**УДК 519.61**

**М. КАСЯНЧУК**

# КОНЦЕПЦІЯ ТЕОРЕТИЧНИХ ПОЛОЖЕНЬ ДОСКОНАЛОЇ ФОРМИ ПЕРЕТВОРЕННЯ КРЕСТЕНСОНА ТА ЙОГО ПРАКТИЧНЕ ЗАСТОСУВАННЯ

***Тернопільський національний економічний університет,***
***46020, м.* Тернопіль*, вул. Львівська, 11***

**Анотація.** Показано, що базис Крестенсона на даний час залишається досить перспективним для застосування у сучасних обчислювальних системах під час виконання операцій додавання, віднімання та множення великих цілих чисел. Запропоновано та проаналізовано метод пошуку набору будь–якої кількості модулів досконалої форми перетворення Крестенсона, що дозволяє розглядати як завгодно великий діапазон десяткових чисел. Обгрунтовано та узагальнено використання модифікованої досконалої форми базису Крестенсона.

**Abstract.** It is shown that Krestenson's base up to now remains perspective enough for application in the modern computer systems, especially during implementation of operations of addition, deduction and multiply of large integers. The method of any amount of the accomplished form modules of the Krestenson's transformation set searching is offered and analyzed, that allows to examine any large range of decimal numerals. The use of modified accomplished form of Krestenson's base is grounded and generalized.

**Ключові слова:** базис Крестенсона, система числення, модуль.

## ВСТУП

Відомо, що двійкова система числення (або базис Радемахера), яка використовується в сучасних комп'ютерних системах, має певні недоліки – наявність міжрозрядних зв'язків та велику розрядність [1]. Тому актуальним є розвиток і застосування непозиційних систем числення, в яких відсутні вказані недоліки. Прикладом може бути система залишкових класів (СЗК), або, як її ще називають, представлення чисел у базисі Крестенсона [2], [3]. Хоча вона не набула значного поширення у зв'язку з необхідністю визначення умов переповнення, складністю та громіздкістю зворотнього перетворення чисел у десяткову систему числення, а також складнощами реалізації операцій ділення та порівняння, але СЗК можна ефективно використовувати у мультибазисних процесорах, спеціалізованих обчислювальних машинах для виконання операцій додавання, віднімання та множення, наприклад, у задачах лінійної алгебри (матрично–векторні операції) тощо. Необхідно відмітити, що ця система особливо ефективна при обчисленнях з великими числами [4], [5], а також у задачах криптографії.

## ТЕОРЕТИЧНІ ОСНОВИ ДОСКОНАЛОЇ ФОРМИ ПЕРЕТВОРЕННЯ КРЕСТЕНСОНА

Будь–яке ціле додатнє число $N$ у десятковій системі числення представляється у базисі Крестенсона у вигляді набору $(b_1, b_2, \dots, b_n)_{p1, p2, \dots, pn}$ найменших додатніх залишків від ділення цього числа на фіксовані цілі додатні попарно взаємно прості числа $p_1, p_2, \dots, p_n$ ($b_i = N \bmod p_i$), які називаються модулями ($n$ – кількість модулів). При цьому повинна виконуватись умова $0 \le N \le \prod_{i=1}^{n} p_i - 1$.

Зворотнє перетворення із базису Крестенсона у десяткову систему числення грунтується на використанні китайської теореми про остачі [6]:

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

де $B_i=M_i m_i$, $M_i = \frac{P}{p_i}$, $m_i$ шукається з виразу $(M_i m_i) mod\ p_i = 1$ і $\left(\sum_{i=1}^{n} B_i\right) mod\ P = 1$.

Слід зазначити, що пошук коефіцієнтів $m_i = M_i^{-1}\ mod\ p_i$ становить значну обчислювальну складність. У роботі [3] було запропоновано досконалу форму СЗК (ДФ СЗК), у якій підбір модулів такий, що $m_i$=1, тобто

$$M_i \bmod p_i = 1. \tag{2}$$

Крім того, у [3] було визначено рівняння, яке повинно виконуватись для модулів у ДФ СЗК та знайдено набори модулів при $n$=3 (2, 3, 5, $P$=30), $n$=4 (2, 3, 7, 41, $P$=1722 та 2, 3, 11, 13, $P$=858), $n$=5 (2, 3, 11, 17, 59, $P$=66198). Подальшому розвитку теоретичної концепції ДФ СЗК та її практичному застосуванню і присвячена наша робота.

