

УДК 519.7

ПОБУДОВА МОДИФІКОВАНОЇ ДОСКОНАЛОЇ ФОРМИ СИСТЕМИ ЗАЛИШКОВИХ КЛАСІВ НА ОСНОВІ РОЗВ'ЯЗКУ СИСТЕМ КОНГРУЕНЦІЙ

М.М. Касянчук¹

На основі розв'язку систем конгруенцій розроблено метод побудови набору з трьох модулів, що утворюють модифіковану досконалу форму системи залишкових класів, за умови, коли відома різниця між першими двома модулями. Отримано умову існування відповідного набору з трьох модулів і описано графічні залежності третього модуля від різних заданих параметрів. Представлено аналітичні вирази для пошуку третього модуля та можливого діапазону обчислень. Показано, що будь-які три послідовні елементи у послідовності Фібоначчі утворюють модифіковану досконалу форму системи залишкових класів.

Ключові слова: система залишкових класів, модифікована досконала форма, модуль, конгруенція, розпаралелення.

Вступ. На сьогодні, у зв'язку із значним ростом об'ємів обчислень [1], дедалі більше уваги привертають до себе непозиційні системи числення, в яких можлива реалізація розпаралелення процесу виконання арифметичних операцій. Однією з них є система залишкових класів (СЗК) [2]. До її недоліків відносять труднощі під час виконання немодульних операцій [3], зокрема, порівняння чисел, ділення [4], визначення знаку числа, оцінка виходу результату за допустимий діапазон тощо. Однак безсумнівними перевагами СЗК є відсутність міжрозрядних переносів, оскільки додавання, віднімання, множення, піднесення до степеня тощо виконуються окремо і незалежно по кожному модулю над малорозрядними операндами, які менші від вибраних модулів, що дає змогу розпаралелити виконання вказаних операцій шляхом розподілу по ядрах багатоядерних процесорів [5]. Це особливо актуально з огляду на активний розвиток високопродуктивних обчислювальних систем, які необхідні для таких сучасних галузей, як кодування інформаційних потоків [6], оброблення зображень [7], біометрична ідентифікація [8], криптографія [9], виконання високорозмірних матричних обчислень [10] тощо.

Аналіз літературних джерел та постановка задачі. У СЗК будь-яке ціле додатне число N десятикової системи числення видається у вигляді набору $(b_1, b_2, \dots, b_n)_{p_1, p_2, \dots, p_n}$ найменших невід'ємних залишків від його ділення на фіксовані цілі додатні попарно взаємно прості числа $p_1, p_2, \dots, p_n$ ($b_i = N \bmod p_i$), які називають модулями (n – кількість модулів) [11]. При цьому має виконуватись умова $0 \leq N < P-1$, де $P = \prod_{i=1}^n p_i$.

Зворотне перетворення в десятикову систему числення відбувається згідно з китайською теоремою про остачі і є досить громіздким [11]:

$$N = \left(\sum_{i=1}^n b_i B_i \right) \bmod P, \quad (1)$$

¹ доц. М.М. Касянчук, канд. фіз.-мат. наук – Тернопільський національний економічний університет

$$\text{де: } B_i = M_i m_i, \quad M_i = \frac{P}{p_i}, \quad m_i = M_i^{-1} \bmod p_i.$$

Ця процедура має значну обчислювальну складність, що також є одним із істотних недоліків СЗК. У серії робіт [12-16] розглянуто методи підбору модулів, що утворюють модифіковану досконалу форму (МДФ) СЗК, у якій виконується така рівність:

$$m_i = M_i^{-1} \bmod p_i = \pm 1. \quad (2)$$

Це дає змогу уникнути виконання громіздкої операції пошуку оберненого елемента за модулем. Розробці ще одного такого методу на основі розв'язку систем конгруенцій, коли відома різниця між першими двома модулями, і присвячена дана робота.

