

ПЕРЕТВОРЕННЯ У СИСТЕМІ ЗАЛИШКОВИХ КЛАСІВ ЧИСЛА З ОДНІЄЇ СИСТЕМИ МОДУЛІВ В ІНШУ

Анотація. Метою дослідження є аналітичний розгляд системи залишкових класів для реалізації операції перетворення чисел з однієї системи залишкових класів в іншу. Метод. Системний аналіз, теорія чисел і китайська теорема про залишки є інструментами методології дослідження. Метод використовує представлення числа як його залишками, так і в поліадичному коді. Методика базується на визначенні позиційних характеристик для даного модуля на основі отриманих позиційних характеристик для решти модулів вихідної системи з подальшою побудовою на їх основі залишків для модулів шуканої системи. Пропонований спосіб алгоритмічно простий. Результати. Виконано теоретичне обґрунтування розглянутого підходу для отримання ефективного розв'язку операції немодульного перетворення в системі залишкових класів для переходу від представлення числа однією системою модулів до його представлення іншою системою модулів. Показано, що запропонований спосіб забезпечує бажаний результат. На основі запропонованого підходу досягається підвищення ефективності операції перетворення. Наукова новизна. Запропоновано теоретичне обґрунтування представленого підходу до розв'язання операції немодульного перетворення в системі залишкових класів для переходу від представлення числа в одній системі модулів до його представлення в іншій системі модулів. Представляється доцільним застосувати запропонований підхід як перспективний напрямок дослідження складних операцій у системі залишкових класів. Практичне значення. Впливає з важливості теоретичних висновків та отриманих результатів дослідження. Воно базується на тому, що існує достатньо простий та ефективний підхід до вирішення задачі виконання немодульної операції перетворення в системі залишкових класів для переходу від представлення числа в одній системі модулів до його представлення в іншій системі модулів. Розглянуті рішення мають високу швидкість та можуть бути ефективними при розробці модульних обчислювальних структур для перспективних інформаційних технологій.

Ключові слова: залишкові класи; системи модулів; діапазон чисел; перетворення.

Постановка проблеми. Застосування паралельної обробки даних на основі системи залишкових класів (СЗК) [1] дозволяє суттєво підвищити швидкодію операцій обробки даних. СЗК називається система числення, у якій довільне число представляється як набір найменших невід'ємних залишків по модулях $m_1, m_2, \dots, m_n$, тобто $N = (\alpha_1, \alpha_2, \dots, \alpha_n)$. Тут $\alpha_i = N \pmod{m_i}$. При цьому, якщо числа m_i взаємно прості, то такому представленню відповідає лише одне число N діапазону $[0, M)$, де $M = m_1 m_2 \dots m_n$. Нехай системою основ поліадичного коду також є система $m_1, m_2, \dots, m_r$. Число N_1 в поліадичному коді представляється наступним чином

$$N_1 = \pi_1 + \pi_2 m_1 + \dots + \pi_i m_1 m_2 \dots m_{i-1} + \dots + \pi_n m_1 m_2 \dots m_{n-1},$$

де $0 \leq \pi_i \leq m_i - 1, i = 1, 2, \dots, n$.

При обробці даних, представлених в СЗК, часто необхідні проміжні перетворення чисел з однієї системи залишкових класів в іншу [2].

Вирішення такої задачі може знадобитися, наприклад, при розширенні діапазону представлення чисел, відновлення залишку, порівнянні чисел на підставі позиційних характеристик, визначенні рангу числа, модульному діленню чисел у тих випадках, коли здійснюється ділення на число, кратне одному або декільком модулям системи. Тому операція переходу від однієї системи модулів до іншої, при якій за відомими залишками числа в одній СЗК визначають значення залишків цього числа в іншій СЗК, відноситься до однієї з основних немодульних операцій в системі залишкових класів.

Формалізована постановка задачі така.

Нехай є дві СЗК $C1 = \{m_1, m_2, \dots, m_n\}$, $M_1 = m_1 m_2 \dots m_n$,

$C2 = \{p_1, p_2, \dots, p_r\}$, $M_2 = p_1 p_2 \dots p_r$ і число $N = (\alpha_1, \alpha_2, \dots, \alpha_n)$ таке, що

$$N = (\alpha_1, \alpha_2, \dots, \alpha_n) < \min \{M_1, M_2\}.$$

Необхідно для представлення числа $N = (\alpha_1, \alpha_2, \dots, \alpha_n)$ в СЗК $C1$ виконати перетворення на представлення $N = (\beta_1, \beta_2, \dots, \beta_t, \dots, \beta_r)$ цього числа в СЗК $C2$, де $\beta_t = N \pmod{p_t}$, $t = 1, 2, \dots, r$.