## ПРАКТИЧНЕ ЗАСТОСУВАННЯ ДОСКОНАЛОЇ ФОРМИ ПЕРЕТВОРЕННЯ КРЕСТЕНСОНА

Запишемо вираз (2) у вигляді системи:

$$\begin{cases} M_1 \bmod p_1 = 1; \\ \dots \\ M_n \bmod p_n = 1. \end{cases} \tag{3}$$

Розв’язуючи (3) стандартними методами теорії чисел згідно китайської теореми про залишки [7] та врахувавши, що у ДФ СЗК $m_i$=1, матимемо:

$$\left(\sum_{i=1}^{n} M_i\right) mod\ P = 1. \tag{4}$$

Вираз (4) еквівалентний рівності:

$$\sum_{i=1}^{n} \frac{1}{p_i} = k + \frac{1}{\prod_{i=1}^{n} p_i}, \tag{5}$$

де $k$=1, 2, 3, ... .

Дослідження цього рівняння для великої кількості модулів, враховуючи, що сума ряду $\sum_{i=1}^{n} \frac{1}{p_i}$ розбіжна, тобто $k$ може бути як завгодно великим, є досить громіздкою задачею. Поклавши $k$=1, що відповідає найбільшому значенню $P$, перепишемо (5) у такому вигляді:

$$\frac{1}{p_1} + \frac{1}{p_2} + \frac{1}{p_3} + \dots + \frac{1}{p_n} = 1 + \frac{1}{p_1 p_2 p_3 \dots p_n}. \tag{6}$$

Модуль $p_1$ виберемо так, щоб при відніманні величини $\frac{1}{p_1}$ від 1 в правій частині (6) в чисельнику отримати 1. Видно, що $p_1$=2.Тоді маємо:

$$\frac{1}{p_2} + \frac{1}{p_3} + \dots + \frac{1}{p_n} = \frac{1}{2} + \frac{1}{2 p_2 p_3 \dots p_n}. \tag{7}$$

Аналогічно звідси випливає, що $p_2$=3:

$$\frac{1}{p_3} + \dots + \frac{1}{p_n} = \frac{1}{6} + \frac{1}{6 p_3 p_4 \dots p_n}. \tag{8}$$

Легко побачити, що $p_3$=7, $p_4$=43, $p_5$=1807. Для останнього модуля $p_n$ справедлива рівність:

$$\frac{1}{p_n} = \frac{1}{\prod_{i=1}^{n-1} p_i} + \frac{1}{p_n \cdot \prod_{i=1}^{n-1} p_i}. \quad (9)$$

Звідси отримуємо, що

$$p_n = \prod_{i=1}^{n-1} p_i - 1. \quad (10)$$

Отже, остаточний вираз для побудови системи модулів ДФ СЗК базису Крестенсона має такий вигляд:

$$\begin{cases} p_1 = 2 \\ p_i = p_1 p_2 \ldots p_{i-1} + 1, \ 1 < i < n \\ p_n = p_1 p_2 \ldots p_{n-1} - 1. \end{cases} \quad (11)$$

Слід зазначити, що запропонований метод не вичерпує всіх можливих наборів для базису Крестенсона при заданих $n$. Наприклад, при $n$=5 набір модулів, отриманий за допомогою системи (11), буде $P_{51}$ = 2, 3, 7, 43, 1805. Однак відомі також набори $P_{52}$ = 2, 3, 7, 83, 85 та $P_{53}$ = 2, 3, 11, 17, 59. При $n$=6 набір модулів, отриманий з (11), буде таким: $P_{61}$ = 2, 3, 7, 43, 1807, 3263441. Усі можливі набори модулів для ДФ СЗК базису Крестенсона при $n$=6, відповідні їм діапазони десяткових чисел та розрядність у двійковій системі наведені у таблиці 1.

Як видно з таблиці, набір модулів, отриманий за допомогою системи (11), найоптимальніший, оскільки в цьому випадку величина $P$ є максимальна, що дозволяє розглядати найбільший діапазон десяткових чисел. При цьому досягається зменшення розрядності приблизно вдвічі.

