УДК 581.3

Informatics and Mathematical Methods in Simulation
Vol. 6 (2016), No. 1, pp. 19-25

ПОБУДОВА ТРЬОХМОДУЛЬНОЇ МОДИФІКОВАНОЇ ДОСКОНАЛОЇ ФОРМИ СИСТЕМИ ЗАЛИШКОВИХ КЛАСІВ НА ОСНОВІ РОЗВ'ЯЗКУ КВАДРАТНОГО РІВНЯННЯ

М.М. Касянчук

Тернопільський національний економічний університет,
вул. Львівська, 11, Тернопіль, 46020, Україна; E-mail: kasyanchuk@ukr.net

Виконання арифметичних операцій над багаторозрядними числами є досить важливою задачею сучасної теорії чисел, прикладної і обчислювальної математики, а також асиметричної криптографії. Тому велика увага приділяється розпаралелюванню процесу обчислень, що реалізується, зокрема, при використанні системи залишкових класів. Дана стаття присвячена розробці аналітичного методу побудови трьохмодульної модифікованої досконалої форми системи залишкових класів, яка дозволяє уникнути виконання громіздкої процедури пошуку оберненого елемента за модулем та множення на базисні числа, на основі розв'язку квадратного рівняння, отриманого за допомогою теореми Вієта. Визначено умову, при виконанні якої існує набір шуканих модулів, та проведено її дослідження. Показано, що відповідна заміна змінних дозволяє суттєво скоротити перебір усіх можливих варіантів та зменшити обчислювальну складність для знаходження модулів. Побудовано та проаналізовано графічні залежності абсолютних величин отриманих модулів та визначено ділянки їх монотонності. Наведено приклад обчислення можливих значень шуканих модулів за допомогою розробленого алгоритму.

Ключові слова: система залишкових класів, модифікована досконала форма, модуль, квадратне рівняння, теорема Вієта, обернений елемент за модулем, базисні числа

Вступ

Відомо [1], що найперспективнішим шляхом підвищення швидкодії сучасних обчислювальних систем є розпаралелювання процесу обробки інформації. Цією властивістю, на відміну від найпоширенішого на даний час двійкового представлення чисел, володіють деякі непозиційні системи числення, зокрема система залишкових класів (СЗК) [2]. Хоча вона має певні недоліки (відсутність операцій ділення та порівняння, труднощі у виявленні переповнення розрядної сітки тощо), однак дозволяє ефективно виконувати додавання, віднімання, множення, піднесення до степеня над великорозрядними числами [3], що є дуже важливим у наш час, зокрема, у асиметричній криптографії (алгоритми RSA, Ель-Гамаля, електронного цифрового підпису тощо) [4], при великих матричних обчисленнях, інших задачах прикладної математики [3].

Представленню десяткового числа N у СЗК відповідають найменші невід'ємні залишки b_i цього числа у системі взаємно простих модулів p_i, тобто $b_i = N \bmod p_i$ [1]. При цьому діапазон обчислень має лежати в межах $0 \le N \le P-1$, де $P = \prod_{i=1}^{n} p_i$. Зворотнє перетворення у десяткову систему числення відбувається на основі китайської теореми

про залишки [5]: $N = \left(\sum_{i=1}^{n} b_i B_i \right) \bmod P$, де $B_i = M_i m_i$, $M_i = \frac{P}{p_i}$, базисні числа m_i шукаються з виразу:

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

Необхідність обчислення оберненого елемента в (1) істотно збільшує складність переведення чисел з СЗК у десяткову систему. Спрощення цієї задачі відбувається у досконалій формі СЗК (ДФ СЗК), коли усі $m_i = 1$ [1], що дозволяє уникнути процедури пошуку оберненого елемента і множення на базисні числа. В [6] визначені умови для аналітичного визначення m_i. Але в обох випадках значення p_i швидко збільшуються, що неприйнятно при необхідності використання модулів приблизно однакової розрядності.