Аналіз останніх досліджень і публікацій. Вперше підхід до розв'язання цієї задачі запропонований у класичній роботі [1]. Наступні дослідження, наприклад [2], показали можливість більш економних рішень. Однак алгоритм [2] включає значну кількість різнотипних кроків, що збільшує час реалізації. У роботі [3] наведено рішення, що дозволяє спростити практичну реалізацію та прискорити одержання результату. У цій статті запропоновано ще один підхід, який також спрощує практичну реалізацію та прискорює одержання низки результатів.

Формулювання мети дослідження. Метою дослідження є аналітичний розгляд СЗК для реалізації операцій перетворення чисел з однієї системи залишкових класів в іншу.

Виклад основного матеріалу. Підхід до побудови алгоритму перетворення складається з двох етапів.

На першому етапі визначаються позиційні характеристики $0 \leq \pi_i \leq m_i - 1, i = 1, 2, \dots, n$ числа N в системі $C1$. На другому етапі на підставі отриманих позиційних характеристик формуються залишки $\beta_1, \beta_2, \dots, \beta_r$.

Отже, перший етап:

$$N_1 = \pi_1 + \pi_2 m_1 + \dots + \pi_i m_1 m_2 \dots m_{i-1} + \dots + \pi_n m_1 m_2 \dots m_{n-1}$$

$$\alpha_1 = N_1 \pmod{m_1} = \pi_1, \quad \pi_1 = \alpha_1.$$

На першій ітерації

$$N_2 = N_1 - \pi_1 = \pi_2 m_1 + \dots + \pi_i m_1 m_2 \dots m_{i-1} + \dots + \pi_n m_1 m_2 \dots m_{n-1} =$$

$$= m_1 (\pi_2 + \dots + \pi_i m_2 \dots m_{i-1} + \dots + \pi_n m_2 \dots m_{n-1})$$

$$\pi_2 = \left(\frac{N_2}{m_1} \right) \pmod{m_2}.$$

На другій ітерації

$$N_3 = N_2 - \pi_2 = \pi_3 m_2 + \dots + \pi_i m_2 \dots m_{i-1} + \dots + \pi_n m_2 \dots m_{n-1} =$$

$$= m_2 (\pi_3 + \dots + \pi_i m_3 \dots m_{i-1} + \dots + \pi_n m_3 \dots m_{n-1})$$

$$\pi_3 = \left(\frac{N_3}{m_2} \right) \pmod{m_3}.$$

.....
.....

На i -й ітерації

$$\begin{aligned} N_{i+1} &= N_i - \pi_i = \pi_{i+1} m_i + \dots + \pi_n m_i m_{i+1} \dots m_{n-1} = \\ &= m_i (\pi_{i+1} + \dots + \pi_n m_{i+1} \dots m_{n-1}) \\ \pi_{i+1} &= \left(\frac{N_{i+1}}{m_i} \right) (\bmod m_{i+1}). \end{aligned}$$

На n - й ітерації

$$\begin{aligned} N_n &= N_{n-1} - \pi_{n-1} = \pi_n m_{n-1} \\ \pi_n &= \left(\frac{N_n}{m_{n-1}} \right) (\bmod m_n). \end{aligned}$$

Таким чином, отримано всі позиційні характеристики $0 \leq \pi_i \leq m_i - 1, i = 1, 2, \dots, n$ числа N в системі C_1

Другий етап.

Значення шуканих залишків приймається $\beta_1 = 0, \beta_2 = 0, \dots, \beta_t = 0, \dots, \beta_r = 0$.

На першій ітерації

$$\begin{aligned} \beta_t^1(1) &= (\beta_t^1(0) + \pi_n) (\bmod p_t), \\ \beta_t^1(2) &= (m_{n-1} \beta_t^1(1)) (\bmod p_t). \end{aligned}$$

На другій ітерації

$$\begin{aligned} \beta_t^2(1) &= (\beta_t^1(2) + \pi_{n-1}) (\bmod p_t), \\ \beta_t^2(2) &= (m_{n-2} \beta_t^2(1)) (\bmod p_t). \end{aligned}$$

.....
.....