Таблиця 1

**Можливі набори модулів при $n$=6 для ДФ СЗК базису Крестенсона та відповідні їм діапазони десяткових чисел (в дужках – розрядність у базисі Радемахера)**

| № | $p_1$, $p_2$ | $p_3$ | $p_4$ | $p_5$ | $p_6$ | P |
|---|---|---|---|---|---|---|
| 1 | 2, 3 (2) | 7 (3) | 43 (6) | 1807 (11) | 3263441 (22) | $1{,}0650050423922\times10^{13}$ (44) |
| 2 | | | | 1811 (11) | 654133 (20) | $2{,}139450562578\times10^{12}$ (41) |
| 3 | | | | 1819 (11) | 252701 (18) | $8{,}30151592914\times10^{11}$ (41) |
| 4 | | | | 1825 (11) | 173471 (18) | $5{,}7175174245\times10^{11}$ (40) |
| 5 | | | | 1871 (11) | 51985 (16) | $1{,}7565866661\times10^{11}$ (38) |
| 6 | | | | 1901 (11) | 36139 (16) | $1{,}24072631634\times10^{11}$ (37) |
| 7 | | | | 1945 (11) | 25271 (15) | $8{,}876868357\times10^{10}$ (37) |
| 8 | | | | 2053 (12) | 15011 (14) | $5{,}5656554898\times10^{10}$ (36) |
| 9 | | | | 2167 (12) | 10841 (14) | $4{,}2427359282\times10^{10}$ (36) |
| 10 | | | | 2501 (12) | 6499 (13) | $2{,}9354722194\times10^{10}$ (35) |
| 11 | | | | 3041 (12) | 4447 (13) | $2{,}4423128562\times10^{10}$ (35) |
| 12 | | | | 3611 (12) | 3613 (12) | $2{,}3562056658\times10^{10}$ (35) |
| 13 | | | 47 (6) | 395 (9) | 779729 (20) | $6{,}0797809317\times10^{10}$ (36) |
| 14 | | | | 481 (9) | 2203 (12) | $2{,}091735282\times10^{9}$ (31) |
| 15 | | | 53 (6) | 271 (9) | 799 (10) | $4{,}81993554\times10^{8}$ (29) |
| 16 | | | 71 (7) | 103 (7) | 61429 (16) | $1{,}8867671634\times10^{10}$ (35) |
| 17 | | 11 (4) | 23 (5) | 31 (5) | 47057 (16) | $2{,}214408306\times10^{9}$ (32) |

## ЗАСТОСУВАННЯ БАЗИСУ КРЕСТЕНСОНА У ВИПАДКУ ОБМЕЖЕНОЇ КІЛЬКОСТІ МОДУЛІВ

У випадку обмеженої кількості модулів та необхідності розгляду великих чисел зручно використати іншу форму СЗК, яку назвемо модифікованою досконалою (МДФ), тобто підібрати такий набір модулів, що $m_i$=±1. Порівняно з ДФ СЗК, обчислювальну складність збільшується, але вона менша, ніж при пошуку оберненого елемента $m_i = M_i^{-1} \ mod \ p_i$.

Запропонований метод дозволяє побудувати систему з двох модулів, що неможливо у ДФ СЗК. Для цього необхідно вибрати два будь–які послідовні числа $p_1$ та $p_2=p_1+1$, які завжди будуть взаємно простими, оскільки для них виконується умова:

$$\begin{cases}(p_1+1)\,mod\ p_1=1\\ p_1\ mod(p_1+1)=-1.\end{cases} \tag{12}$$

Система (12) дозволяє записати загальну формулу для визначення різноманітних наборів будь–якої кількості модулів, для яких коефіцієнти $m_i=\pm1$. Вважаючи $p_1$ найменшим у наборі модулів, можемо отримати:

$$\begin{cases}p_2=p_1+1\\ p_i=p_1p_2\ldots p_{i-1}\pm1,\end{cases} \tag{13}$$

де $i=3, 4, \ldots, n$.

З (13) видно, що для будь–якого модуля $p_i$ виконується умова $M_i \bmod p_i=\pm1$.

