DOI:
УДК 681.04
Ю.Д. Поліський, к.т.н., polissky477@gmail.com
НДІ автоматизації чорної металургії, м. Дніпро

ПРО КВАДРАТНЕ КОРІННЯ В СИСТЕМІ ЗАЛИШКОВИХ КЛАСІВ

В роботі досліджено систему залишкових класів щодо можливості реалізації немодульної операції знаходження квадратного кореня по модулю.
***Ключові слова**: залишкові класи; системи модулів; діапазон чисел; квадратний корінь, ранг числа.*

The system of residual classes on the possibility of realization of a nonmodular operation of finding the square root by modulus is investigated in the work.
***Keywords**: residual classes; module systems; range of numbers; square root; number rank.*

Постановка проблеми

Система числення залишкових класів (СЗК) — це система, в якій довільне число представлено у вигляді набору найменших невід'ємних залишків по модулях $m_1, m_2, \ldots, m_n$, тобто $N = (\alpha_1, \alpha_2, \ldots, \alpha_n)$. Тут $\alpha_i = N(\mathrm{mod}\, m_i)$. При цьому, якщо числа m_i взаємно прості, то такому представленню відповідає тільки одне число N в діапазоні $[0, M)$, де $M = m_1 m_2 \ldots m_n$.

Переваги та недоліки СЗК детально розглянуті в класичній роботі [1]. До переваг СЗК, зокрема, відносяться мала розрядність залишків, висока точність і надійність, здатність системи до самокорекції. Недоліки обумовлені труднощами при реалізації немодульних операцій. У багатьох обчислювальних завданнях, що виконуються в СЗК, однією з найбільш трудомістких немодульних операцій є операція знаходження квадратного кореня по модулю.

Аналіз останніх досліджень і публікацій

У ряді робіт, наприклад [2, 3] запропоновані різні за складністю методи реалізації даної операції, однак, розв'язання її далеке від досконалості. Результати виконаних досліджень свідчать про можливість отримання більш ефективного рішення, яке дозволяє дещо спростити практичну реалізацію операції знаходження квадратного кореня по модулю.

Формулювання мети дослідження

Метою дослідження є аналітичний розгляд СЗК для реалізації немодульної операції знаходження квадратного кореня по модулю.

Виклад основного матеріалу

Нехай N_1, $m > N_1 \geq 0$. Тоді квадратним коренем із числа N_1 по модулю m називається таке число N_2, $m > N_2 \geq 0$, під час зведення якого у квадрат отримуємо число N_1, тобто, $N_1 = N_2^{\,2}(\mathrm{mod}\, m)$. Так, наприклад, при $m = 13$ для $N_2 = 3$ $N_1 = 3^2(\mathrm{mod}\, 13) = 9$ і для $N_2 = 10$ $N_1 = 10^2(\mathrm{mod}\, 13) = 9$.

Нехай $\alpha_k = N_k(\mathrm{mod}\, m)$ і $\alpha_{k+\Delta} = N_{k+\Delta}(\mathrm{mod}\, m) = \alpha_k + \Delta$, де $\Delta = 1, 2, \ldots, m-1$ залишки чисел N_k і $N_{k+\Delta}$ за модулем m такі, що залишки квадратів цих чисел за модулем m рівні. Тоді можна записати $\alpha^2_{k+\Delta} - \alpha^2_k = \alpha^2_k + 2\alpha_k\Delta + \Delta^2 - \alpha^2_k = \lambda m$, де λ — ранг числа.

Звідси $\alpha_k = \dfrac{\lambda m - \Delta^2}{2\Delta}$.

Наприклад, для $m = 13$ при $\Delta = 1$, $\lambda = 1$ отримуємо $\alpha_k = 6$ і $\alpha_{k+\Delta} = 7$.

У табл. 1, табл. 2, табл.3 представлені значення α_k і $\alpha_{k+\Delta}$ за різних Δ і λ для $m = 13$, $m = 7$ і $m = 11$ відповідно.

