УДК 681.04 DOI: 10.31319/2519-8106.1(38)2018.128944
Ю.Д. Поліський, к.т.н., polissky477@gmail.com
НДІ автоматизації чорної металургії, м. Дніпро

РЕАЛІЗАЦІЯ ДЕЯКИХ ПРОБЛЕМНИХ ОПЕРАЦІЙ У СИСТЕМАХ ЗАЛИШКОВИХ КЛАСІВ

В роботі досліджені системи залишкових класів з попарно взаємно простими модулями і системи залишкових класів з усіма парними модулями з можливістю реалізації базових проблемних операцій визначення приналежності числа до даної половині діапазону і порівняння чисел.
Ключові слова: *залишкові класи, проблемні операції, модулі, порівняння чисел.*

Systems of residual classes with pairwise mutually simple modules and systems of residual classes with all even modules are investigated with the possibility of implementing basic problem operations for determining the number of a given half of the range and comparing numbers.
Keywords: *residual classes, problem operations, modules, comparison of numbers.*

Постановка проблеми

До обчислювальних структур постійно пред'являються вимоги підвищення швидкодії. Застосування системи залишкових класів (СЗК) з попарно взаємно простими модулями дозволяє підвищити продуктивність таких систем за рахунок природного розпаралелювання обробки даних. Останнім часом для реалізації деяких проблемних операцій запропоновані рішення [1], в яких поряд з використанням систем попарно взаємно простих модулів застосовуються також і системи, в яких модулі не є взаємно простими, зокрема — всі парні. При значних перевагах СЗК застосування цих систем наштовхується на певні труднощі.

Аналіз останніх досліджень і публікацій

Переваги СЗК детально викладені в [2,3,4]. Однак виникають складності [5] при реалізації проблемних базових операцій визначення приналежності числа до даної половині діапазону і порівняння чисел.

Формулювання мети дослідження

Метою дослідження є аналітичний розгляд СЗК з попарно взаємно простими модулями і СЗК з усіма парними модулями для реалізації базових проблемних операцій визначення приналежності числа до даної половині діапазону і порівняння чисел.

Виклад основного матеріалу

Під СЗК [6] розуміють систему числення, в якій довільне число N представляється у вигляді набору найменших невід'ємних залишків по модулях m_1, m_2,..., m_n, тобто $N=(\alpha_1,\alpha_2,...,\alpha_n)$. Тут $\alpha_i = N(\mathrm{mod}\, m_i)$. При цьому, якщо числа m_i попарно взаємно прості, то такому представленню відповідає тільки одне число N діапазону $[0, M)$, де $M = m_1 m_2 ... m_n$.

Якщо системою модулів поліадичного коду також є система m_1, m_2,..., m_n, число N в поліадичному коді представляється у вигляді

$$N = \pi_1 + \pi_2 m_1 + ... + \pi_i m_1 m_2 ... m_{i-1} + ... + \pi_{n-1} m_1 m_2 ... m_{n-2} + \pi_n m_1 m_2 ... m_{n-1},$$

де $0 \le \pi_i \le m_i - 1$.

Покажемо, що таке представлення є єдиним.

Нехай $\widetilde{N} = \widetilde{N}_1 + \widetilde{N}_2$, де $\widetilde{N}_1 = \pi_1 + \pi_2 m_1 + ... + \pi_{i-1} m_1 m_2 ... m_{i-2}$, $\widetilde{N}_2 = \pi_i m_1 m_2 ... m_{i-1}$.

Нехай число $\widetilde{N}_1$ збільшилося на величину Δ. Для того, щоб представлення числа N в поліадичному коді при цьому не змінилося, необхідно, щоб число $\widetilde{N}_2$ зменшилося на ту ж величину Δ.

Нехай в результаті збільшення числа $\tilde{N}_1$ отримано найбільше значення $\tilde{N}_{1,\max} = m_1 m_2 ... m_{i-1} - 1$, яке досягається при $\pi_t = m_t - 1$, $t = 1,2,...,(i-1)$.

Нехай в результаті зменшення числа $\tilde{N}_2$ отримано найменше значення $\tilde{N}_{2,\min} = m_1 m_2 ... m_{i-1}$, яке досягається при $\pi_i = 1$.

Оскільки $\tilde{N}_{1,\max} < \tilde{N}_{2,\min}$, наведене вище представлення числа N в поліадичному коді є єдиним.

Однією з ключових складних операцій СЗК є операція визначення приналежності числа до першої $R1$ або другої $R2$ половині діапазону.

