НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
ПОЛТАВСЬКА ПОЛІТЕХНІКА
ІМЕНІ ЮРІЯ КОНДРАТЮКА

ЗБІРНИК МАТЕРІАЛІВ

76-Ї НАУКОВОЇ КОНФЕРЕНЦІЇ ПРОФЕСОРІВ, ВИКЛАДАЧІВ, НАУКОВИХ ПРАЦІВНИКІВ, АСПІРАНТІВ ТА СТУДЕНТІВ УНІВЕРСИТЕТУ

ТОМ 1

14 травня – 23 травня 2024 р.

УДК 004.056.5

А.С.Янко к.т.н., доцент
О.І.Крук, О.О Крук аспіранти
Національний університет
«Полтавська політехніка імені Юрія Кондратюка»

МЕТОД ПІДНЕСЕННЯ ДО СТЕПЕНЮ ЗА МОДУЛЕМ ДОДАТНИХ ТА ВІД'ЄМНИХ ЦІЛИХ ЧИСЕЛ

Дослідження в галузі застосування непозиційної системи числення (НСЧ), до якої відноситься модульна система числення (МСЧ), показують, що її практичне використання в комп'ютерних системах дозволяє значно підвищити продуктивність реалізації арифметичних операцій. Слід зазначити, що існує клас задач і алгоритмів, де крім виконання основних цілочисельних арифметичних операцій, необхідно реалізувати операцію піднесення чисел до степеня у всій числовій області. Операція піднесення до степеня цілих чисел за модулем є одним із ключових елементів багатьох криптографічних алгоритмів і має багато практичних застосувань в інформатиці та інших галузях. Багато сучасних мов програмування не мають засобів, які можуть реалізувати операцію піднесення чисел до степеня, особливо складно реалізувати дану операцію для від'ємних чисел [1]. Існуючі практичні методи не можуть бути використані для виконання операції піднесення до степеня у від'ємній числовій області [2], через відсутність простої математичної моделі для процесу піднесення до степеня цілих чисел натурального числа в МСЧ, як в додатних і від'ємних числових областях. Тому основною метою дослідження є розробка ефективної системи математичних співвідношень процесу піднесення чисел до степеня в МСЧ у всій числовій області.

Реалізація процесу операції піднесення чисел до степеня за модулем МСЧ у всій числовій області, передбачає представити вихідне число $M_{МСЧ} = (m_1 \,||\, m_2 \,||\, ... \,||\, m_{n-1} \,||\, m_n \,||\, m_{n+1} \,||\, ... \,||\, m_d)$ у модульній структурі (МС) $M^{\rightarrow}_{МСЧ}$:

$$\begin{cases} M^{\rightarrow}_{МСЧ} = \dfrac{1}{2}C + \left|M_{МСЧ}\right|, \text{ якщо } M \geq 0, \\ M^{\rightarrow}_{МСЧ} = \dfrac{1}{2}C - \left|M_{МСЧ}\right|, \text{ якщо } M < 0, \end{cases} \tag{1}$$

тобто для додатних чисел: $M^{\rightarrow}_{МСЧ} = \dfrac{1}{2}C + \left|M_{МСЧ}\right|$ і для негативних: $M^{\rightarrow}_{МСЧ} = \dfrac{1}{2}C - \left|M_{МСЧ}\right|$, де $C = \prod_{n=1}^{d} h_n$, h_n – довільний модуль МСЧ. Система математичних співвідношень процес піднесення чисел до степеня був розроблений на основі аналітичного співвідношення $(M^t_{МСЧ})^{\rightarrow} = f(M^{\rightarrow}_{МСЧ})$, що визначає відношення результату $M^t_{МСЧ}$ операції піднесення числа $M_{МСЧ}$

в МСЧ до степеня *t*, представленому в МС, від числа $M^{\rightarrow}_{МСЧ}$ відразу в МС [2]. Оброблені числа $M^{t}_{МСЧ}$ та $(M^{\rightarrow}_{МСЧ})^{t}$ знаходяться в діапазоні:

$$\begin{cases} -\frac{1}{2}C \le M^{t}_{МСЧ} \le \frac{1}{2}(C-1), \\ 0 \le (M^{\rightarrow}_{МСЧ})^{t} \le C-1. \end{cases} \quad (2)$$

В якості математичної моделі процесу піднесення чисел до довільного степеня *t* натурального числа в МСЧ доцільно розглядати математичне співвідношення:

$$(M^{t}_{МСЧ})^{\rightarrow} = (M^{\rightarrow}_{МСЧ})^{t} \quad (3)$$

Математичне співвідношення (3) – це узагальнений процес піднесення чисел до степеня за модулем МСЧ. На основі розробленого математичного співвідношення (3) та використання табличної реалізації операції модульного множення вдосконалено метод піднесення чисел до степеня за модулем МСЧ у всій числовій області [3]. Розвиток методу здійснювався шляхом застосування спеціального кодування чисел у МСЧ із застосуванням табличного принципу обробки даних. Результат розробленого методу представлено у вигляді прикладів операції піднесення чисел, представлених у МСЧ. Аналіз розв'язку прикладів показав практичну цінність розробленого методу.

Література

1. Pakkiraiah Ch., Satyanarayana R. Design and FPGA Realization of an Energy Efficient Artificial Neural Modular Exponentiation Architecture. *Computing, Communication and Learning.* 2023. P. 115-126.

2. Krasnobayev V., Yanko A., Martynenko A., Kovalchuk D. Method for computing exponentiation modulo the positive and negative integers. XI *International Scientific and Practical Conference ICST-202*3, September 21–23, 2023, Odessa, Ukraine, 2023, 3513, pp. 374–383.

3. Krasnobaev V., Yanko A., Kovalchuk D. Methods for tabular implementation of arithmetic operations of the residues of two numbers represented in the system of residual classes. *Radio Electronics, Computer Science, Control (4)*. – 2022. – P. 18–27. https://doi.org/10.15588/1607-3274-2022-4-2