Виклад основного матеріалу. Не порушуючи загальності, згідно з [12], обмежимо наші міркування трьома модулями. У випадку великорозрядних чисел, коли задана різниця між другим та першим модулями ($p_2 - p_1 = q < p_1$, причому p_1 і q повинні бути взаємно простими), представимо їх у такому вигляді: $p_1 = qn - r$, $p_2 = qn - r + q$ і побудуємо систему рівнянь для МДФ СЗК, відповідну (2):

$$\begin{cases} (qn - r) p_3 \bmod (qn - r + q) = qp_3 \bmod (qn - r + q) = \mp 1 \\ (qn - r + q) p_3 \bmod (qn - r) = qp_3 \bmod (qn - r) = \pm 1 \\ (qn - r)(qn - r + q) \bmod p_3 = \pm 1. \end{cases} \quad (3)$$

Розглянемо спочатку перші два рівняння (3), які з урахуванням відповідних математичних перетворень набудуть такого вигляду:

$$\begin{cases} z \bmod (qn - r + q) = \mp 1 \\ z \bmod (qn - r) = \pm 1, \end{cases} \quad (4)$$

де $z = qp_3$.

Ця система розв'язується за допомогою китайської теореми про залишки, що передбачає пошук оберненого елемента за модулем. Оскільки вираз (4) розглядаємо в загальному вигляді, без числових значень, то в цьому випадку застосувати розширений алгоритм Евкліда неможливо. Для пошуку оберненого елемента зручно використати метод, описаний у [17]. До 1 потрібно додати модуль і перевірити, чи ділиться отриманий результат націло на відповідне число. Якщо ні, то модуль додається доти, поки результат не буде цілим числом, яке і є шуканим оберненим елементом. Отже:

$$(qn - r)^{-1} \bmod (qn - r + q) = -q^{-1} \bmod (qn - r + q) = -\frac{k_1(qn - r + q) + 1}{q}; \quad (5)$$

$$(qn - r + q)^{-1} \bmod (qn - r) = q^{-1} \bmod (qn - r) = \frac{k_2(qn - r) + 1}{q}, \quad (6)$$

де k_1, k_2 дорівнюють кількості доданих модулів $(qn - r + q)$ та $(qn - r)$ відповідно. Тоді запис виразу розширеного алгоритму Евкліда

$$\frac{k(qn - r) + 1}{q}(qn - r + q) - \frac{k(qn - r + q) + 1}{q}(qn - r) = 1 \quad (7)$$

показує рівність коефіцієнтів $k_1 = k_2 = k$ в обох рівняннях (5) і (6).

Далі розглядаємо китайську теорему про залишки для чотирьох випадків, записаних в (4): (1; 1), (1; -1), (-1; 1), (-1; -1). Друга та третя пари залишків приводять до складних для аналізу виразів:

$$z \bmod (qn-r)(qn-r+q) = \pm \frac{2k(qn-r)(qn-r+q) + 2(qn-r) + q}{q} \bmod (qn-r)(qn-r+q), \quad (8)$$

з яких, як показують чисельні розрахунки, отримується або $p_3 < p_2$, або взагалі не виконується третє рівняння системи (3).

З першої та четвертої пари залишків можна записати

$$z \bmod (qn-r+q)(qn-r) = \pm 1. \quad (9)$$

Тоді з (9), аналогічно до (5), (6), шукаються відповідні обернені елементи:

$$p_3 = q^{-1} \bmod (qn-r)(qn-r+q) = \frac{k_3(qn-r)(qn-r+q)+1}{q}; \quad (10)$$

$$p_3 = -q^{-1} \bmod (qn-r)(qn-r+q) = -\frac{k_3(qn-r)(qn-r+q)+1}{q} = \frac{(b-k_3)(qn-r)(qn-r+q)-1}{q}, \quad (11)$$

де k_3 дорівнює кількості доданих модулів $(qn-r+q)(qn-r)$.

Далі, враховуючи (10), (11), з третього рівняння (3):

$$p_3 = qn(n+1) - r(2n+1) + \frac{r^2 \pm 1}{q}. \quad (12)$$

На рис. 1 показано залежність модуля p_3 від параметрів q та r при $n=3$, а на рис. 2 – залежність p_3 від n та r при сталій різниці $q=p_2-p_1=5$, згідно з (12), де в чисельнику останнього доданка прийнято (r^2-1) . Як видно з рис. 1, при малих q і великих r модуль p_3 змінюється гіперболічно, в інших випадках – лінійно. На рис. 2 графіком є параболоїд, а модуль p_3 зростає інтенсивніше при малих r і великих n .