В роботі [7] доведено, що при представленні числа N в поліадичному коді, яке для попарно взаємно простих чисел m_i є єдиним, критерієм приналежності числа до даної половині діапазону служить значення π_n

$$N \in \begin{cases} R1, & 0 \le \pi_n \le \dfrac{m_n}{2} - 1 \\ R2, & \dfrac{m_n}{2} \le \pi_n \le m_n - 1 \end{cases}$$

Знання про приналежність числа до даної половині діапазону дозволяє вирішити задачу порівняння чисел.

Нехай $N_1 = (\alpha_1, \alpha_2, ..., \alpha_{n-j})$ і $N_2 = (\beta_1, \beta_2, ..., \beta_{n-j})$ — порівнювані числа, $N_1 \ne N_2$, та $\Delta = N_1 - N_2$ — різниця чисел N_1 і N_2.

Необхідно визначити результат

$$\Re = \begin{cases} \Re_1, N_1 > N_2 \\ \Re_2, N_1 < N_2 \end{cases}$$

Порівняння чисел N_1 і N_2 виконується відповідно до алгоритму

$$\Re_1 = \begin{cases} N_1 > N_2, (N_1 \in R2 \cap N_2 \in R1) \cup (N_1, N_2 \in R1 \cup N_1, N_2 \in R2) \cap \Delta \in R1) \\ N_1 < N_2, N_1 \in R1 \cap N_2 \in R2 \cup (N_1, N_2 \in R1 \cup N_1, N_2 \in R2) \cap \Delta \in R2) \end{cases}$$

Ефективний алгоритм порівняння чисел, не пов'язаний з визначенням належності числа до даної половині діапазону [8], полягає в наступному.

Якщо після $(j-1)$-й ітерації ($j = 1,2,\ldots,n-1$) результат порівняння не отримано, виконується j-я ітерація для діапазону $\left[0, M^{j-1}\right)$, де $M^{j-1} = m_1 m_2 \ldots m_{n-(j-1)}$.

$$\tilde{\alpha}_i^j = \left(\tilde{\alpha}_i^{j-1} - \tilde{\alpha}_{n-(j-1)}^{j-1}\right) (\mathrm{mod}\, m_i), \quad i = 1,2,\ldots,n-(j-1),$$

$$\tilde{\beta}_i^j = \left(\tilde{\beta}_i^{j-1} - \tilde{\beta}_{n-(j-1)}^{j-1}\right) (\mathrm{mod}\, m_i), \quad i = 1,2,\ldots,n-(j-1).$$

Нехай

$$\tilde{N}_1{}^j = \left(\tilde{\alpha}_1{}^j, \tilde{\alpha}_2{}^j, \ldots, \tilde{\alpha}_{n-j}^j\right),$$

$$\tilde{N}_2{}^j = \left(\tilde{\beta}_1^j, \tilde{\beta}_2^j, \ldots, \tilde{\beta}_{n-j}^j\right).$$

$$\Re = \begin{cases} N_1 > N_2, \left(\tilde{N}_1{}^j = \tilde{N}_2{}^j\right) \cap \left(\tilde{\alpha}_n^{j-1} > \tilde{\beta}_n{}^{j-1}\right) \\ N_1 < N_2, \left(\tilde{N}_1{}^j = \tilde{N}_2{}^j\right) \cap \left(\tilde{\alpha}_n^{j-1} < \tilde{\beta}_n{}^{j-1}\right) \end{cases}$$

Якщо $\tilde{N}_1{}^j \neq \tilde{N}_2{}^j$, виконується $(j+1)$-я ітерація для діапазону $\left[0, M^j\right)$, де $M^j = m_1 m_2 \dots m_{n-j}$. Для цього приймаємо $\tilde{N}_1{}^{1,j} = \frac{\tilde{N}_1{}^j}{m^{n-(j-1)}}$ та $\tilde{N}_2{}^{1,j} = \frac{\tilde{N}_2{}^j}{m^{n-(j-1)}}$ в якості порівнюваних чисел.

