическое разложение связан с теорией полиадических чисел. Дадим краткое введение в эту теорию.

На кольце $\mathbb{Z}$ целых чисел можно ввести топологию τ , рассматривая множество идеалов (m) в качестве полной системы окрестностей нуля аддитивной группы целых чисел. При этом операции сложения и умножения непрерывны и кольцо целых чисел с введенной топологией имеет структуру топологического кольца (см. [1], [2]). Обозначим это кольцо $\mathbb{Z}_\tau$. На кольце $\mathbb{Z}_\tau$ можно ввести метрику (см. [1], [3]), положив

$$\rho(x, y) = \sum_{m=1}^{\infty} \frac{\delta_m(x, y)}{2^m}, \quad (2)$$

где

$$\delta_m(x, y) = \begin{cases} 0, & \text{если } x \equiv y \pmod{m}, \\ 1, & \text{если } x \not\equiv y \pmod{m}. \end{cases} \quad (3)$$

Бесконечная последовательность $x_1, x_2, \dots$ целых чисел называется фундаментальной, если для любого $k \in \mathbb{N}$ существует $\mathcal{N} \in \mathbb{N}$ такое, что для всех $m, n > \mathcal{N}$ справедливо сравнение $x_m \equiv x_n \pmod{k!}$.

Метрическое пространство $\mathbb{Z}_\tau$ не является полным. Например, последовательность $1!, 1! + 2!, \dots, 1! + 2! + \dots + n!, \dots$ является фундаментальной, но не имеет предела в $\mathbb{Z}_\tau$. Для фундаментальных последовательностей $\{x_k\}$ и $\{y_k\}$ рассмотрим последовательности $\{x_k + y_k\}$, $\{x_k - y_k\}$, $\{x_k \cdot y_k\}$. Эти последовательности также являются фундаментальными. Таким образом, фундаментальные последовательности элементов из кольца $\mathbb{Z}_\tau$ образуют кольцо.

Будем называть последовательность $c_1, c_2, \dots$ нулевой последовательностью, если $\lim_{n \rightarrow \infty} c_n = 0$, где предел понимается в смысле топологии кольца $\mathbb{Z}_\tau$.

Назовем фундаментальные последовательности $\{x_k\}$ и $\{y_k\}$ эквивалентными, если их разность $\{x_k - y_k\}$ является нулевой последовательностью. Это свойство является рефлексивным, симметричным и транзитивным, т.е. определяет отклонение эквивалентности.

Полиадическим числом будем называть класс эквивалентных фундаментальных последовательностей из $\mathbb{Z}_\tau$.

Легко проверить, что если последовательность $\{x_k\}$ эквивалентна последовательности $\{u_k\}$, а последовательность $\{y_k\}$ эквивалентна $\{w_k\}$, то $\{x_k + y_k\}$ эквивалентна $\{u_k + w_k\}$, $\{x_k - y_k\}$ эквивалентна $\{u_k - w_k\}$, $\{x_k \cdot y_k\}$ эквивалентна $\{u_k \cdot w_k\}$. Поэтому на множестве полиадических чисел можно ввести операции сложения и умножения, что позволяет говорить о кольце $\mathfrak{G}$ целых полиадических чисел. Вложение кольца $\mathbb{Z}$ в $\mathfrak{G}$ осуществляется сопоставлением элементу $x \in \mathbb{Z}$ класса $\mathfrak{x}$ фундаментальных последовательностей, эквивалентных последовательности $x, x, x, \dots$

Так как $\mathbb{Z}_\tau$ - метрическое пространство, его пополнение приводит к топологическому пространству $\mathfrak{G}_\tau$. Кольцо $\mathfrak{G}_\tau$ можно метризовать. Пусть $\mathfrak{x} \in \mathfrak{G}_\tau$ состоит из последовательности $\{x_k\}$, а $\mathfrak{y} \in \mathfrak{G}_\tau$ - последовательности $\{y_k\}$.