Це пояснює, що, наприклад, для $q=7$ третій модуль можна знайти тільки при $r=1$ та $r=6$. Крім цього, якщо $p_2-p_1=1$, тобто $q=1$, $r=0$, або $p_2-p_1=2$ ($q=2$, $r=1$), то треті модулі можуть набирати по два значення відповідно: $p_3 = n^2+n\pm 1$ та $p_3 = 2n^2-(1\pm 1)/2$. У табл. 1 наведено аналітичні вирази для третього модуля p_3 та можливого діапазону обчислень P залежно від числа n при зміні значення q від 1 до 7. Цікавим є випадок, коли третій модуль дорівнює сумі абсолютних величин двох попередніх. Тоді з (12) можна отримати

$$qn(n+1) - r(2n+1) + \frac{r^2 \pm 1}{q} = 2(qn-r) + q. \text{ Перейшовши до квадратного рівняння } r^2 - qr(2n-1) + q^2(n^2-n-1) \pm 1 = 0 \text{ відносно } r, \text{ знайдемо:}$$

$$r = \frac{q(2n-1) \pm \sqrt{5q^2+4}}{2}, \quad (14)$$

тобто вираз $(5q^2+4)$ має бути повним квадратом деякого числа. У табл. 2 представлено можливі набори модулів, отримані згідно з (14), для різних q .

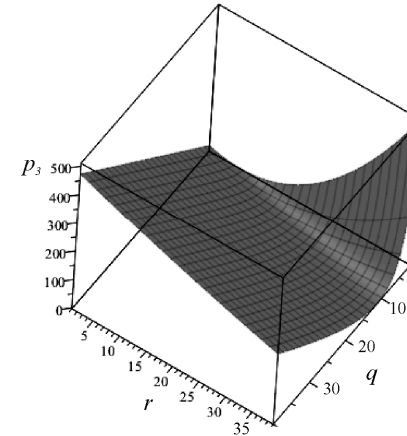


Рис. 1. Залежність модуля p_3 від параметрів q та r при $n=3$

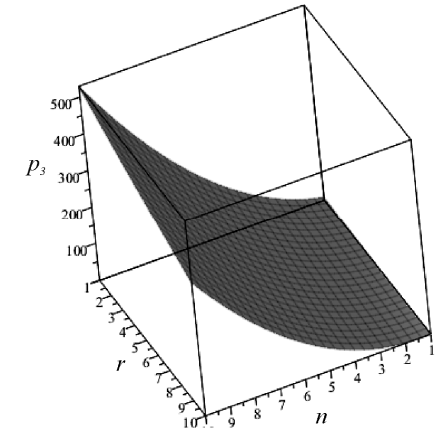


Рис. 2. Залежність модуля p_3 від параметрів n та r при сталій різниці модулів $q=p_2-p_1=5$

З виразу (12) випливає умова існування третього модуля, яка має вигляд

$$r^2 \bmod q = \pm 1. \quad (13)$$

Табл. 1. Аналітичні вирази для модуля p_3 та можливого діапазону обчислень P залежно від числа n при зміні параметрів q та r

№	q	r	p_1	p_2	p_3	P
1	1	0	n	n+1	n^2+n+1, n^2+n-1	$n^4+2n^3+2n^2+n, n^4+2n^3-n$
2	2	1	$2n-1$	$2n+1$	$2n^2, 2n^2-1$	$8n^4-2n^2, 8n^4-6n^2+1$
3	3	2	$3n-2$	$3n+1$	$3n^2-n-1$	$27n^4-18n^3-12n^2+5n+2$
4	3	1	$3n-1$	$3n+2$	$3n^2+n-1$	$27n^4+18n^3-12n^2-5n+2$
5	4	3	$4n-3$	$4n+1$	$4n^2-2n-1$	$64n^4-64n^3-12n^2+14n+3$
6	4	1	$4n-1$	$4n+3$	$4n^2+2n-1$	$64n^4+64n^3-12n^2-14n+3$
7	5	4	$5n-4$	$5n+1$	$5n^2-3n-1$	$125n^4-150n^3+27n+4$
8	5	3	$5n-3$	$5n+2$	$5n^2-n-1$	$125n^4-50n^3-50n^2+11n+6$
9	5	2	$5n-2$	$5n+3$	$5n^2+n-1$	$125n^4+50n^3-50n^2-11n+6$
10	5	1	$5n-1$	$5n+4$	$5n^2+3n-1$	$125n^4+150n^3-27n+4$
11	6	5	$6n-5$	$6n+1$	$6n^2-4n-1$	$216n^4-288n^3+30n^2+44n+5$
12	6	1	$6n-1$	$6n+5$	$6n^2+4n-1$	$216n^4+288n^3+30n^2-44n+5$
13	7	6	$7n-6$	$7n+1$	$7n^2-5n-1$	$343n^4-490n^3+84n^2+65n+6$
14	7	1	$7n-1$	$7n+6$	$7n^2+5n-1$	$343n^4+490n^3+84n^2-65n+6$