Якщо результат порівняння не отримано до $(n-1)$-й ітерації, то після її виконання

$$\Re = \begin{cases} N_1 > N_2, \left(\left(\tilde{N}_1{}^{1,n-1} = \tilde{N}_2{}^{1,n-1}\right) \cap \left(\tilde{\alpha}_1^{1,n-2} > \tilde{\beta}_1^{1,n-2}\right)\right) \cup \\ \cup \left(\left(\tilde{N}_1{}^{1,n-1} \neq \tilde{N}_2{}^{1,n-1}\right) \cap \left(\tilde{\alpha}_1^{1,n-1} > \tilde{\beta}_1^{1,n-1}\right)\right), \\ N_1 < N_2, \left(\left(\tilde{N}_1{}^{1,n-1} = \tilde{N}_2{}^{1,n-1}\right) \cap \left(\tilde{\alpha}_1^{1,n-2} < \tilde{\beta}_1^{1,n-2}\right)\right) \cup \\ \cup \left(\left(\tilde{N}_1{}^{1,n-1} \neq \tilde{N}_2{}^{1,n-1}\right) \cap \left(\tilde{\alpha}_1^{1,n-1} < \tilde{\beta}_1^{1,n-1}\right)\right) \end{cases}$$

В СЗК з використанням систем модулів, які не є взаємно простими, зокрема — з усіма парними модулями, представленню $N = (\alpha_1, \alpha_2, ..., \alpha_n)$ відповідають кілька чисел діапазону $[0, M)$.

Величина M, що дорівнює добутку m_1, m_2, ..., m_n в системі взаємно простих модулів m_i, є, по суті, найменшим спільним кратним цих модулів, тобто $M = m_1 m_2 ... m_n = \langle m_1, m_2, ..., m_n \rangle$. Якщо поняття величини M як найменшого спільного кратного поширити на систему модулів, які не є взаємно простими, то і в цьому випадку кожному числу з $\left[0, \hat{M}\right)$ відповідатиме єдиний набір $\hat{N} = (\hat{\alpha}_1, \hat{\alpha}_2, ..., \hat{\alpha}_n)$. При такому узагальненні число N в поліадичному коді для тієї ж системи модулів, які не є взаємно простими, представляється у вигляді

$$\hat{N} = \pi_1 + \pi_2 \langle m_1 \rangle + ... + \pi_i \langle m_1, m_2, ..., m_{i-1} \rangle + ... + \pi_n \langle m_1, m_2, ..., m_{n-1} \rangle,\ 0 \le \pi_i \le m_i - 1,\ i = 1, 2, \dots, n.$$

Покажемо, що при всіх парних модулях таке уявлення числа в поліадичному коді не є єдиним.

Нехай $\hat{N} = \left(\hat{\alpha}_1, \hat{\alpha}_2, \dots, \hat{\alpha}_n\right)$.

Виконаємо операцію $\hat{N}(i) = \hat{\alpha}_i - \hat{\alpha}_1$, $i = 1, 2, \dots, n$.

Тоді $\hat{N}(i)$ стає кратним m_1 так само, як і $\langle m_1, m_2, ..., m_{i-1} \rangle$ за визначенням.

Нехай $\hat{N}(i) = \left\langle m_1, m_2, \dots, m_{i-1} \right\rangle$. Оскільки відповідно до табл.1 найбільше значення $\pi_{i-1} = m_{i-1} - 1$, а $\theta = \frac{\left\langle m_1, m_2, \dots, m_{i-1} \right\rangle}{\left\langle m_1, m_2, \dots, m_{i-2} \right\rangle} \le m_{i-1}$, число $\hat{N}(i) = \left\langle m_1, m_2, \dots, m_{i-1} \right\rangle$ може бути отримано так само, як $\pi_{i-1} \left\langle m_1, m_2, \dots, m_{i-2} \right\rangle$ при відповідному виборі π_{i-1}. Таким чином, при всіх парних модулях представлення числа в поліадичному коді не є єдиним.

Таблиця 1

m_1	…	m_{i-1}	m_i	…	m_n
$0 \le \pi_1 \le m_1 - 1$	…	$m_{i-2} \le \pi_{i-1} \le m_{i-1} - 1$	$m_{i-1} \le \pi_i \le m_i - 1$	…	$m_{n-1} \le \pi_n \le m_n - 1$
1	…	$\pi_{i-1} \langle m_1, m_2, ..., m_{i-2} \rangle$	$\pi_i \langle m_1, m_2, ..., m_{i-1} \rangle$	…	$\pi_n \langle m_1, m_2, ..., m_{n-1} \rangle$

Наприклад, в системі модулів $m_1=10, m_2=6, m_3=14, m_4=22$ при $\pi_1=0, \pi_2=2, \pi_3=3, \pi_4=8$ представлення числа $N=1790$ в поліадичному коді має вигляд $N=1790=0+2\langle 10\rangle+3\langle 10,6\rangle+8\langle 10,6,14\rangle$, при $\pi_1=0, \pi_2=2, \pi_3=10, \pi_4=7$ представлення того ж числа $N=1790$ в поліадичному коді має вигляд $N=1790=0+2\langle 10\rangle+10\langle 10,6\rangle+7\langle 10,6,14\rangle$.