На r - й ітерації

$$\beta_t^r(1) = (\beta_t^{r-1}(2) + \pi_1) (\bmod p_t).$$

Проілюструємо викладене для переходу від представлення числа $N = 1957 = (4, 7, 10, 1)$ в системі модулів $m_1 = 7, m_2 = 13, m_3 = 11, m_4 = 2$, $M_1 = m_1 m_2 m_3 m_4 = 7 * 13 * 11 * 2 = 2002$ до його представлення в системі модулів $p_1 = 5, p_2 = 17, p_3 = 27$, $M_2 = p_1 p_2 p_3 = 51 * 17 * 27 = 2295$, $M_2 > M_1$. До визначення залишків $\beta_1, \beta_2, \beta_3$ їх початкові значення приймаються $\beta_1 = 0, \beta_2 = 0, \beta_3 = 0$.

Отже, перший етап.

$$\pi_1 = \alpha_1, \pi_1 = (4, 4, 4, 0)_1$$

Тому на першій ітерації згідно з $N_2 = N_1 - \pi_1$ - табл.1 із рядка 4,7,10,1 віднімаємо рядок 4,4,4,0 по модулях $m_1 = 7, m_2 = 13, m_3 = 11, m_4 = 2$. Отримуємо рядок 0,3,6,1, і в подальшому стовбець щодо $m_1 = 7$ вилучаємо із розгляду. Далі згідно з $\pi_2 = (\frac{N_2}{m_1})(\text{mod } m_2)$ виконуємо ділення рядка 3,6,1 по модулях $m_2 = 13, m_3 = 11, m_4 = 2$ на $m_1 = 7$, тобто на рядок 7,7,1. Отримуємо рядок 6,4,1.

Таблиця 1

Число	Модулі				Ітерації
	7	13	11	2	
	Залишки				
1957	4	7	10	1	- = : = - = : = - = : = - =
4	4	4	4	0	
1953	0	3	6	1	
7	x	7	7	1	
279	x	6	4	1	
6	x	6	6	0	
273	x	0	9	1	
13	x	x	2	1	
21	x	x	10	1	
10	x	x	10	0	
11	x	x	0	1	
11	x	x	X	1	
1	x	x	X	1	
1	x	x	X	1	
0	x	x	X	0	

Звідси $\pi_2 = 6$, $\pi_2 = (6, 6, 0)$.

На другій ітерації згідно з $N_3 = N_2 - \pi_2$ - табл.1 із рядка 6,4,1 віднімаємо рядок 6,6,0 по модулях $m_2 = 13, m_3 = 11, m_4 = 2$. Отримуємо рядок 0,9,1, і в подальшому стовбець щодо $m_2 = 13$ теж вилучаємо із розгляду. Далі згідно з $\pi_3 = (\frac{N_3}{m_2})(\text{mod } m_3)$ виконуємо ділення рядка 9,1 по модулях $m_3 = 11, m_4 = 2$ на $m_2 = 13$, тобто на рядок 2,1. Отримуємо рядок 10,1.

Звідси $\pi_3 = 10$, $\pi_3 = (10, 0)$.

На третій ітерації згідно з $N_4 = N_3 - \pi_3$ - табл.1 із рядка 10,1 віднімаємо рядок 10,0 по модулях $m_3 = 11, m_4 = 2$. Отримуємо рядок 0,1, і в подальшому стовбець щодо $m_3 = 11$ теж вилучаємо із розгляду. Далі згідно з $\pi_4 = (\frac{N_4}{m_3})(\text{mod } m_4)$ виконуємо ділення рядка 1 по модулю $m_4 = 2$ на $m_3 = 11$, тобто на рядок 1. Отримуємо рядок 1.

Звідси $\pi_4 = 1$, $\pi_4 = (1)$.

Другий етап ілюструється табл.2.

Таблиця 2

Число	Модулі			Ітерації
	5	17	27	
	Залишки			
0	0	0	0	
1	1	1	1	+
1	1	1	1	=
11	1	11	11	*
11	1	11	11	=
10	0	10	10	+
21	1	4	21	=
13	3	13	13	*
273	3	1	3	=
6	1	6	6	+
279	4	7	9	=
7	2	7	7	*
1953	3	15	9	=
4	4	4	4	+
1957	2	2	13	=

Перша ітерація.

До стрічки $\beta_1(0)$, тобто $\beta_1 = 0, \beta_2 = 0, \beta_3 = 0$, додаємо $\pi_4 = 1$ та отримуємо суму $\beta^1(1) = 1, 1, 1$ по модулях $p_1 = 5, p_2 = 17, p_3 = 27$. Отриману суму множимо на

$m_3 = 11$ по тих же модулях $p_1 = 5, p_2 = 17, p_3 = 27$ та отримуємо стрічку $\beta^1(2) = 1, 11, 11$.

Друга ітерація.