У роботі [7] описана модифікована ДФ СЗК (МДФ СЗК), у якій базисні числа $m_i = \pm 1$, що також виключає необхідність пошуку оберненого числа. У [8] розроблений метод побудови трьохмодульної МДФ СЗК на прикладі $p_2 - p_1 = 5$. Однак на даний час відсутні аналітичні методи пошуку модулів, які задовольняють умовам МДФ СЗК.

Метою роботи є розробка алгоритму знаходження системи з трьох модулів для МДФ СЗК на основі побудови та розв'язку квадратного рівняння, побудованого за допомогою теореми Вієта.

Основна частина

У працях [9], [10] за допомогою розв'язування систем конгруенцій було отримано вираз для пошуку набору модулів ДФ СЗК. Аналогічні міркування приводять до умови, яка має виконуватися для МДФ СЗК:

$$\sum_{i=1}^{n} \frac{1}{p_i} = h \pm \frac{1}{\prod_{i=1}^{n} p_i}, \quad (2)$$

де $h = 0, \pm 1, \pm 2, \pm 3, \ldots$.

Для спрощення обмежимося трьома взаємно простими значеннями модулів та приймемо $h = 0$, що відповідає найбільшому діапазону обчислень при заданій кількості модулів. Рівняння (2) буде мати вигляд:

$$\frac{1}{p_1} + \frac{1}{p_2} + \frac{1}{p_3} = \pm \frac{1}{p_1 p_2 p_3} . \quad (3)$$

Потрібно відмітити, що умова $m_i = 1$ визначає додатній знак модулів, а $m_i = -1$ – від'ємний. Після відповідних перетворень, вважаючи відомим перший модуль, вираз (3) набуде такого вигляду:

$$p_2 p_3 + p_1 (p_2 + p_3) = \pm 1 . \quad (4)$$

У рівняння (4) входять добуток та сума невідомих модулів p_2 та p_3. Для їх пошуку введемо позначення $p_2 p_3 = k p_1 \pm 1$. Тоді відповідно $p_2 + p_3 = -k$. За допомогою теореми Вієта можна побудувати квадратне рівняння, цілочисельними коренями якого будуть значення шуканих модулів:

$$x^2 + kx + kp_1 \pm 1 = 0\,. \tag{5}$$

Розв'язавши (5), невідомі модулі можна записати таким чином:

$$p_{2,3} = \frac{1}{2}\left(-k \pm \sqrt{k^2 - 4(kp_1 \pm 1)}\right). \tag{6}$$

З (6) видно, що розв'язки (5) будуть цілочисельні, коли дискримінант рівняння (5) являтиме собою повний квадрат деякого числа, яке зручно представити в такому вигляді:

$$k^2 - 4(kp_1 \pm 1) = (k - 2(p_1 + a))^2\,. \tag{7}$$

Парність другого доданку в дужках в правій частині виразу випливає з вигляду дискримінанта у лівій частині (7). Після відповідних перетворень з (7) отримується:

$$k = 2p_1 + a + \frac{p_1^2 \pm 1}{a}\,. \tag{8}$$

Отже, МДФ СЗК з трьох модулів існує, коли виконується умова $(p_1^2 \pm 1) \bmod a = 0$. Це означає, що параметр a обмежується інтервалом $\left[-p_1^2 - 1;\, p_1^2 + 1\right]$, $a \neq 0$. Дослідивши (8), можна побачити, що екстремуми k визначаються з умови $a = \pm\sqrt{m^2 \pm 1}$. На рис.1 представлено графік залежності величини k від a, що змінюється від -26 до 26, при $p_1 = 5$.

