

АЛГОРИТМИ ПРЯМОГО ПЕРЕТВОРЕННЯ ПОЗИЦІЙНОГО ЧИСЛА ДО СИСТЕМИ ЗАЛИШКОВИХ КЛАСІВ ТА ЙОГО ЗВОРОТНОГО ПЕРЕТВОРЕННЯ

Анотація. Підвищення швидкодії комп'ютерних структур пов'язане із залученням нових принципів, заснованих на використанні системи числення залишкових класів. При виконанні низки обчислювальних операцій з використанням непозиційної системи числення залишкових класів вирішується задача прямого перетворення чисел із позиційної системи числення в систему числення залишкових класів та зворотного перетворення чисел із системи числення залишкових класів у позиційну систему. Ряд робіт містить способи реалізації цих операцій різної складності, але їхнє рішення далеке від досконалості. Результати дослідження вказують на можливість отримання більш ефективного рішення, що спрощує практичну реалізацію операцій прямого перетворення чисел із позиційної системи числення до системи числення залишкових класів та зворотного перетворення чисел. Метою дослідження є аналіз реалізації операцій прямого перетворення чисел із позиційної системи числення в систему числення залишкових класів та зворотного перетворення чисел. Інструментами методології дослідження є системний аналіз, теорія чисел та китайська теорема про залишки. Методологія дослідження полягає в аналізі спеціальних таблиць залишків за модулями. Пропонується алгоритм виконання складних операцій, що ґрунтується на використанні поліадичного коду числа, представленого в системі числення залишкових класів. Пропонується простий та ефективний підхід з використанням ітераційних табличних операцій із залишками. Для кожного значення заданих залишків константи знаходять шляхом простої вибірки відповідної таблиці. Метод, що лежить в основі реалізації цих складних операцій, полягає в підсумовуванні обраних констант до шуканого значення, при цьому відповідні константи віднімаються від значень відомих залишків до звернення останнього в нуль. Метод алгоритмічно простий і нескладний для схемної реалізації, і його слід розглядати як один із напрямків досліджень щодо підвищення ефективності обчислень у системі залишкових класів.

Ключові слова: залишкові класи; системи модулів; таблиці; пряме та зворотне перетворення чисел.

Постановка проблеми. Підвищення швидкодії обчислювальних структур пов'язано нині із залученням нових принципів на підставі використання системи залишкових класів (СЗК) [1]. Система числення залишкових класів - це си-

стема, в якій довільне число представлено у вигляді набору найменших невід'ємних залишків по модулях $p_1, p_2, \dots, p_n$, тобто $N = (\alpha_1, \alpha_2, \dots, \alpha_n)$. Тут $\alpha_i = N \pmod{p_i}$. При цьому, якщо числа p_i взаємно прості, то такому представленню відповідає тільки одне число N в діапазоні $[0, M)$, де $M = p_1 p_2 \dots p_n$.

У СЗК арифметичні операції складання, віднімання та множення виконуються із залишками незалежно один від одного за простими правилами. Тому операції над розрядами можна виконувати одночасно, що забезпечує високий рівень паралелізму. До переваг такого представлення чисел належить також мала розрядність залишків, висока точність і надійність, здатність системи до самокорекції. Однак виникають серйозні труднощі при реалізації немодульних операцій, для виконання яких необхідне знання цифр операндів за всіма розрядами. До таких немодульних операцій відносяться, зокрема, пряме перетворення чисел із позиційної системи числення у систему залишкових класів та зворотне перетворення чисел із СЗК у позиційну систему числення.

Формалізована постановка задачі наступна.

Нехай є деяка позиційна, наприклад, десяткова система числення $C1 = \{m_n = 10^{n-1}, \dots, m_2 = 10^1, m_1 = 10^0\}$, $M_1 = 10^n$, система залишкових класів $C2 = \{p_1, p_2, \dots, p_r\}$, $M_2 = p_1 p_2 \dots p_r$ і число N у системі $C1$ $N = \varepsilon_1 \varepsilon_2 \dots \varepsilon_n$ таке, що $N < \min\{M_1, M_2\}$. Необхідно для числа $N = \varepsilon_1 \varepsilon_2 \dots \varepsilon_n$, представленого в $C1$, виконати перетворення на представлення $N = (\alpha_1, \alpha_2, \dots, \alpha_r)$ цього числа в СЗК $C2$, де $\alpha_i = N \pmod{p_i}$. Другим етапом є зворотне перетворення числа N до системи $C1$.