До стрічки $\beta^1(2) = 1, 11, 11$ додаємо $\pi_3 = 10$ та отримуємо суму $\beta^2(1) = 1, 4, 21$ по модулях $p_1 = 5, p_2 = 17, p_3 = 27$. Отриману суму множимо на $m_2 = 13$ по тих же модулях $p_1 = 5, p_2 = 17, p_3 = 27$ та отримуємо стрічку $\beta^2(2) = 3, 11, 3$.

Третя ітерація.

До стрічки $\beta^2(2) = 3, 11, 3$ додаємо $\pi_2 = 6$ та отримуємо суму $\beta^3(1) = 4, 7, 9$ по модулях $p_1 = 5, p_2 = 17, p_3 = 27$. Отриману суму множимо на $m_1 = 7$ по тих же модулях $p_1 = 5, p_2 = 17, p_3 = 27$ та отримуємо стрічку $\beta^3(2) = 3, 15, 9$.

Четверта ітерація.

До стрічки $\beta^3(2) = 3, 15, 9$ додаємо $\pi_1 = 4$ та отримуємо суму $\beta^4(1) = 2, 2, 13$ по модулях $p_1 = 5, p_2 = 17, p_3 = 27$. Отже, отримано число $N = 1957 = (2, 2, 13)$.

Таким чином, розглянутий алгоритм забезпечує перетворення представлення чисел у системах залишкових класів.

Висновки. Досліджено метод реалізації в системі залишкових класів проблемної операції переходу від представлення числа однією системою модулів до його представлення іншою системою модулів. Підхід базується на визначенні залишків за модулями вхідної системи на основі отриманих залишків по модулях вихідної системи. Показано, що запропонований метод забезпечує отримання шуканого результату. На основі запропонованого підходу досягається підвищення швидкодії виконання операції перетворення. 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.Магомедов Ш.Г, Преобразование представлений чисел в модулярной арифметике в системах остаточных классов с разными основаниями. Вестник АГТУ. Сер.: Управление, вычислительная техника и информатика. Махачкала. 2014. № 4. С.32-39.

3.Полисский Ю.Д. О преобразовании представлений чисел в остатках из одной системы модулей в другую // Наука та прогрес транспорту. Вісник Дніпропетровського національного університету залізничного транспорту, 2016, № 3 (63) С. 130-137.

REFERENCES

- 1.Akushsky I.Ya., Yuditsky D.I. Machine arithmetic in residual classes. M.: Soviet radio. 1968. 440 p.
- 2.Magomedov Sh.G. Transformation of representations of numbers in modular arithmetic in systems of residual classes with different bases. Bulletin of ASTU. Ser.: Management, computer technology and informatics. Makhachkala. 2014. No. 4. P.32-39.
- 3.Polissky Yu.D. On the transformation of representations of numbers in remainders from one system of modules to another // Science and progress of transport. Bulletin of the Dnipropetrovsk National University of Railway Transport, 2016, No. 3 (63), P. 130-137.

Received 14.04.2023.

Accepted 19.04.2023.

Transformation in the system of residual number classes from one system of modules to another

The purpose of the study. The purpose of the study is an analytical consideration of the system of residual classes for the implementation of the operation of converting numbers from one system of residual classes to another. Method. System analysis, number theory, and the Chinese remainder theorem are tools of the research methodology. The method uses the representation of the number both by its remainders and in the polyadic code. The methodology is based on determining the positional characteristics for this module on the basis of the received positional characteristics for the remaining modules of the original system, with the subsequent construction on their basis of the residuals for the modules of the sought system. The proposed method is algorithmically simple. The results. The theoretical substantiation of the considered approach to obtain an effective solution of the non-modular transformation operation in the system of residual classes for the transition from the representation of a number by one system of modules to its representation by another system of modules is performed. It is shown that the proposed method provides the desired result. On the basis of the proposed approach, an increase in the performance of the conversion operation is achieved. Scientific novelty. The theoretical justification of the presented approach to the solution of the non-modular transformation operation in the system of residual classes

for the transition from the representation of a number in one system of modules to its representation in another system of modules is proposed. It seems appropriate to apply the proposed approach as a prospective direction of research of complex operations in the system of residual classes. Practical significance. It follows from the importance of theoretical conclusions and obtained research results. It is based on the fact that there is a reasonably simple and effective approach to solving the problem of performing a non-modular conversion operation in the system of residual classes for the transition from the representation of a number in one system of modules to its representation in another system of modules. The considered solutions have high speed and can be effective in the development of modular computing structures for promising information technologies.

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).