Секция «Математика и механика»

Сравнительный анализ некоторых способов представления натуральных чисел

Матвеев Владимир Юрьевич
Аспирант
МПГУ, Математический факультет, Москва, Россия
E-mail: salomaa@mail.ru

Задача представления натуральных чисел в виде сумм слагаемых определенного вида рассматривалась многими авторами (см., например [1], [2], [3], [4], [5]). Рассматриваются 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^a3^b, a, b – неотрицательные целые числа. Во-вторых, это представление чисел с помощью цепи с двойным основанием, т.е. представление числа N в виде

$$N = \sum_{i=1}^{m} s_i 2^{a_i} 3^{b_i}, \text{где } s_i \in \{-1; 1\}, a_1 \geqslant a_2 \geqslant \ldots \geqslant a_m \geqslant 0, b_1 \geqslant b_2 \geqslant \ldots \geqslant b_m \geqslant 0.$$

Любое натуральное число N допускает единственное разложение в виде

$$N = \sum_{n=1}^{k} a_n \cdot n!, a_n \in \{0; 1; \ldots; n\}$$

Это разложение назовем полиадическим (или факториальным). Термин полиадическое разложение связан с теорией полиадических чисел [1]. По поводу представления числа N в виде суммы слагаемых вида 2^a3^b известна асимптотическая оценка длины такого разложения числа N:

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

где для любого $\varepsilon > 0$ при $N > N(\varepsilon)$ $C_0 = 5,70996 + 4,125 \cdot \varepsilon$.
Для цепи с двойной базой оценки длины разложения вида $O\left(\frac{\log N}{\log \log N}\right)$ не доказаны [4]. Для получения разложения с двойной базой и для получения разложения в цепь с двойной базой требуется сравнительно большое количество вычислений элементов вида 2^a3^b. При этом показатели получающихся при этом чисел 2^a3^b распределены, как показывают примеры, несколько хаотично. Известно также, [3] что существуют числа N такие, что длина их представления с помощью двойной базы не меньше, чем

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

Для длины k полиадического разложения справедлива асимптотическая оценка $k \sim \frac{\ln N}{\ln \ln N}$. При этом требуется $k(k+1)$ вспомогательных вычислений. Так как асимптотические закономерности могут давать искаженное представление об истинном характере

поведения величин, в заданном интервале были проведены соответствующие численные эксперименты со случайными числами. Было проведено 10 выборок по 100 чисел каждая. Разрядность каждого из чисел выборки колеблется от 159 до 160 разрядов. Вычисления показали что факториальное разложение имеет среднюю длину около 80. При этом требуется около 5000 вспомогательных вычислений. Разложения с двойной базой имеет среднюю длину около 60, а разложение в цепь имеет среднюю длину около 100. Однако для этих разложений требуется около 180000 вспомогательный вычислений.

Список литературы

[1] Постников А. Г. Введение в аналитическую теорию чисел. М. Наука. 1971.

[2] Dimitrov V. S., Jullien G. A. and Miller W. C., "An Algorithm for Modular Exponentiation". Inform. Process. Lett. 66 (1998), no. 3, 155-159.

[3] Dimitrov V. S., Rowe E. W. Lower bounds on the lenghts of double base representations. Proc. Amer. Math. Soc. v.139, №10, 2011, pp. 3423-3430

[4] Doche Ch., Imbert L. Extended Double-Base Number System with Application to Elliptic Curve Cryptography. INDOCRYPT 2006, LNCS 4329, Springer-Verlag 2006, pp. 335-348

[5] 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 153.3 (2012) pp. 217-249