Определим

$$\rho(\mathfrak{x}, \mathfrak{y}) = \lim_{k \rightarrow \infty} \rho(x_k, y_k), \quad (4)$$

где расстояние $\rho(x_k, y_k)$ между элементами $x_k, y_k \in \mathbb{Z}_\tau$ определено равенством (2).

Элементы $\mathfrak{a} \in \mathfrak{G}_t$ имеют каноническое представление в виде ряда

$$\mathfrak{a} = \sum_{n=1}^{\infty} a_n \cdot n! \quad (5)$$

где $a_n \in \{0, 1, \dots, n\}$.

Кольцо $\mathfrak{G}_\tau$ является прямым произведением колец $\mathbb{Z}_{p_i}$ по всем простым числам p_i , при этом ряд $\mathfrak{a}$ сходится в любом $\mathbb{Z}_{p_i}$. Действительно, степень, в которой простое число p входит в разложение числа $n!$ на простые множители, равна $\frac{n-S_n}{p-1}$, где S_n - сумма цифр в p -ичном разложении числа n . Следовательно, для любого p_i при $n \rightarrow \infty$

$$|a_n \cdot n!|_{p_i} \rightarrow 0,$$

что является достаточным условием сходимости ряда (5) в $\mathbb{Z}_{p_i}$.

Теоретико-числовые приложения полиадического анализа даны в [1].

2. Представление в DBNS и цепи с двойной базой

По поводу представления DBNS числа N в виде суммы слагаемых вида $2^a 3^b$ известна [4] асимптотическая оценка длины такого разложения числа N :

$$C_0 \frac{\log_2 N}{\log_2 \log_2 N},$$

где для любого $\varepsilon > 0$ при $N > N(\varepsilon)$ $C_0 = 5,70996 + 4,125 \cdot \varepsilon$.

Алгоритм разложения DBNS таков

Вход: k , n -разрядное положительное целое число;

Выход: Последовательность $(\alpha_i, \beta_i)_{i>0}$ такая что $k = \sum_{i=0}^m 2^{\alpha_i} 3^{\beta_i}$ причем $\alpha_1 \geq \dots \geq \alpha_m \geq 0$ и $\beta_1 \geq \dots \geq \beta_m \geq 0$

1: $\alpha_{max} \leftarrow \log_2 n$, $\beta_{max} \leftarrow \log_3 n$

2: while $k > 0$ do

3: Определить $z = 2^{\alpha_m} 3^{\beta_m}$ как наилучшее приближение к числу k причем $\alpha_{max} \geq \alpha_m \geq 0$, $\beta_{max} \geq \beta_m \geq 0$ и $(k - z) \geq 0$

4: print(s, α_m, β_m)

5: $\alpha_{max} \leftarrow \alpha_m$, $\beta_{max} \leftarrow \beta_m$

6: $k \leftarrow k - z$

К недостаткам этого алгоритма можно отнести необходимость вычисления достаточно большого количества чисел вида $2^a 3^b$.

Кроме того, $2^a 3^b$ показатели получающихся при этом чисел $2^a 3^b$ распределены, как показывают примеры, несколько хаотично.

Известно также [6], что существуют числа N такие, что длина их представления с помощью двойной базы не меньше, чем

$$\frac{C_0 \log_N}{(\log \log_N)(\log \log \log_N)},$$

например, число 103- наименьшее число, не имеющее представления (1) длины 2, число 4985 - наименьшее число, не имеющее представления (1) длины 3, число 641687 - наименьшее число не имеющее представления длины 4, а число 326552784 - наименьшее число, не имеющее представления длины 6.