Звідси випливає, що пошук критерію для визначення приналежності числа до першої або другої половини діапазону стає одним із напрямків дослідження СЗК з усіма парними модулями.

Реалізація операції порівняння чисел $\hat{N}_1=\left(\hat{\alpha}_1,\hat{\alpha}_2,\ldots,\hat{\alpha}_{n-j}\right)$ і $\hat{N}_2=\left(\hat{\beta}_1,\hat{\beta}_2,\ldots,\hat{\beta}_{n-j}\right)$ при всіх парних модулях по другому з наведених вище алгоритмів досягається таким підбором модулів, при якому $\theta_{i-1}=\dfrac{\langle m_1,m_2,\ldots,m_i\rangle}{\langle m_1,m_2,\ldots,m_{i-1}\rangle}$ — число непарне, і кожна пара чисел $\lambda_1=\theta_{i-1},m_1,\ \lambda_2=\theta_{i-1},m_2,\ldots,\lambda_{i-1}=\theta_{i-1},m_{i-1}$ — числа взаємно прості.

Приклад порівняння пари чисел $N_1=532$, $N_2=1828$ при $m_1=10, m_2=6, m_3=14, m_4=22$ представлений в табл.2. Тут

$$\theta_1=\frac{\langle m_1,m_2\rangle}{\langle m_1\rangle}=\frac{\langle 10,6\rangle}{\langle 10\rangle}=3.$$

$$\theta_2=\frac{\langle m_1,m_2,m_3\rangle}{\langle m_1,m_2\rangle}=\frac{\langle 10,6,14\rangle}{\langle 10,6\rangle}=7.$$

$$\theta_3=\frac{\langle m_1,m_2,m_3,m_4\rangle}{\langle m_1,m_2,m_3\rangle}=\frac{\langle 10,6,14,22\rangle}{\langle 10,6,14\rangle}=11.$$

Таблиця 2

Модулі	10	6	14	22	Модулі	10	6	14
Порівнювані числа	Залишки				Наведені числа	Наведені залишки		
						$\tilde{\alpha}_i^1=(\alpha_i-\alpha_4)(\mathrm{mod}\ m_i)$		
						$\tilde{\beta}_i^1=(\beta_i-\beta_4)(\mathrm{mod}\ m_i)$		
	α_1	α_2	α_3	α_4		$\tilde{\alpha}_1^1$	$\tilde{\alpha}_2^1$	$\tilde{\alpha}_3^1$
	β_1	β_2	β_3	β_4		$\tilde{\beta}_1^1$	$\tilde{\beta}_2^1$	$\tilde{\beta}_3^1$
$N^1{}_1=532$	2	4	0	4	$\tilde{N}_1^1$	8	0	10
$N^1{}_2=1828$	8	4	8	2	$\tilde{N}_2^1$	6	2	6

Оскільки $\tilde{N}_1^1(8,0,10) \neq \tilde{N}_2^1(6,2,6)$, приймаємо для другої ітерації $N^2{}_1 = \frac{\tilde{N}_1^1}{\theta_3}$ і $N^2{}_2 = \frac{\tilde{N}_2^1}{\theta_3}$ в якості порівнюваємих чисел.

Таблиця 3

Модулі	10	6	14	Модулі	10	6
Порівнювані числа	Залишки			Наведені числа	Наведені залишки	
					$\tilde{\alpha}_i^2 = \left(\tilde{\alpha}_i^1 - \tilde{\alpha}_3^1\right) (\text{mod } m_i)$	
					$\tilde{\beta}_i^2 = \left(\tilde{\beta}_i^1 - \tilde{\beta}_3^1\right) (\text{mod } m_i)$	
	$\tilde{\alpha}_1^1$	$\tilde{\alpha}_2^1$	$\tilde{\alpha}_3^1$		$\tilde{\alpha}_1^2$	$\tilde{\alpha}_2^2$
	$\tilde{\beta}_1^1$	$\tilde{\beta}_2^1$	$\tilde{\beta}_3^1$		$\tilde{\beta}_1{}^2$	$\tilde{\beta}_2{}^2$
$N^2{}_1$	8	0	6	$\tilde{N}_1^2$	2	0
$N^2{}_2$	6	4	12	$\tilde{N}_2^2$	4	4

Оскільки $\tilde{N}_1^2(2,0) \neq \tilde{N}_2^2(4,4)$, приймаємо для третьої ітерації $N^3{}_1 = \frac{\tilde{N}_1^2}{\theta_2}$ і $N^3{}_2 = \frac{\tilde{N}_2^2}{\theta_2}$ в якості порівнюваємих чисел.