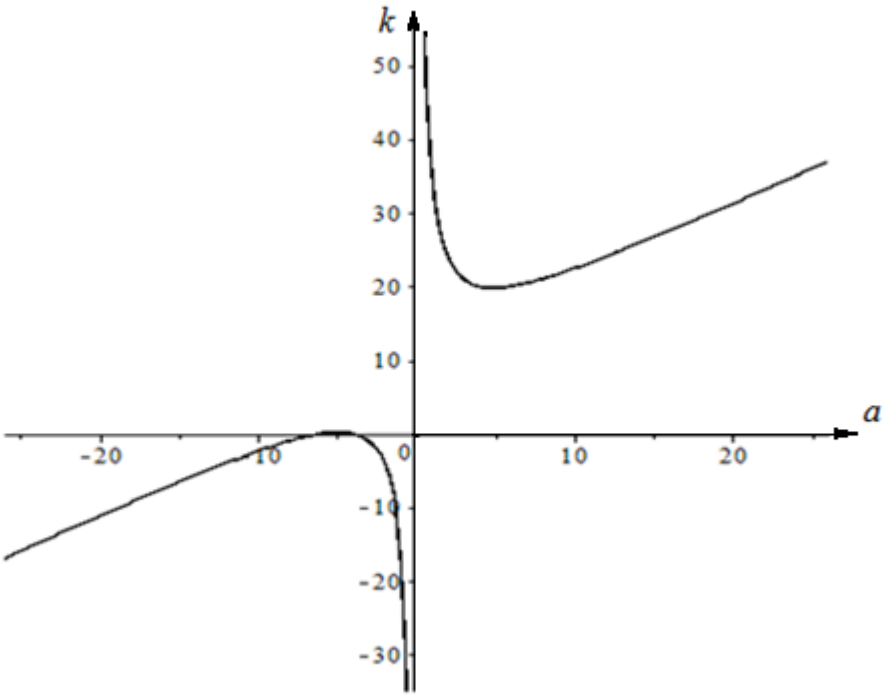

Рис. 1. Графік залежності величини *k* від параметра a

Графік та побудоване з (7) відносно a квадратне рівняння $a^2 + a(2p_1 - k) + p_1^2 \pm 1 = 0$ показують, що фіксованій величині k відповідають два значення параметра *a*, причому, згідно теореми Вієта, якщо одне з них є цілочисельне,

то і друге теж повинно бути цілим числом. Це дозволяє зменшити діапазон дослідження a до таких меж: $[-p_1+1; p_1-1]$, $a \neq 0$. На рис.2 для прикладу показана поверхня, яка, згідно виразу $k = 2p_1 + a + \frac{p_1^2 - 1}{a}$, характеризує залежність параметра k від значень $p_1 = 2 \ldots 10$ та $a = 1 \ldots \ p_1 - 1$.

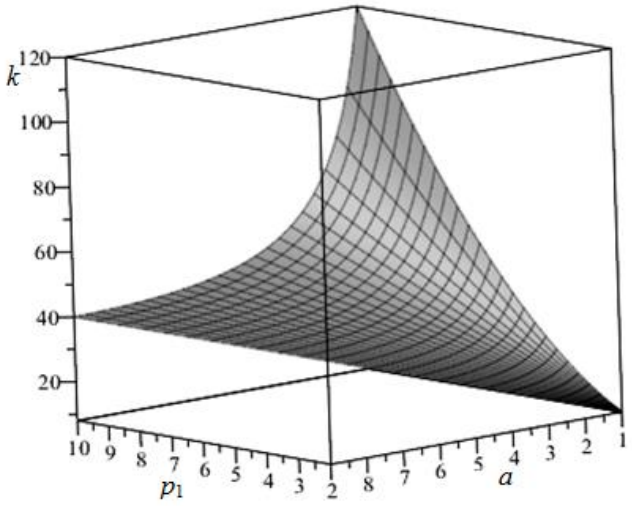

Рис. 2. Графік залежності параметра k від значень $p_1 = 2 \ldots 10$ та $a = 1 \ldots \ p_1 - 1$

Як видно з графіка, величина k досягає максимуму при найбільшому значенні модуля p_1 та найменшому значенні параметра a. Мінімум k знаходиться при мінімальних значеннях p_1 і a.

На рис.3,4 показано відповідно графіки залежності модулів $p_2 = \frac{1}{2}\left(-k + \sqrt{k^2 - 4(kp_1 - 1)}\right)$ та $p_3 = \frac{1}{2}\left(-k - \sqrt{k^2 - 4(kp_1 - 1)}\right)$ від значень модуля $p_1 = 2...10$ і параметра $a = 1... p_1 - 1$.