Таблиця 1

$m=13$						
Δ	λ	α_k	r_k	$\alpha_{k+\Delta}$	$r_{k+\Delta}$	$\alpha^2{}_k \pmod m = \alpha^2{}_{k+\Delta} \pmod m$
1	1	6	2	7	3	10
3	3	5	1	8	4	12
5	5	4	1	9	6	3
7	7	3	0	10	7	9
9	9	2	0	11	9	4
11	11	1	0	12	11	1

Таблиця 2

$m=7$						
Δ	λ	α_k	r_k	$\alpha_{k+\Delta}$	$r_{k+\Delta}$	$\alpha^2{}_k \pmod m = \alpha^2{}_{k+\Delta} \pmod m$
1	1	3	1	4	2	2
3	3	2	0	5	3	4
5	5	1	0	6	5	1

Таблиця 3

$m=11$						
Δ	λ	α_k	r_k	$\alpha_{k+\Delta}$	$r_{k+\Delta}$	$\alpha^2{}_k \pmod m = \alpha^2{}_{k+\Delta} \pmod m$
1	1	5	2	6	3	3
3	3	4	1	7	4	5
5	5	3	0	8	5	9
7	7	2	0	9	7	4
9	9	1	0	10	9	1

Аналіз табл. 4, табл. 5, табл. 6, побудованих на підставі табл. 1, табл. 2, табл. 3 відповідно, показує, що по кожному модулю для деяких чисел від 1 до $m-1$ відсутні корені, а інші числа мають по два квадратного кореня. Звідси, для n — модульного числа, що має квадратне коріння, їх кількість $g=2^n$.

Розглянемо, знаходження квадратного коріння, наприклад, числа, що має залишки $\beta_1=9, \beta_2=4, \beta_3=3$ у системі модулів $m_1=13, m_2=7, m_3=11$.

Із табл. 4 для залишку $\beta_1=9$ вибираємо $\gamma_{1,1}=3$, $\gamma_{1,2}=10$. Із табл. 5 для залишку $\beta_2=4$ вибираємо $\gamma_{2,1}=2$, $\gamma_{2,2}=5$. Із табл. 6 для залишку $\beta_3=3$ вибираємо $\gamma_{3,1}=5$, $\gamma_{3,2}=6$

Отже, числа із залишками $\beta_1=9, \beta_2=4, \beta_3=3$ в системі модулів $m_1=13, m_2=7, m_3=11$ мають $g=2^3=8$ корені:

$$s_1=16=(3,2,5),\ s_2=380=(3,2,6),\ s_3=159=(3,5,5),\ s_4=523=(3,5,6),$$
$$s_5=478=(10,2,5),\ s_6=842=(10,2,6),\ s_7=621=(10,5,5),\ s_8=985=(10,5,6).$$

Таблиця 4

$m=13$		
Залишки		
Число	Перший корінь	Другий корінь
1	1	12
2	---	---
3	4	9
4	2	11
5	---	---
6	---	---
7	---	---
8	---	---
9	3	10
10	6	7
11	---	---
12	5	8

Таблиця 5

$m=7$		
Залишки		
Число	Перший корінь	Другий корінь
1	1	6
2	3	4
3	---	---
4	2	5
5	---	---
6	---	---

Таблиця 6

$m=11$		
Залишки		
Число	Перший корінь	Другий корінь
1	1	10
2	---	---
3	5	6
4	2	9
5	4	7
6	---	---
7	---	---
8	---	---
9	3	8
10	---	---

Пояснюється це різними рангами [4] чисел з однаковими залишками $\beta_1=9, \beta_2=4, \beta_3=3$.

Таким чином, на наступному етапі виникає завдання визначити який із цих коренів є коренем саме числа S_0, ранг якого λ_t.

Позначимо $\Re=\sqrt{(\lambda+1)M}\downarrow$ — найближче менше до $\sqrt{(\lambda+1)M}$ ціле число. Нехай $\Re(\lambda_{t-1})$ для λ_{t-1} та $\Re(\lambda_t)$ для λ_t. Тоді, якщо виконується умова $\Re(\lambda_{t-1})<s_j\le\Re(\lambda_t)$ [5], саме цей корінь є шуканим коренем. Для числа з нульовим рангом $0<s_j\le\sqrt{M}\downarrow$.

Нехай за даною методикою треба визначити який із наведених вище коренів є коренем числа, залишки якого $\beta_1=9, \beta_2=4, \beta_3=3$ та ранг $\lambda_t=273$.