Таблиця 4

Модулі	10	6	Модулі	10
Порівнювані числа	Залишки		Наведені числа	Наведені залишки
				$\tilde{\alpha}_i^3 = \left(\tilde{\alpha}_i^2 - \tilde{\alpha}_2^2\right) (\text{mod } m_i)$
				$\tilde{\beta}_i^3 = \left(\tilde{\beta}_i^2 - \tilde{\beta}_2^2\right) (\text{mod } m_i)$
	$\tilde{\alpha}_1^2$	$\tilde{\alpha}_2^2$		$\tilde{\alpha}_1^3$
	$\tilde{\beta}_1{}^2$	$\tilde{\beta}_2{}^2$		$\tilde{\beta}_1{}^3$
$N^3{}_1$	6	0	$\tilde{N}_1^3$	6
$N^3{}_2$	2	4	$\tilde{N}_2^3$	8

Оскільки $\tilde{N}_1^3(6) \neq \tilde{N}_2^3(8)$, приймаємо для четвертої ітерації $N^4{}_1 = \frac{\tilde{N}_1^3}{\theta_1}$ і $N^4{}_2 = \frac{\tilde{N}_2^3}{\theta_1}$ в якості порівнюваємих чисел.

Таблиця 5

Модулі	10
Порівнювані числа	Залишки
	$\tilde{\alpha}_1^4$
	$\tilde{\beta}_1^4$
$N^4{}_1$	2
$N^4{}_2$	6

Оскільки $\tilde{\alpha}_1^4(2) < \tilde{\beta}_{12}^4(6)$, $N_1(2,4,0,4) < N_2(8,4,8,2)$.

Висновки

Досліджено системи залишкових класів з попарно взаємно простими модулями і системи залишкових класів з усіма парними модулями. Показано, що представлення чисел в поліадичному коді в першому випадку є єдиним. Це дозволяє реалізувати базову проблемну операцію визначення приналежності числа до даної половині діапазону і на її основі - операцію порівняння чисел. Показано також, що представлення чисел в другому випадку не є єдиним, в зв'язку з чим пошук рішення розглянутих вище базових проблемних операцій вимагає подальших досліджень.

Список використаної літератури

1. Полисский Ю.Д. Алгоритм табличной реализации модульного возведения в степень / /Ю.Д. Полисский // Проблеми математичного моделювання: матеріали наук.-метод. конф., 25–27 трав. 2016 р. – Дніпропетровськ. – 2016. – С. 96–100.
2. Ирхин В.П. Табличная реализация операций модулярной арифметики / В.П.Ирхин // 50 лет модулярной арифметики: тр. юбилейной Междунар. научно-техн. конф. (23.11.–25.11. 2005). – Москва: МИЭТ. – С. 268–273.
3. Методы и алгоритмы округления, масштабирования и деления чисел в модулярной арифметике / Н.И.Червяков [и др.] // 50 лет модуляр. арифметики : тр. юбилейной Междунар. научно-техн. конф. (23.11.–25.11.2005). – Москва : МИЭТ. – С. 291–310.
4. Червяков Н.И. Методы и принципы построения модулярных нейрокомпьютеров / Н.И. Червяков // 50 лет модулярной арифметики : тр. юбилейной Междунар. научно-техн. конф. (23.11.–25.11.2005). – Москва : МИЭТ. – С. 232–242.
5. Кнут,Д. Искусство программирования / Д.Кнут. – Москва : Диалектика-Вильямс, 2013. – 832 с.
6. Акушский И.Я., Юдицкий Д.И. Машинная арифметика в остаточных классах. [Текст] / И.Я Акушский., Д.И. Юдицкий. – М.: Советское радио, 1968. – 440 с.
7. Полисский Ю.Д. Определение принадлежности числа, представленного системой остаточных классов, данной половине диапазона /Ю.Д.Полисский //Проблеми математичного моделювання: матеріали наук.-метод. конф., 24–26 трав. 2017 м.Дніпропетровськ. – 2017. – С. 112–114.
8. Полисский Ю.Д. О некоторых подходах к выполнению проблемных операций в системе остаточных классов. [Текст] /Ю.Д.Полисский // Электронное моделирование.– 2017. – Т. 39. – № 4.– С. 105–114.