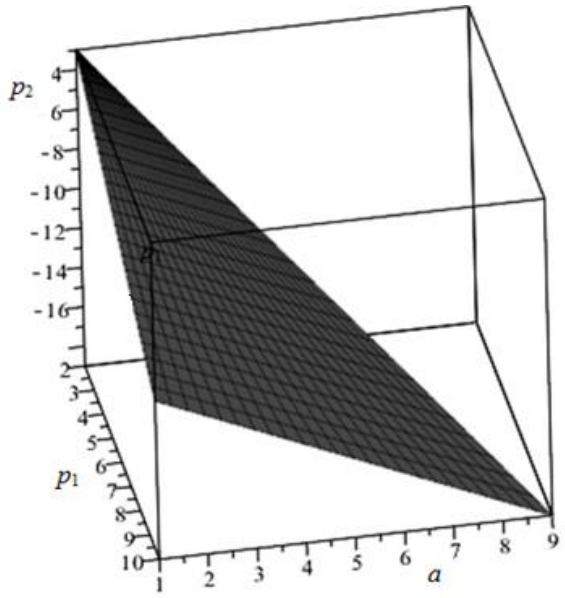

Рис. 3. Графік залежності модуля p_2 від значень модуля p_1 і параметра с

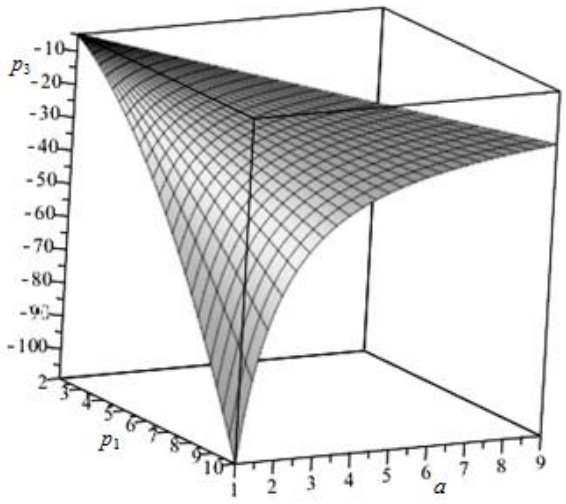

Рис. 4. Графік залежності модуля p_3 від значень модуля p_1 і параметра a

З рис.3,4 видно, що графіком залежності модуля p_2 від значень p_1 і a є площина, а модуля p_3 - гіперболоїд. Мінімального абсолютного значення модулі p_2 та p_3 набувають при найменших величинах p_1 та a. Максимальне абсолютне значення p_2 буде у випадку, коли $p_1 \to \max$, $a \to \max$, відповідно $|p_3| \to \max$, якщо $p_1 \to \max$, $a \to \min$.

В табл.1 представлено можливі значення p_2, p_3, відповідних їм параметрів a, k, а також абсолютних величин модулів для $p_1 = 5$.

Таблиця 1.

Можливі значення p_2, p_3, відповідні їм значення параметрів *a*, *k*, а також абсолютні величини модулів для $p_1 = 5$.

№	*a*	*k*	p_2	p_3	$\lvert p_2 \rvert$	$\lvert p_3 \rvert$
1	-3	-1	-2	3	2	3
2	-2	-4	-3	7	3	7
3	-2	-5	-3	8	3	8
4	-1	-15	-4	19	4	19
5	-1	-17	-4	21	4	21
6	1	37	-6	-31	6	31
7	1	35	-6	-29	6	29
8	2	25	-7	-18	7	18
9	2	24	-7	-17	7	17
10	3	21	-8	-13	8	13
11	4	20	-9	-11	9	11

З табл.1 видно, що модуль p_2 набуває тільки від'ємних значень. При $a < 0$ модуль p_3 додатній і навпаки, якщо $a > 0$, то $p_3 < 0$. Слід зазначити, що в табл.1 відсутнє значення $a = -4$, оскільки в цьому випадку, як випливає з виразу (6), p_2, $p_3 = \pm 1$. Однак такий набір модулів суперечить початковим умовам задачі. На рис.5 зображено графіки залежності абсолютних величин модулів p_2 та p_3 від їх номера згідно табл.1.