Табл. 2. Можливі набори модулів, отримані згідно з (15), для різних q

№	q	r	$p_1=qn-r$	$p_2=qn-r+q$	$p_3=p_1+p_2$
1	1	$n-2$	2	3	5
2	2	$2n-3$	3	5	8
3	3	$3n-5$	5	8	13
4	5	$5n-8$	8	13	21
5	8	$8n-13$	13	21	34
6	13	$13n-21$	21	34	55
7	21	$21n-34$	34	55	89

Згідно з даними табл. 2, значення отриманих модулів, параметра q , а також відповідних числових величин для r утворюють послідовність Фібоначчі, у якій кожен наступний елемент дорівнює сумі двох попередніх. Крім цього, параметр r записується аналітично, однак модулі, що отримуються з його допомогою, набувають конкретних числових значень.

Висновки. У цій роботі представлено метод побудови набору з трьох модулів, які утворюють модифіковану досконалу форму системи залишкових класів, на основі розв'язку систем конгруенцій за умови, коли відома різниця між першими двома модулями. Отримано формулу, яка визначає умову існування відповідного набору модулів, та описано графічні залежності третього модуля від різних параметрів. Представлено аналітичні вирази для пошуку третього модуля та можливого діапазону обчислень, які визначаються відповідно другим та четвертим степенями різниці перших двох модулів. Показано, що будь-які три послідовні елементи у послідовності Фібоначчі утворюють модифіковану досконалу форму системи залишкових класів.