Перейдем к цепям с двойной базой. Алгоритм разложения таков

Вход: k , n -разрядное положительное целое число;

Выход: Последовательность $(s_i, \alpha_i, \beta_i)_{i>0}$ такая что $k = \sum_{i=0}^m s_i 2^{\alpha_i} 3^{\beta_i}$ причем $\alpha_1 \geq \dots \geq \alpha_m \geq 0$ и $\beta_1 \geq \dots \geq \beta_m \geq 0$

1: $\alpha_{max} \leftarrow \log_2 n$, $\beta_{max} \leftarrow \log_3 n$

2: while $k <> 0$ do

3: Определить $z = 2^{\alpha_m} 3^{\beta_m}$ как наилучшее приближение к числу k причем

$\alpha_{max} \geq \alpha_{m+1} \geq \alpha_m \geq 0$ и $\beta_{max} \geq \beta_{m+1} \geq \beta_m \geq 0$

4: print(s, α_m, β_m)

5: $\alpha_{max} \leftarrow \alpha_m$, $\beta_{max} \leftarrow \beta_m$

6: if $k < 0$ then

7: $s \leftarrow -s$

8: $k \leftarrow |k - z|$

Здесь показатели упорядочены, однако оценки длины разложения вида $O\left(\frac{\log N}{\log \log N}\right)$ не доказаны [7].

3. Полиадическое (факториальное) представление натурального числа

Любое натуральное число N допускает единственное разложение в виде

$$N = \sum_{n=1}^k a_n \cdot n!,$$

$$a_n \in \{0; 1; \dots; n\}$$

Алгоритм полиадического представления имеет вид

Вход: k , n -разрядное положительное целое число;

Выход: Последовательность $(a_i, i)_{i \geq 0}$ такая что $k = \sum_{i=0}^m a_i i!$.

1: Определить i_{max} таким что $(i_{max} + 1)! > k$.

2: while $k > 0$ do

3: $a_i \leftarrow i_{max}$, $x_1 \leftarrow 1$, $max_{elem} \leftarrow 0$

4: $x_1 \leftarrow (x_1 + a_i) \setminus 2$

5: if $k \geq x_1 \cdot i_{max}!$

6: $a_i \leftarrow i_{max}$

7: Определить max_{elem} как максимальный элемент на интервале $(x_1 \ a_i)$

такой что $max_{elem} \leq p$

8: else $k < x_1 \cdot i_{max}!$

9: $a_i \leftarrow x_1 - 1$

10: $x_1 \leftarrow 1$

11: Определить max_{elem} как максимальный элемент на интервале $(x_1 \ a_i)$

такой что $max_{elem} \leq p$

12: print(max_{elem}, i_{max})

13: $k \leftarrow k - max_{elem} \cdot i_{max}!$

14: if $i_{max}! > k$ then

15: $i_{max} = i_{max} - 1$

Оценим асимптотическую длину k разложения числа N . Имеют место соотношения

$$k! \leq N < (k+1)!,$$

$$\ln k! \leq \ln N < \ln(k+1)!,$$

$$k \ln k - k \leq \ln N \leq (k+1) \ln k,$$

$$k \ln k \sim \ln N, \ N \rightarrow \infty,$$

$$\ln k \sim \ln \ln N, \ N \rightarrow \infty,$$

откуда $k \sim \frac{\ln N}{\ln \ln N}$.

Таблица чисел вида $a_n \cdot n!$, $a_n = 0; 1, 2, \dots, n$ для каждого n состоит из n чисел.

Размер таблицы чисел вида $a_n \cdot n!$, $a_n = 0; 1, 2, \dots, n$, $n \leq k$ равен $1 + \dots + k = \frac{k(k+1)}{2}$.

Ее составление можно провести, используя только операцию сложения:
если известно число $n!$, то

$$2n! = n! + n!, \quad 3n! = 2n! + n!, \dots, n \cdot n! = (n-1) \cdot n! + n!, \quad (n+1)! = n \cdot n! + n!.$$

4. Несколько примеров разложений чисел указанными выше способами

1. $p_{64} =$

$$= 3490529510847650949147849619903898133417764638493387843990820577$$

Разложение этого числа также представлено в работе [5].