Для даного рангу $\Re(\lambda_{t-1})=522$ та $\Re(\lambda_t)=523$. Перевіряємо послідовно, починаючи з $s_1=16=(3,2,5)$, виконання умови $\Re(\lambda_{t-1})<s_j\le\Re(\lambda_t)$. Ця умова виконується лише для $s_4=523=(3,5,6)$. Отже, $s_4=523=(3,5,6)$ і є коренем числа.

Оцінимо часові витрати.

В найгіршому випадку досягнення результату вимагає $g-1$ ітерацій.

Однак у реальних процесах параметри описуються числами, розподіленими випадковим чином. Наприклад, при рівномірному розподілі чисел ймовірність для $i=2,3,\ldots,n$ дорівнює $p_i=\dfrac{1}{g-(i-1)}$. Якщо процес визначення уявити у вигляді дерева можливих результатів, то повна ймовірність кожного результату визначається, як сума всіх ймовірностей, починаючи від цього результату і закінчуючи коренем дерева (початкового стану). В результаті кількість ітерацій

$$T=1p(1)+2(1-p(1))p(2)+3(1-p(1))(1-p(2))p(3)+\ldots+i(1-p(1))(1-p(2))\ldots(1-p(i-1))p(i)+\ldots+$$
$$+(g-1)(1-p(1))(1-p(2))\ldots(1-p(g-2))p(g-1)+(g-1)(1-p(1))(1-p(2))\ldots(1-p(g-1))=\frac{1}{g}\sum_{2}^{g-1}l+1$$

Так, наприклад, для $g = 8$ знадобиться $T = \frac{1}{g}\sum_{2}^{g-1} l + 1 = 4{,}37$, тобто п'ять ітерацій. Підвищення швидкодії $\theta = 1{,}4$.

Табл. 7 та графік (рис. 2) ілюструють залежність підвищення швидкодії від кількості коренів.

Таким чином, розглянутий підхід забезпечує знаходження квадратного коріння числа в системі залишкових класів.

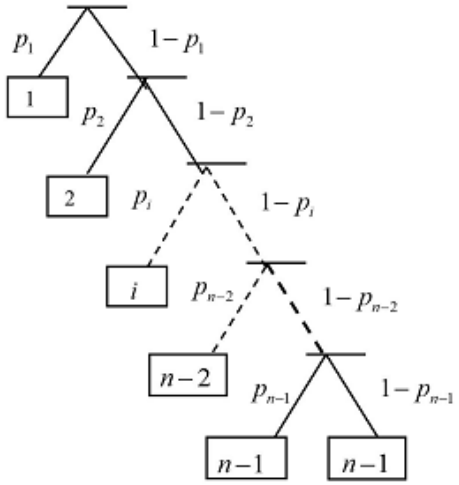

Рис. 1. Дерево можливих результатів

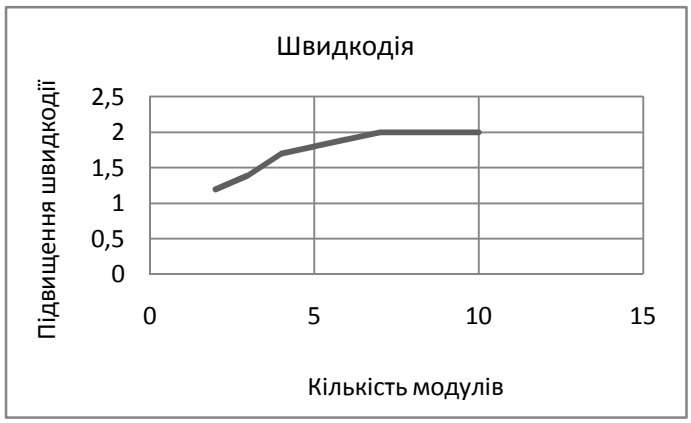

Рис. 2. Графік швидкодії

Таблиця 7

Кількість модулів	Кількість коренів	Підвищення швидкодії
2	4	1,2
3	8	1,4
4	16	1,7
5	32	1,8
6	64	1,9
7	128	2,0
8	256	2,0
9	512	2,0
10	1024	2,0

Висновки

Досліджено метод реалізації в системі залишкових класів проблемної операції визначення квадратного кореня. Показано, що запропонований метод забезпечує отримання шуканого результату. На основі запропонованого підходу при рівномірному розподілі чисел досягається підвищення швидкодії виконання операції визначення квадратного кореня. Представляється доцільним застосувати запропонований підхід в якості перспективного напрямку досліджень складних операцій в системі залишкових класів.