Аналіз останніх досліджень і публікацій. Ряд робіт, наприклад [2, 3] містить різні за складністю методи реалізації даних операцій, однак розв'язання їх далеке від досконалості. Результати виконаних досліджень свідчать про можливість отримання більш ефективного рішення, яке дозволяє де-що спростити практичну реалізацію операцій прямого перетворення чисел із позиційної системи числення в СЗК та зворотне перетворення чисел.

Формулювання мети дослідження. Метою дослідження є аналітичний розгляд СЗК для реалізації операцій прямого перетворення чисел із позиційної системи числення в систему залишкових класів та зворотне перетворення чисел.

Виклад основного матеріалу. Алгоритм прямого перетворення розглянемо на прикладі перетворення, наприклад, числа $N = 97$, тобто $\varepsilon_1 = 9, \varepsilon_2 = 7$ у його представлення $N = (\alpha_1, \alpha_2, \alpha_3)$ у системі модулів $p_1 = 5, p_2 = 7, p_3 = 3$. Для цього необхідні наведені нижче табл.1, табл.2.

Таблиця 1

Модулі				
5			7	3
π_1	δ_1	α_1^1	α_2^1	α_3^1
0	0	0	0	0
1	10	0	3	1
2	20	0	6	2
3	30	0	2	0
4	40	0	5	1
5	50	0	1	2
6	60	0	4	0
7	70	0	0	1
8	80	0	3	2
9	90	0	6	0

Таблиця 2

Модулі				
5			7	3
π_2	δ_2	α_1^2	α_2^2	α_3^2
0	0	0	0	0
1	1	1	1	1
2	2	2	2	2
3	3	3	3	0
4	4	4	4	1
5	5	0	5	2
6	6	1	6	0
7	7	2	0	1
8	8	3	1	2
9	9	4	2	0

Значення шуканих залишків приймається $\alpha_1 = 0, \alpha_2 = 0, \dots, \alpha_r = 0$, тобто $N_0 = (0, 0, \dots, 0)$. На першій ітерації для $\varepsilon_1 = 9$ з табл.1 вибирається рядок $\alpha_1^1 = 0, \alpha_2^1 = 6, \alpha_3^1 = 0$, тобто $\tilde{N}_1 = (0, 6, 0)$, що підсумовується до $N_0 = (0, 0, \dots, 0)$. Отримуємо $N_1 = (0, 6, 0)$.

На другий ітерації для $\varepsilon_2 = 7$ з табл.2 вибирається рядок $\alpha_1^1 = 2, \alpha_2^2 = 0, \alpha_3^2 = 1$, тобто $\tilde{N}_2 = (2, 0, 1)$, що підсумовується до $N_1 = (0, 6, 0)$. Отримуємо $N_2 = (2, 6, 1)$.

Алгоритм зворотного перетворення ґрунтується на використанні поліадичного коду числа, представленого в СЗК.

Якщо системою модулів поліадичного коду також є система $p_1, p_2, \dots, p_n$, то число N в поліадичному коді представляється у вигляді

$$N = \pi_1 + \pi_2 p_1 + \dots + \pi_i p_1 p_2 \dots p_{i-1} + \dots + \pi_n p_1 p_2 \dots p_{n-1}, \quad \text{де } 0 < \pi_i \leq p_i - 1.$$

$$\text{Тоді } \alpha_1 = N \pmod{p_1} = \pi_1 \quad \text{та} \quad \pi_1 = \alpha_1.$$

.....

.....

$$\alpha_i = (\pi_1 + \pi_2 p_1 + \dots + \pi_i p_1 p_2 \dots p_{i-1}) \pmod{p_i}$$

$$\text{та} \quad \pi_i p_1 p_2 \dots p_{i-1} = \alpha_i - (\pi_1 + \pi_2 p_1 + \dots + \pi_{i-1} p_1 p_2 \dots p_{i-2}) \pmod{p_i}.$$

Отже, базовий алгоритм складається з наступних ітерацій.

Значення шуканого числа приймається $N_1^1 = 0$. На першій ітерації по кожному з модулів $p_1, p_2, \dots, p_n$ визначається різниця між залишком по цьому модулю і значенням π_1 , взята по даному модулю, в результаті чого знаходиться значення $\pi_2 p_1$. Назвемо такі різниці наведеними залишками. У той самий час значення π_1 підсумовується з N_1^1 . На другій ітерації по кожному з модулів $p_2, \dots, p_n$ визначається різниця між наведеним залишком по цьому модулю і значенням $\pi_2 p_1$, взятим по даному модулю. У результаті знаходиться значення $\pi_3 p_1 p_2$, а значення $\pi_2 p_1$ підсумовується з отриманим раніш значенням залишку по модулю p_1 . Після виконання $n-1$ ітерацій отримуємо залишок α_n .