Для разложения ниже приведенный чисел требуются таблицы размером:
для $a_k \cdot k!$ - 1285, для $2^a \cdot 3^b$ - 28837, для цепи $2^a \cdot 3^b$ - 28837. Сверху каждой таблицы указан вид слагаемых.

$a_k \cdot k!$:

(5·49!)	(36·48!)	(8·47!)	(27·46!)	(13·45!)	(44·44!)
(9·43!)	(12·42!)	(35·41!)	(26·40!)	(10·39!)	(33·38!)
(29·37!)	(12·36!)	(7·35!)	(17·34!)	(7·33!)	(27·32!)
(16·31!)	(11·30!)	(5·29!)	(1·28!)	(15·27!)	(2·26!)
(22·25!)	(6·24!)	(6·23!)	(15·22!)	(3·21!)	(11·20!)
(5·19!)	(5·17!)	(6·16!)	(9·15!)	(3·14!)	(9·13!)
(6·12!)	(11·11!)	(6·10!)	(5·9!)	(5·8!)	(7·7!)
(1·6!)	(4·5!)	(4·4!)	(0·0!)		

$2^a \cdot 3^b$:

(51,101)	(63,88)	(55,86)	(21,103)	(22,97)	(79,56)
(46,72)	(125,18)	(27,73)	(109,16)	(40,53)	(76,26)
(17,59)	(54,31)	(69,16)	(50,24)	(45,23)	(40,21)
(11,35)	(21,25)	(7,28)	(38,5)	(12,17)	(18,10)
(14,9)	(5,10)	(10,4)	(8,3)	(6,2)	(0,0)

Цепь $2^a \cdot 3^b$:

(51,101)	(44,100)	(44,96)	(43,94)	(29,98)	(28,95)
(24,95)	(20,94)	(14,94)	(13,92)	(8,92)	(13,86)
(7,85)	(6,80)	(2,78)	(0,77)	(2,73)	(1,70)
(0,67)	(0,65)	(1,63)	(0,61)	(1,59)	(0,57)
(0,54)	(0,54)	(0,53)	(0,50)	(0,50)	(0,46)
(0,45)	(0,44)	(0,41)	(0,39)	(0,38)	(0,37)
(0,36)	(0,35)	(0,32)	(0,32)	(0,31)	(0,30)
(0,29)	(0,27)	(0,26)	(0,26)	(0,24)	(0,23)
(0,22)	(0,21)	(0,17)	(0,17)	(0,13)	(0,10)
(0,8)	(0,5)	(0,5)	(0,3)	(0,2)	(0,0)

2. $p_{64} =$

$= 9340255901486795094418746991098389314371676483943378489309285077$

$a_k \cdot k!$:

(15·49!)	(17·48!)	(19·47!)	(14·46!)	(4·45!)	(7·44!)
(8·43!)	(14·42!)	(28·41!)	(6·40!)	(31·39!)	(13·38!)
(20·37!)	(31·36!)	(2·35!)	(22·34!)	(15·33!)	(29·32!)
(22·31!)	(27·30!)	(8·29!)	(17·28!)	(9·27!)	(17·26!)
(9·25!)	(14·24!)	(1·23!)	(12·22!)	(11·21!)	(9·20!)
(16·19!)	(9·18!)	(7·17!)	(11·16!)	(8·15!)	(1·14!)
(10·13!)	(11·12!)	(3·10!)	(6·9!)	(3·7!)	(2·6!)
(1·4!)	(2·3!)	(0·0!)			