Як видно з рис.5, абсолютна величина модуля p_2 повільно збільшується. На відміну від цього, графік для $|p_3|$ швидко зростає, досягає максимуму посередині номерного діапазону, потім спадає з меншою швидкістю до значення $|p_2|$.

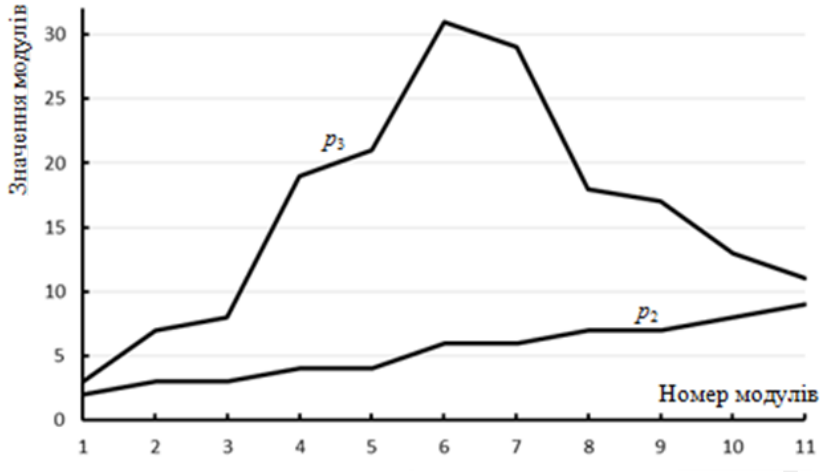

Рис. 5. Графіки залежності абсолютних величин модулів p_2 та p_3 від їх номера згідно табл.1

Висновки

Дана стаття присвячена розробці аналітичного методу побудови трьохмодульної модифікованої досконалої форми системи залишкових класів, яка дозволяє уникнути виконання громіздкої процедури пошуку оберненого елемента за модулем, на основі розв'язку квадратного рівняння, отриманого за допомогою теореми Вієта. Визначено умову, при виконанні якої існує набір шуканих модулів, та проведено її дослідження. Показано, що відповідна заміна змінних дозволяє суттєво скоротити перебір усіх можливих варіантів та зменшити обчислювальну складність для знаходження модулів. Побудовано та проаналізовано графічні залежності абсолютних величин отриманих модулів та визначено ділянки їх монотонності. Наведено приклад обчислення можливих значень шуканих модулів за допомогою розробленого алгоритму.

Список літератури

1. Николайчук, Я.М. Теорія джерел інформації / Я.М. Николайчук. – Тернопіль: ТзОВ «Терно–граф», 2010. – 536 с.
2. Червяков, Н.И. Нейрокомпьютеры в остаточных классах / Н.И.Червяков, П.А. Сахнюк, А.В. Шапошников, А.И. Макоха. - М: Радиотехника, 2003. - 272 с.
3. Задірака, В.К. Комп'ютерна арифметика багаторозрядних чисел / В.К. Задірака, О.С. Олексюк. – К.: 2003. – 264 с.
4. Задірака, В.К. Комп'ютерна криптологія / В.К. Задірака, О.С. Олексюк. – Тернопіль, Київ, 2002. – 504 с.
5. Виноградов, И.М. Основы теории чисел/ И.М. Виноградов. – Москва-Ижевск: НИЦ «Регулярная и хаотическая динамика», 2003. – 176 с.
6. Nykolaychuk, Ya. M. Theoretical Foundations for the Analytical Computation of Coefficients of Basic Numbers of Krestenson's Transformation. // Ya. M. Nykolaychuk, M. M. Kasianchuk, I. Z. Yakymenko / Cybernetics and Systems Analysis. – 2014. – Vol.50. – Issue 5. – P. 649 - 654.
7. Касянчук, М.М. Теорія та математичні закономірності досконалої форми системи залишкових класів / М.М. Касянчук // Праці Міжнародного симпозіуму «Питання оптимізації обчислень (ПОО–XXXV)». Т.1. – Київ–Кацивелі. – 2009. – С. 306–310.