Робота алгоритму зворотного перетворення для переходу від представлення числа $N_1^1 = 97 = (2, 6, 1)$ в системі модулів $p_1 = 5, p_2 = 7, p_3 = 3$ до його представлення в позиційній десятковій системі числення за першим варіантом наступна.

До визначення значення числа приймемо початкове значення рівним нулю, тобто $N_1^1 = 0$.

На першій ітерації з табл.3 для $\alpha_1^1 = 2$ вибираємо константи 2, 2, 2 відповідно за модулями $p_1 = 5, p_2 = 7, p_3 = 3$, які віднімаємо із залишків 2, 6, 1. Отримуємо $N_1^1 = 95 = (0, 4, 2)$. З цієї ж табл.3 для $\alpha_1^1 = 2$ вибираємо константу $\Delta_1 = 2$, яку додаємо до залишку 0. В результаті отримуємо $N_1^1 = 2$.

Таблиця 3

Модулі					Константи Δ_1
5			7	3	
π_1	δ_1	α_1^1	α_2^1	α_3^1	
0	0	0	0	0	0
1	1	1	1	1	1
2	2	2	2	2	2
3	3	3	3	0	3
4	4	4	4	1	4

Таблиця 4

Модулі				Константи Δ_2
7			3	
π_2	$\delta_2 = \pi_2 p_1$	α_2^2	α_3^2	
0	0	0	0	0
1	5	5	2	5
2	10	3	1	10
3	15	1	0	15
4	20	6	2	20
5	25	4	1	25
6	30	2	0	30

Таблиця 5

Модулі			
3			Константи Δ_3
π_3	$\delta_3 = \pi_3 p_1 p_2$	α_3^3	
0	0	0	0
1	35	2	35
2	70	1	70

На другій ітерації з табл.4 для $\alpha_2^2 = 4$ вибираємо константи 4, 1 відповідно по модулях $p_2 = 7, p_3 = 3$, які віднімаємо із залишків 4, 2. Отримуємо $N_1^2 = 70 = (0, 0, 1)$. З цієї ж табл.4 вибираємо константу $\Delta_2 = 25$, яку додаємо до залишку $N_2^1 = 2$. В результаті отримуємо $N_2^2 = 27$.

На третій ітерації з табл.5 для $\alpha_3^3 = 1$ вибираємо константу 1 по модулю $p_3 = 3$, яку віднімаємо з залишку 1. Отримуємо $N_1^3 = 0 = (0, 0, 0)$. З цієї ж табл.5 для $\alpha_3^3 = 1$ вибираємо константу $\Delta_3 = 70$, яку додаємо до залишку 27. В результаті отримуємо $N_2^3 = 97$.

Для другого варіанту алгоритму зворотного перетворення числа скористу-

ємо представленням чисел у зворотному коді [4].

При заданні числа N залишками число $\bar{N} = (\bar{\alpha}_1, \bar{\alpha}_2, \dots, \bar{\alpha}_n)$ є представленням числа $N = (\alpha_1, \alpha_2, \dots, \alpha_n)$ у зворотному коді, де $\bar{\alpha}_i = (p_i - 1) - \alpha_i$ - зворотний код залишку α_i .

Зворотним кодом числа $N_1^1 = 97$ у системі модулів $p_1 = 5, p_2 = 7, p_3 = 3$, $M_1 = p_1 p_2 p_3 = 5 * 7 * 3 = 105$ є число $\bar{N}_1^1 = 7 = (2, 0, 1)$.

До визначення значення числа приймемо початкове значення рівним $M_1 - 1 = p_1 p_2 p_3 - 1 = 5 * 7 * 3 - 1 = 104$, тобто $\bar{N}_2^1 = 104$.

На першій ітерації з табл.3 для $\bar{\alpha}_1^1 = 2$ вибираємо константи 2, 2, 2 відповідно за модулями $p_1 = 5, p_2 = 7, p_3 = 3$, які віднімаємо від залишків 2, 0, 1. Отримуємо $\bar{N}_1^1 = 5 = (0, 5, 2)$. З цієї ж табл.3 для $\bar{\alpha}_1^1 = 2$ вибираємо константу $\bar{\Delta}_1 = 2$, яку віднімаємо від $M_1 - 1 = 104$. В результаті отримуємо $\bar{N}_2^1 = 102$.