## УЗАГАЛЬНЕННЯ ДОСКОНАЛОЇ ТА МОДИФІКОВАНОЇ ДОСКОНАЛОЇ ФОРМ СИСТЕМИ ЗАЛИШКОВИХ КЛАСІВ

Узагальнюючи вирази (11) та (13) та враховуючи, що для зменшення складності обчислень якомога більша кількість $m_i$ повинна дорівнювати 1, представимо набір модулів у такому вигляді:

$$\begin{cases}p_1;\\ p_2=p_1+1;\\ .....\\ p_i=p_1\cdot p_2\ \ldots\ p_{i-1}+1;\\ .....\\ p_n=p_1\cdot p_2\ \ldots\ p_{n-1}-1.\end{cases} \tag{14}$$

Для знаходження $m_i$ використаємо таку систему рівнянь:

$$\begin{cases}M_n\ mod\ \ p_n=(p_1\cdot p_2\ \ldots\ p_{n-1})mod(p_1\cdot p_2\ \ldots\ p_{n-1}-1)=1=m_n;\\ M_{n-1}\ mod\ \ p_{n-1}=(p_1\cdot p_2\ \ldots\ p_{n-2}\cdot p_n)mod(p_1\cdot p_2\ \ldots\ p_{n-2}+1)=(-1)\cdot(-1)=1=m_{n-1};\\ .....\\ M_i\ mod\ \ p_i=(p_1\cdot p_2\ \ldots\ p_{i-1}\cdot p_{i+1\ \ldots}\cdot p_n)mod(p_1\cdot p_2\ \ldots\ p_{i-1}+1)=(-1)\cdot1\cdot1\cdot\ldots\cdot(-1)=1=m_i;\\ .....\\ M_2\ mod\ \ p_2=(p_1\cdot p_3\ \ldots\ \cdot p_n)mod(p_1+1)=(-1)\cdot1\cdot1\cdot\ldots\cdot(-1)=1=m_2;\\ M_1\ mod\ \ p_1=(p_2\cdot p_3\ \ldots\ \cdot p_n)mod\ p_1=1\cdot1\cdot\ldots\cdot(-1)=-1=m_1.\end{cases} \tag{15}$$

З (15) видно, що всі $m_i$, крім $m_1$=–1, рівні 1. Якщо вибрати $p_1$=2, то система (15) переходить у (11), оскільки $1\,mod\ \ 2=-1\,mod\ \ 2$.

## ВИСНОВКИ

У роботі розглянуто концепцію теоретичних положень досконалої форми перетворення Крестенсона та обгрунтовано можливості його практичного застосування. Показано, що відповідний підбір модулів дозволяє істотно спростити обчислення у системі залишкових класів, наприклад, для виконання операцій з багаторозрядними числами. На завершення автор висловлює щиру вдячність професору Я.М.Николайчуку за корисні консультації щодо отриманих результатів.

## СПИСОК ЛІТЕРАТУРИ

1. Рабинович З.Л. Типовые операции в вычислительных машинах / З.Л. Рабинович, В.А. Раманаускас. – К.: Техніка, 1980. –264 с.
2. Акушский И.Я. Машинная арифметика в остаточных классах / И.Я. Акушский, Д.И. Юдицкий. – М.: Сов. радио, 1968. – 460 с.
3. Задірака В.К.. Комп'ютерна арифметика багаторозрядних чисел / В.К. Задірака, О.С. Олексюк: Наукове видання. – К.: 2003. – 264 с.
4. Николайчук Я.М. Разработка теории и комплексов технических средств формирования, передачи и обработки цифровых сообщений в низовых вычислительных сетях автоматизированных систем: дис. докт. техн. наук. – К.: Академия наук УССР Ордена Ленина, Институт кибернетики им. В.М.Глушкова, 1991: –573 с.
5. Нетрадиционная система остаточных классов и её основоположник И.Я.Акушский / М.В. Синьков, Т.В. Синькова, А.В. Федоренко, А.А. Чапор // История вычислительной техники в лицах. – К.: КИТ, ПТОО «А.С.К.», 1995. – С. 91–101.
6. Бухштаб А.А. Теория чисел / А.А.Бухштаб. – М.: Просвещение, 1966. – 384 с.
7. Бородін О.І. Теорія чисел / О.І. Бородін. – К.: Вища школа, 1970. – 275 с.

Надійшла до редакції 21.06.2010р.

**КАСЯНЧУК М. – доцент кафедри комп'ютерної інженерії, Тернопільський національний економічний університет, Тернопіль, Україна.**