8. Николайчук, Я.Н. Теоретические основы модифицированной совершенной формы системы остаточных классов / Я.Н. Николайчук, М.Н. Касянчук, И.З. Якименко // Кибернетика и системный анализ. – 2016. – Том 52. – № 2. – С. 51 – 55.
9. Kasianchuk, M. Algorithms of findings of perfect shape modules of remaining classes system / M. Kasianchuk, I. Yakymenko, I. Pazdriy, O. Zastavnyy // Proceedings of the XIII-th International Conference «The Experience of Designing and Application of CAD Systems in Microelectronics (CADSM-2015)». - Polyana-Svalyava (Zakarpattya), Ukraine. - 2015. – P. 168 - 171.
10. Касянчук, М.М. Аналітичний пошук модулів досконалої форми системи залишкових класів та їх використання в китайській теоремі про залишки / М.М. Касянчук, І.З. Якименко, І.Р. Паздрій, Я.М. Николайчук // Вісник Хмельницького національного університету: Технічні науки. – 2015. - №1. – С. 170 - 176.

ПОСТРОЕНИЕ ТРЁХМОДУЛЬНОЙ МОДИФИЦИРОВАННОЙ СОВЕРШЕННОЙ ФОРМЫ СИСТЕМЫ ОСТАТОЧНЫХ КЛАССОВ НА ОСНОВЕ РЕШЕНИЯ КВАДРАТНОГО УРАВНЕНИЯ

М.Н. Касянчук

Тернопольский национальный экономический университет,
ул. Львовская, 11, г.Тернополь, 46020, Украина; E-mail: kasyanchuk@ukr.net

Выполнение арифметических операций над многоразрядными числами является весьма важной задачей современной теории чисел, прикладной и вычислительной математики, а также асимметричной криптографии. Поэтому большое внимание приделяется распараллеливанию процесса вычислений, что реализуется, в частности, использованием системы остаточных классов. Данная статья посвящена разработке аналитического метода построения трёхмодульной модифицированной совершенной формы системы остаточных классов, которая позволяет избежать выполнения громоздкой процедуры поиска обратного элемента по модулю и умножения на базисные числа, на основе решения квадратного уравнения, полученного с помощью теоремы Виета. Определено условие, при выполнении которого существует набор искомых модулей, и проведено его исследование. Показано, что соответствующая замена переменных позволяет существенно сократить перебор всех возможных вариантов и уменьшить вычислительную сложность для нахождения модулей. Построены и проанализированы графические зависимости абсолютных величин полученных модулей и определены участки их монотонности. Приведён пример вычисления возможных значений искомых модулей с помощью разработанного алгоритма.

Ключевые слова: система остаточных классов, модифицированная совершенная форма, модуль, квадратное уравнение, теорема Виета, обратный элемент по модулю, базисные числа

CONSTRUCTION OF THREE MODULAR MODIFIED PERFECT FORMS OF SYSTEM OF RESIDUAL CLASSES BASED SOLUTION OF QUADRATIC EQUATION

M.M. Kasianchuk

Ternopil National Economic University,
11, Lvivska Str., Ternopil, 46020, Ukraine; E-mail: kasyanchuk@ukr.net

Perform of arithmetic operations with multidigital numbers are quite important task of modern numbers theory, applied and computational mathematics and asymmetric cryptography. So much attention is paid for paralleling computation process, which is implemented particularly in the system of residual classes usage. This article is focused on the development of the analytical method of construction of triple-modular modified perfect form of the system of residual classes, which allows to avoid the cumbersome execution procedure of search of inverse element by module and multiplying by the basis number, based on the solution of the quadratic equation obtained with using of Vieta's formula. The condition which is required for existence of set of modules is defined and investigated. It is shown that the corresponding change of variables allows to reduces significantly of all possible options and to exhauses the computational complexity for finding modules. The image depending of absolute values of obtained modules is constructed and analyzed and the areas of monotony are identified. An example of the possible values of the calculation modules using the algorithm is launched.

Keywords: system of residual classes, modified perfect form, module, quadratic equations, Vieta's formula, inverse element for the module, the basis number