$2^a \cdot 3^b$:

(54,100)	(7,125)	(0,124)	(10,111)	(50,81)	(142,17)
(61,62)	(19,82)	(62,50)	(22,69)	(78,28)	(53,39)
(45,40)	(31,44)	(16,49)	(58,17)	(33,28)	(41,19)
(39,14)	(15,25)	(5,28)	(0,28)	(35,1)	(7,13)
(10,8)	(2,10)	(4,4)	(0,3)	(2,0)	

Цепь $2^a \cdot 3^b$:

(203,6)	(198,4)	(190,6)	(188,3)	(183,3)	(182,1)
(176,2)	(176,0)	(171,0)	(170,0)	(166,0)	(162,0)
(161,0)	(154,0)	(151,0)	(150,0)	(147,0)	(145,0)
(141,0)	(138,0)	(136,0)	(135,0)	(132,0)	(130,0)
(129,0)	(126,0)	(123,0)	(109,0)	(107,0)	(106,0)
(102,0)	(101,0)	(98,0)	(96,0)	(94,0)	(90,0)
(88,0)	(86,0)	(78,0)	(72,0)	(69,0)	(67,0)
(65,0)	(59,0)	(56,0)	(53,0)	(51,0)	(50,0)
(47,0)	(45,0)	(40,0)	(33,0)	(30,0)	(28,0)
(26,0)	(24,0)	(22,0)	(20,0)	(17,0)	(14,0)
(11,0)	(9,0)	(8,0)	(5,0)	(3,0)	(2,0)
(0,0)					

3. $p_{65} =$

$= 32769132993266709549961988190834461413177642967992942539798288533$

Разложение этого числа также представлено в работе [5].

$a_k \cdot k!$:

(1·50!)	(3·49!)	(42·48!)	(34·47!)	(3·46!)	(17·44!)
(21·43!)	(19·42!)	(3·41!)	(26·40!)	(31·39!)	(2·38!)
(30·37!)	(14·36!)	(19·35!)	(7·34!)	(17·33!)	(1·32!)
(21·31!)	(18·30!)	(5·29!)	(10·28!)	(26·26!)	(15·25!)
(5·24!)	(16·23!)	(2·22!)	(20·21!)	(5·20!)	(5·19!)
(12·18!)	(1·17!)	(9·16!)	(10·15!)	(9·14!)	(8·13!)
(4·12!)	(3·10!)	(7·9!)	(6·6!)	(2·4!)	(2·2!)
(0·0!)					

$2^a \cdot 3^b$:

(78,86)	(77,82)	(75,79)	(42,95)	(11,109)	(35,89)
(128,26)	(35,78)	(132,12)	(56,54)	(81,34)	(76,32)
(76,28)	(25,51)	(48,32)	(52,25)	(41,26)	(22,34)
(8,35)	(1,32)	(27,11)	(4,21)	(13,10)	(7,11)
(15,3)	(1,9)	(9,1)	(0,3)	(1,0)	

Цепь $2^a \cdot 3^b$:

(143,45)	(137,44)	(128,45)	(132,39)	(130,35)	(130,32)
(130,28)	(126,27)	(119,27)	(116,26)	(116,24)	(115,22)
(108,21)	(104,20)	(99,20)	(95,19)	(92,19)	(84,20)
(96,9)	(90,9)	(91,6)	(91,3)	(84,4)	(79,3)
(76,2)	(73,2)	(72,1)	(68,1)	(65,0)	(59,1)
(56,0)	(51,0)	(49,0)	(44,0)	(40,0)	(38,0)
(36,0)	(35,0)	(29,0)	(27,0)	(19,0)	(16,0)
(13,0)	(11,0)	(7,0)	(4,0)	(2,0)	(0,0)

4. $p_{65} =$ $= 23679319293627690459916891809384416141377469276999224357989825833$ $a_k \cdot k!$:

(38·49!)	(45·48!)	(23·47!)	(6·46!)	(7·45!)	(26·44!)
(31·43!)	(21·42!)	(20·41!)	(36·40!)	(20·39!)	(34·38!)
(27·37!)	(2·36!)	(34·35!)	(8·34!)	(23·33!)	(5·32!)
(27·31!)	(2·30!)	(13·29!)	(1·28!)	(20·27!)	(20·26!)
(19·25!)	(22·24!)	(10·23!)	(11·22!)	(1·21!)	(14·20!)
(11·19!)	(16·18!)	(15·17!)	(12·16!)	(2·15!)	(3·14!)
(8·13!)	(12·12!)	(9·11!)	(7·10!)	(3·9!)	(4·8!)
(6·7!)	(2·6!)	(1·5!)	(4·4!)	(2·3!)	(2·2!)
(0·0!)					