Література

1. Задірака В.К. Комп'ютерна арифметика багаторозрядних чисел / В.К. Задірака, О.С. Олексюк. – К.: Вид-во НУ "Львівська політехніка", 2003. – 264 с.
2. Omondi A. Residue number systems: theory and implementation / A. Omondi, B. Premkumar. – London: Imperial College Press. – 2007. – 296 p.
3. Краснобаев В.А. Метод арифметического сравнения данных, представленных в системе остаточных классов / В.А. Краснобаев, А.С. Янко, С.А. Кошман // Кибернетика и системный анализ: сб. науч. тр. – 2016. – Т. 52, № 1. – С. 157-162.
4. Chervyakov N.I. An Approximate Method for Comparing Modular Numbers and its Application to the Division of Numbers in Residue Number Systems / N.I. Chervyakov, M.G. Babenko, P.A. Lyakhov, I.N. Lavrinenko // Cybernetics and Systems Analysis. – 2014. – Vol. 50, № 6. – Pp. 977-984.
5. Pikh V. Synthesis of High-performance Components of Spectral Analyzers and Special Processors for Data Encryption in Rademacher-Krestenson's Theoretical-numerical Basis / V. Pikh, V. Kimak, B. Krulikovskiy // Proceedings of the XIII-th International Conference "The Experience of Designing and Application of CAD Systems in Microelectronics (CADSM-2015)". – Polyana-Svalyava (Zakarpattia), Ukraine. – 2015. – Pp. 182-184.
6. Yatskiv V. Multilevel method of data coding in WSN / V. Yatskiv, Su Jun, N. Yatskiv, A. Sachenko, O. Osolinskiy // Proceedings of the 2011 IEEE 6th International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS-2011). – Prague, Czech Republic. – 2011. – Pp. 863-866.
7. Березький О.М. Статистичне оброблення цитологічних зображень / О.М. Березький, К.М. Березька, С.Ю. Попіна, Г.М. Мельник // Вісник Хмельницького національного університету: зб. наук. праць. – Сер.: Технічні науки. – 2012. – № 5. – С. 161-164.
8. Andrijchuk V.A. Modern Algorithms and Methods of the Person Biometric Identification / V.A. Andrijchuk, I.P. Kuritnyk, M.M. Kasyanchuk, M.P. Karpinski // Proceedings of the Third IEEE Workshop on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS-2005). – Sofia, Bulgaria. – 2005. – Pp. 403-406.
9. Kasyanchuk M.M. Algorithms theory of RSA and El Gamal in differentiated notation of Rademacher-Krestenson basis / M.M. Kasyanchuk, I.Z. Yakymenko, O.I. Volynskiy, I.R. Pituh // Reports of Khmelnytsky National University. Technical sciences. – 2011. – № 3. – Pp. 265-273.
10. Yakymenko I. Matrix Algorithms of Processing of the Information Flow in Computer Systems Based on Theoretical and Numerical Krestenson's Basis / I. Yakymenko, M. Kasyanchuk // Proceedings of the X-th International Conference "Modern Problems of Radio Engineering, Telecommunications and Computer Science" (TCSET-2010). – L'viv – Slavske. – 2010. – Pp. 241.
11. Николайчук Я.М. Теория джерел інформації / Я.М. Николайчук. – Тернопіль: Вид-во ТзОВ "Терно-граф", 2010. – 536 с.
12. Касянчук М.Н. Теория и методы построения системы модулей модифицированной совершенной формы системы остаточных классов / М.Н. Касянчук, Я.Н. Николайчук, И.З. Якименко // Проблемы управления и информатики: сб. науч. тр. – 2016. – № 4. – С. 109-115.
13. Nykolaychuk Ya.M. Theoretical Foundations of the Modified Perfect form of Residue Number System / Ya.M. Nykolaychuk, M.M. Kasyanchuk, I.Z. Yakymenko // Cybernetics and Systems Analysis. – 2016. – Vol. 52, № 2. – Pp. 219-223.
14. Kasyanchuk M. Conception of theoretical bases of the accomplished form of Krestenson's transformation and its practical application / M. Kasyanchuk // Proceedings of the 4-th International Conference "Advanced Computer Systems and Networks: Design and Application" (ACSN-2009). – L'viv. – 2009. – Pp. 299-301.
15. Касянчук М.М. Теорія та математичні закономірності досконалої форми системи залишкових класів / М.М. Касянчук // Питання оптимізації обчислень (ПОО – XXXV): праці Міжнар. симпозіуму. – Т. 1. – Київ – Кадивелі. – 2009. – С. 306-310.
16. Касянчук М.М. Побудова трьохмодульної модифікованої досконалої форми системи залишкових класів на основі розв'язку квадратного рівняння / М.М. Касянчук // Інформатика та математичні методи в моделюванні: зб. наук. праць. – 2016. – Т. 6, № 1. – С. 19-25.
17. Касянчук М.М. Теорія алгоритмів перетворень китайської теореми про залишки в матрично-розмежованому базисі Радемахера – Крестенсона / М.М. Касянчук, Я.М. Николайчук, І.З. Якименко // Вісник Національного університету "Львівська політехніка". – Сер.: Комп'ютерні системи проектування. Теорія і практика. – Львів: Вид-во НУ "Львівська політехніка". – 2010. – № 688. – С. 118-125.

Надійшла до редакції 29.09.2016 р.

Касянчук М.Н. Построение модифицированной совершенной формы системы остаточных классов на основе решения систем конгруэнций

На основе решения систем конгруэнций разработан метод построения набора из трех модулей, образующих модифицированную совершенную форму системы остаточных классов, при условии, если известна разница между первыми двумя модулями. Получено условие существования соответствующего набора из трех модулей и описаны графические зависимости третьего модуля от различных заданных параметров. Представлены аналитические выражения для поиска третьего модуля и возможного диапазона вычислений. Показано, что любые три последовательные элемента в последовательности Фибоначчи образуют модифицированную совершенную форму системы остаточных классов.

Ключевые слова: система остаточных классов, модифицированная совершенная форма, модуль, конгруэнция, распараллеливание.

Kasyanchuk M.M. Construction of a Modified Perfect Form of the Residual Class-Based Systems Based on Solution of Systems of Contingencies

Based on solution of the congruential systems we exploited the method of constructing a set of three modules which forming a modified form of the perfect system of residual classes, and difference between the first of two modules was taking into account. The condition of existence of the corresponding set of three modules has achieved and the graphical dependence of the third module from various preset settings has described. The analytical expressions were presented for exploration of the third module and a possible range of calculations. It was shown that some of three consecutive elements in the Fibonacci sequence have formed a modified form of perfect system of residual classes.

Keywords: system of residual classes, modified perfect form, module, congruence, parallelization.