Список використаної літератури

1. Акушский И.Я., Юдицкий Д.И. Машинная арифметика в остаточных классах. М.: Советское радио. 1968. 440 с.
2. Гашков С.Б., Фролов А.Б., Попова Е.П. Об оценках сложности алгоритмов извлечения квадратных корней в конечных полях и кольцах вычетов // *Вестник МЭИ.* 2018. № 5. С. 79—88.

3. Визор Я.Е. Один из методов вычисления первообразных корней в остаточных классах // *Математичні машини і системи*, 2006, № 3. С. 3–11.
4. Поліський Ю.Д. Про один алгоритмічний підхід до визначення рангу числа в системі залишкових класів // *Математичне моделювання*. 2021. № 1(44). С. 17–22.
5. Полисский Ю.Д. Модификация алгоритма сравнения чисел в системе остаточных классов // *Проблеми математичного моделювання: матеріали Всеукр. наук.-метод. конф*., 23-25 трав. 2018 р. м.Кам'янске: ДДТУ. 2018. С. 128–131.

ON SQUARE ROOTS IN THE SYSTEM OF RESIDUAL CLASSES

Polissky Yu.

Abstract

When performing a number of computational operations in a non-positional number system of residual classes, there is a problem of determining the square root of a number modulo. A number of works offer different methods of implementation of this operation, however, its solution is far from perfect. The purpose of the study is an analytical consideration of the system of residual classes for the implementation of a nonmodular operation of finding the square root of the modulus. Thus the square root from some number on the module is called such number during which reduction in a square we receive initial number. The tools of the research methodology are systems analysis, number theory and the Chinese residual theorem. The research methodology is based on the analysis of special tables of residuals modulo for different values of difference and rank of number. The rank of a number is a characteristic that shows how many times you need to subtract the value of the range from the resulting number to return it to the range. This analysis shows that for each module there are no roots for some numbers, and other numbers have two square roots. Determining a particular root from this number is done by checking that it belongs to one of the intervals constructed based on the rank of the number. The time estimation of the proposed method is given, based on the fact that in real processes the parameters are described by numbers distributed randomly. This estimate is illustrated by a tree of possible results, a table and a graph of performance. The result of the work is a completed theoretical justification of the proposed approach to the effective solution of the problem of determining the square root of a number.The method of realization in the system of residual classes of the problem operation of determining the square root is investigated. It is shown that the proposed method provides the desired result. On the basis of this approach at uniform distribution of numbers increase of speed of performance of operation of definition of a square root is reached. The proposed approach is algorithmically simple and it is expedient to consider it as one of the directions of research of ways of increase of efficiency of calculations in system of residual classes.

References

[1] Akushsky I.Ya., & Yuditsky D.I. (1968). *Mashinaia arifmetika v ostatochnikh klassakh [Machine arithmetic in the residual classes]*. Moscow: Soviet Radio [in USSRian].
[2] Gashkov S.B., Frolov A.B., Popova E.P. (2018). Ob otcenkah slojnosti algoritmov izvlechenia kvadratnih korneij v konechnih poliah i koltsah vitchetov [On estimates of the complexity of algorithms for extracting square roots in finite fields and rings of residues]. *Vestnik MEI. 2018. № 5. S. 79–88.*
[3] Vizor Ya.E. (2006) Odin iz metodov vichislenia pervoobraznih korneij v ostatochnih klassah [One of the methods of calculating primitive roots in residual classes] *Mathematical Machines and Systems*, 2006, № 3. P. 3–11.
[4] Poliskiy Yu.D. Ob odnom algoritmicheskom podhode k opredeleniju ranga chisla v sisteme ostatochnih klassov [On an algorithmic approach to determining the rank of a number in a system of residual classes] *Mathematical modeling*. 2021. № 1 (44). P. 17–22.
[5] Polissky Yu.D. Modifikatsia algoritma sravnenia chisel v sisteme ostatochnih klassov [Modification of the algorithm for comparing numbers in the system of residual classes] *Vseukr. science method. conf., 23-25 herbs. 2018 p. m. Kam'yanske: DDTU.* 2018. P. 128–131.