На другій ітерації з табл.4 для $\bar{\alpha}_2^2 = 5$ вибираємо константи 5, 2 відповідно по модулях $p_2 = 7, p_3 = 3$, які віднімаємо із залишків 5, 2. Отримуємо $\bar{N}_1^2 = 0$. З цієї ж табл.4 вибираємо константу $\bar{\Delta}_2 = 5$, яку віднімаємо із $\bar{N}_2^1 = 102$. В результаті отримуємо $\bar{N}_2^2 = 97$.

Отже, результат перетворення спочатку досягається за другим варіантом. Тому є доцільним одночасне виконання обох варіантів.

Таким чином, розглянуті алгоритми забезпечують пряме перетворення чисел із позиційної системи числення в систему залишкових класів та зворотне перетворення чисел.

Висновки. Досліджено метод реалізації з використанням системи залишкових класів проблемної операції прямого перетворення чисел із позиційної системи числення в систему залишкових класів та зворотне перетворення чисел. На основі запропонованого підходу досягається виконання шуканої операції. Представляється доцільним застосувати запропонований підхід в якості перспективного напрямку досліджень складних операцій в системі залишкових класів.

ЛІТЕРАТУРА

- 1.Акушский И.Я., Юдицкий Д.И. Машинная арифметика в остаточных классах. М.:Советское радио. 1968. 440 с.
2. Кнут Д. Искусство программирования / Д.Кнут. – М.: Диалектика-Вильямс, 2013. – 832 с.
- 3.Лавриненко А.Н., Червяков Н.И. Исследование немодульных операций в системе остаточных классов. *Научные ведомости, Серия История. Политология. Экономика. Информатика*. 2012.№1 (120). Вып.21/1 с.110-122.
- 4.Полисский Ю.Д. Алгоритм выполнения сложных операций в системе остаточных классов с помощью представления чисел в обратных кодах. *Электронное моделирование*. Киев. 2014. №4 Т. 36. С. 117–123

REFERENCES

1. Akushsky I.Ya., Yuditsky D.I. Machine arithmetic in residual classes. M.: Soviet radio. 1968. 440 p.
2. Knut D. The Art of Programming / D.Knut. - M.:Dialectics-Williams, 2013. - 832 p.
3. Lavrinenko A.N., Chervyakov N.I. Study of non-modular operations in the system of residual classes. Scientific sheets, Series History. Political science. Economy. Informatics. 2012. No. 1 (120). Issue 21/1 p.110-122.
4. Polissky Yu.D. An algorithm for performing complex operations in the system of residual classes using the representation of numbers in inverse codes. Electronic modeling. Kyiv. 2014. No. 4 V. 36. S. 117–123.

Received 10.05.2022.

Accepted 12.05.2022.

Algorithms of direct transformation of a position number to the system of residual classes and its inverse transformation

Increasing the speed of computer structures is associated with the involvement of new principles based on the use of the number system of residual classes. When performing a number of computational operations using a non-positional number system of residual classes, the problem of direct conversion of numbers from the positional number system to the number system of residual classes and the reverse conversion of numbers from the number system of residual classes to the positional one is solved. A number of works contain methods for implementing these operations of varying complexity, but their solution is far from perfect. The results of the study indicate the possibility of obtaining a more efficient solution that simplifies the practical implementation of operations for direct conversion of numbers from the positional number system to the number system of residual classes and inverse conversion of numbers. The aim of the study is to analyze the implementation of the operations of

direct conversion of numbers from the positional number system to the number system of residual classes and the reverse conversion of numbers. The tools of the research methodology are system analysis, number theory and the Chinese remainder theorem. The research methodology consists in the analysis of special tables of residues by modules. An algorithm for performing complex operations based on the use of a polyadic code of a number presented in the number system of residual classes is proposed. A simple and efficient approach is proposed using iterative table operations with residuals. For each value of the given residuals, the constants are obtained by a simple selection from the corresponding table. The method underlying the implementation of these complex operations is to sum the chosen constants to the desired value, while the corresponding constants are subtracted from the values of the known remainders until the latter vanishes. The method is algorithmically simple and uncomplicated for circuit implementation, and it should be considered as one of the areas of research to improve the efficiency of computations in the system of residual classes.

Поліський Юрій Давидович - кандидат технічних наук, старший науковий співробітник, Заслужений винахідник України, Науково-дослідний інститут автоматизації чорної металургії (НДІАчормет) м. Дніпро.

Polissky Yuriy Davydovych - Candidate of technical science, senior researcher, Honored Inventor of Ukraine, Research Institute of Automation of Ferrous Metallurgy (NDIACHormet), Dnipro.