 $2^a \cdot 3^b$:

(49,104)	(164,27)	(82,73)	(142,31)	(125,35)	(19,95)
(96,41)	(77,47)	(19,79)	(39,62)	(17,71)	(54,43)
(83,20)	(2,67)	(32,44)	(45,30)	(24,39)	(27,32)
(53,11)	(0,40)	(15,25)	(37,7)	(13,18)	(1,22)
(13,11)	(4,14)	(1,11)	(0,7)	(0,4)	(3,0)

Цепь $2^a \cdot 3^b$:

(198,10)	(192,8)	(192,5)	(178,9)	(173,6)	(171,4)
(171,2)	(164,4)	(163,2)	(159,1)	(157,0)	(152,1)
(151,0)	(147,0)	(143,0)	(142,0)	(138,0)	(135,0)
(132,0)	(130,0)	(126,0)	(125,0)	(122,0)	(120,0)
(115,0)	(110,0)	(109,0)	(107,0)	(104,0)	(101,0)
(99,0)	(94,0)	(92,0)	(87,0)	(85,0)	(82,0)
(76,0)	(74,0)	(71,0)	(69,0)	(65,0)	(62,0)
(59,0)	(58,0)	(53,0)	(50,0)	(46,0)	(43,0)
(41,0)	(39,0)	(37,0)	(35,0)	(33,0)	(30,0)
(29,0)	(24,0)	(21,0)	(19,0)	(16,0)	(14,0)
(9,0)	(8,0)	(5,0)	(3,0)	(0,0)	

5. $p_{64} =$ $= 3192936276132993266790459916893143716764930928507767992942535058$ $a_k \cdot k$:

(5·49!)	(12·48!)	(9·47!)	(42·46!)	(10·45!)	(20·44!)
(2·43!)	(27·42!)	(15·41!)	(2·40!)	(34·39!)	(26·38!)
(20·37!)	(23·36!)	(3·34!)	(30·33!)	(31·32!)	(25·31!)
(23·30!)	(16·29!)	(13·28!)	(10·27!)	(1·26!)	(4·25!)
(24·24!)	(17·23!)	(5·22!)	(7·21!)	(7·20!)	(15·19!)
(18·18!)	(7·17!)	(1·16!)	(1·15!)	(9·14!)	(3·13!)
(5·12!)	(2·10!)	(4·9!)	(3·8!)	(4·7!)	(2·6!)
(1·5!)	(2·4!)	(1·3!)	(2·2!)		

 $2^a \cdot 3^b$:

(16,123)	(16,118)	(12,116)	(11,112)	(47,85)	(49,79)
(64,64)	(16,87)	(57,57)	(81,36)	(49,50)	(87,21)
(75,22)	(94,6)	(33,37)	(27,35)	(35,25)	(47,13)
(2,37)	(55,0)	(17,20)	(7,23)	(0,23)	(15,9)
(4,12)	(13,3)	(5,4)	(6,1)	(0,2)	(1,0)

Цепь $2^a \cdot 3^b$:

