УДК 581.3
В.В. Суслін, Ю.М. Кладій, А.М. Гринчук, С.В. Стихальська
Тернопільський національний економічний університет, Україна

ПОБУДОВА МОДИФІКОВАНОЇ ДОСКОНАЛОЇ ФОРМИ СИСТЕМИ ЗАЛИШКОВИХ КЛАСІВ НА ОСНОВІ ТЕОРЕМИ ВІЄТА

V.V.Suslin, Yu.M.Kladij, A.M.Hrynchuk, S.V.Stykhalska

CONSTRUCTION OF A MODIFIED PERFECT FORM OF A SYSTEM OF RESIDUAL CLASSES BASED ON THE VIETA'S THEOREM

Відомо [1], що найперспективнішим шляхом підвищення швидкодії сучасних обчислювальних систем є розпаралелення процесу обробки інформації. Цією властивістю володіють деякі непозиційні системи числення, зокрема система залишкових класів (СЗК) [2]. Хоча вона має певні недоліки, однак дозволяє ефективно виконувати арифметичні операції над великорозрядними числами, що є дуже важливим у наш час, наприклад, під час захисту інформації [3].

Представленню десяткового числа N у СЗК відповідають найменші невід'ємні залишки b_i цього числа у системі взаємно простих модулів p_i, тобто $b_i=N \bmod p_i$ [4]. 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 [4]: $N=\left(\sum_{i=1}^{n} b_i B_i\right) \bmod P$, де $B_i=M_i m_i$, $M_i=\frac{P}{p_i}$, базисні числа m_i шукаються з виразу: $m_i=M_i^{-1} \bmod p_i$.

Необхідність обчислення оберненого елемента істотно збільшує складність переведення чисел з СЗК у десяткову систему [5]. Спрощення цієї задачі відбувається у модифікованій досконалій формі СЗК (МДФ СЗК), коли усі $m_i=\pm 1$ [6], що дозволяє уникнути процедури пошуку оберненого елемента і множення на базисні числа.

Тому *метою* нашої роботи є розробка алгоритму знаходження системи з трьох модулів для МДФ СЗК на основі теореми Вієта.

В роботах [6, 7] був отриманий такий вираз: $p_2p_3+p_1(p_2+p_3)=\pm 1$. У це рівняння входять модуль p_1, який вважається відомим, а також добуток і сума невідомих модулів p_2 та p_3. Для їх пошуку введемо позначення $p_2p_3=kp_1 \pm 1$. Тоді відповідно $p_2+p_3=-k$. За допомогою теореми Вієта можна побудувати квадратне рівняння, цілочисельними коренями якого будуть значення шуканих модулів:

$$x^2+kx+kp_1 \pm 1=0. \quad (1)$$

Розв'язавши (1), невідомі модулі можна записати таким чином:

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

З (2) видно, що розв'язки (1) будуть цілочисельні, коли дискримінант рівняння (1) є повним квадратом деякого числа, яке зручно представити в такому вигляді: $k^2-4(kp_1 \pm 1)=(k-2(p_1+a))^2$. Після відповідних перетворень маємо: $k=2p_1+a+\frac{p_1^2 \pm 1}{a}$.

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 $[-p_1+1; p_1-1]$, $a \neq 0$.

В таблиці 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, відповідних їм параметрів *a*, *k*, а також абсолютних величин 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 таблиці 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 таблиці відсутнє значення *a*=-4, оскільки в цьому випадку p_2, p_3=±1. Однак такий набір модулів суперечить початковим умовам задачі.

Отже, відповідна заміна змінних дозволяє суттєво скоротити перебір усіх можливих варіантів та зменшити обчислювальну складність для знаходження модулів МДФ СЗК.

Література

1. Kasianchuk M. Conception of theoretical bases of the accomplished form of Krestenson's transformation and its practical application / M. Kasianchuk // Proceedings of the 4-th International Conference "Advanced Computer Systems and Networks: Design and Application" (ACSN–2009). – L'viv. – 2009. – P. 299–301.

2. 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.

3. 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. – P.403–406.

4. Бородін О.І. Теорія чисел / О.І.Бородін. – К.: Вища школа, 1970. – 275 с.

5. *Rajba T.* Research of Time Characteristics of Search Methods of Inverse Element by the Module / *T. Rajba, A. Klos-Witkowska, S. Ivasiev, I. Yakymenko, M. Kasianchuk //* Proceedings of the 2017 IEEE 9th International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS–2017) – Bucharest, Romania. – V.1. – September, 2017. – P.82–85.

6. 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.

7. 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. – 2016. – т.6, №1. – С. 19–25.