(16,123)	(16,118)	(12,116)	(11,112)	(9,109)	(5,108)
(3,106)	(8,100)	(8,97)	(7,95)	(3,95)	(6,90)
(6,87)	(6,84)	(2,83)	(2,81)	(4,77)	(5,74)
(5,71)	(0,70)	(5,63)	(0,63)	(0,60)	(0,58)
(0,57)	(0,55)	(0,52)	(0,49)	(0,49)	(0,48)
(0,47)	(0,46)	(0,43)	(0,42)	(0,42)	(0,38)
(0,37)	(0,35)	(0,34)	(0,33)	(0,30)	(0,29)
(0,28)	(0,26)	(0,25)	(0,24)	(0,24)	(0,23)
(0,21)	(0,16)	(0,16)	(0,15)	(0,13)	(0,12)
(0,10)	(0,9)	(0,8)	(0,7)	(0,4)	(0,4)
(0,2)	(0,2)	(0,1)	(0,0)		

5. Численные эксперименты.

Так как асимптотические закономерности могут давать искаженное представление об истинном характере поведения величин, в заданном интервале были проведены соответствующие численные эксперименты со случайными числами.

Описание алгоритма генерирования n -разрядного псевдослучайного числа.

Вход: k, n -разрядное положительное целое число;

Выход: num n -разрядное положительное целое число;

1: $num \leftarrow 0$

2: while $num < k$ do

3: Генерировать одноразрядное псевдослучайное число z такое что $0 \leq z \leq 9$

4: $num \leftarrow (num \cdot 10) + z$

5: print(num)

Статистические данные.

Было проведено 10 выборок по 100 чисел каждая. Разрядность каждого из чисел выборки колеблется от 159 до 160 разрядов.

В таблицах приведены средние значения длин разложений.

	Выборка 1	Выборка 2	Выборка 3	Выборка 4
$a_k \cdot k!$	81	81	81	81
$2^a \cdot 3^b$	62	61	62	61
Цепь $2^a \cdot 3^b$	98	96	96	95
	Выборка 5	Выборка 6	Выборка 7	
$a_k \cdot k!$	81	81	81	
$2^a \cdot 3^b$	62	62	61	
Цепь $2^a \cdot 3^b$	100	92	98	
	Выборка 8	Выборка 9	Выборка 10	
$a_k \cdot k!$	81	81	81	
$2^a \cdot 3^b$	62	62	62	
Цепь $2^a \cdot 3^b$	94	92	102	

В этих пределах требуются таблицы размером: для $a_k \cdot k!$ - 5151, для $2^a \cdot 3^b$ - 175839, для цепи $2^a \cdot 3^b$ - 175839.

СПИСОК ЦИТИРОВАННОЙ ЛИТЕРАТУРЫ

1. Постников А. Г. Введение в аналитическую теорию чисел. М.: Наука, 1971.
2. Понтрягин Л. С. Непрерывные группы. М.: Наука, 1984 .
3. Новоселов Е. В. Топологическая теория делимости целых чисел // Учен. зап. Елабуж. гос. пед. ин-та. 1960. №3. С. 3—23.

4. Чирский В. Г., Шакиров Р. Ф. О представлении натуральных чисел с использованием нескольких оснований // Чебышевский сборник. 2013. Т. 14. Вып. 1(45). С. 86—93.
5. Dimitrov V. S., Jullien G. A. and Miller W. C., "An Algorithm for Modular Exponentiation" // Inform. Process. Lett. 1998. V. 66. №3. P. 155—159.
6. Dimitrov V. S., Rowe E. W. Lower bounds on the lengths of double base representations // Proc. Amer. Math. Soc. 2011. V. 139. №10. P. 3423—3430.
7. Doche Ch., Imbert L. Extended Double-Base Number System with Application to Elliptic Curve Cryptography // INDOCRYPT 2006, LNCS 4329. Springer-Verlag, 2006. P. 335—348.
8. Edward B. Burger, David C. Clyde, Cory H. Colbert, Gea Hyun Shin and Zhaoning Wang (Williamstown, MA) A generalization of a theorem of Lekkerkerker to Ostrowski's decomposition of natural numbers // Acta Arithmetica. 2012. V. 153. №3. P. 217—249.

Московский педагогический государственный университет
Поступило 10.02.2013