УДК 519.7

М.М. КАСЯНЧУК, І.З. ЯКИМЕНКО, І.Р. ПАЗДРІЙ, Я.М. НИКОЛАЙЧУК
Тернопільський національний економічний університет

АНАЛІТИЧНИЙ ПОШУК МОДУЛІВ ДОСКОНАЛОЇ ФОРМИ СИСТЕМИ ЗАЛИШКОВИХ КЛАСІВ ТА ЇХ ЗАСТОСУВАННЯ В КИТАЙСЬКІЙ ТЕОРЕМІ ПРО ЗАЛИШКИ

У даній роботі показано, що система залишкових класів *є досить перспективною для застосування в сучасних обчислювальних системах, особливо під час виконання операцій над багаторозрядними числами. Отримано аналітичні вирази та визначено умови, які дозволяють обчислити усі варіанти систем модулів для заданої їх кількості у досконалій формі системи залишкових класів. В результаті проведених досліджень показано, що запропонований метод істотно зменшує обчислювальну складність китайської теореми про залишки за рахунок уникнення операції пошуку оберненого елемента за модулем.*

Ключові слова: система залишкових класів, досконала форма, набір модулів, факторизація, китайська теорема про залишки.

M.M. KASIANCHUK, I.Z. YAKYMENKO, I.R. PAZDRIY, YA.M. NYKOLAYCHUK
Ternopil National Economic University

SEARCH MODULES ANALYSIS OF RESIDUAL PERFECT FORM CLASS AND THEIR APPLICATION IN THE CHINESE REMAINDER THEOREM

Abstract – This paper shows that the system of residual classes is quite promising for use in modern computing systems, especially when performing operations on multi-digit numbers. It is one from alternatives to binary system which allows to use the new approaches for computing managing under performing of basic mathematical operations. To optimize of computations and them parallelization the use of perfect form of residual classes system are appropriated.

The analytical expressions and the conditions that allow to calculate all versions of modules for a given number of them in perfect form system of residual classes. The particular cases are considered and specific characters of changes of the respective modules values are studied. It is shown that the proposed method significantly reduces the computational complexity of Chinese remainder theorem by the avoiding of operation of finding of inverse element by module. Our results allow us to use them effectively in asymmetric systems of information security and computer networks for data transmission by open channels.

Keywords: system of residual classes, perfect form, a set of modules, factorization, the Chinese Remainder Theorem.

Вступ

На даний час система залишкових класів (СЗК) або теоретико-числовий базис (ТЧБ) Крестенсона [1], який її породжує, є однією з альтернатив двійковій системі числення (або ТЧБ Радемахера), що дозволяє застосовувати нові підходи до організації обчислювальних систем при виконанні елементарних математичних операцій [2].

Хоча СЗК не позбавлена недоліків, до яких відносяться, зокрема, відсутність ділення та порівняння чисел, необхідність визначення умов переповнення розрядної сітки, однак її успішно можна застосовувати для додавання, віднімання та множення цілих чисел [3]. Це стосується матрично-векторних розрахунків [4], множення та піднесення до степеня великорозрядних чисел [5] тощо. Особливо корисним може бути застосування СЗК в задачах сучасної криптографії (алгоритми RSA, Ель-Гамаля [6], електронного цифрового підпису тощо) та кодування даних [7, 8]. Безсумнівною перевагою СЗК є також можливість виконання операцій над числами, які менші за вибрані модулі, розпаралелення процесу обчислень та відсутність міжрозрядних переносів.

СЗК – це непозиційна система числення [3], десяткові числа N в якій представляються невід'ємними залишками b_i від ділення на кожен з системи взаємно простих модулів p_i. Операції додавання, віднімання і множення в СЗК відбуваються незалежно по кожному модулю без переносів між розрядами. Діапазон обчислень обмежується виразом $0 \le N \le \prod_{i=1}^{n} p_i - 1$.

Зворотне перетворення з СЗК у десяткову систему числення ґрунтується на використанні китайської теореми про залишки [9] і є досить громіздким процесом, що являється ще одним недоліком СЗК, який стримував її розвиток і поширення:

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

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

На даний час пошук оберненого елемента $m_i = M_i^{-1} mod\, p_i$ здійснюється такими способами: 1) брутальною атакою; 2) за допомогою функції Ейлера; 3) використовуючи наслідок алгоритму Евкліда [10].

Всі вони є досить громіздкими і характеризуються значною обчислювальною та часовою складністю при виконанні великої кількості ділень з остачею, піднесення до степеня та знаходження функції

Ейлера. Крім того, ці операції повинні виконуватися над багаторозрядними числами, що може привести до переповнення розрядної сітки.

У роботі [1] описана досконала форма СЗК (ДФ СЗК), у якій підбір модулів такий, що

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

тобто m_i=1. В [11], [12] розвинуто дану теорію, однак не вказано методу побудови всіх можливих варіанті в наборів модулів ДФ СЗК при заданій їх кількості.

Мета роботи. Виходячи з вищесказаного, метою нашої роботи є подальший розвиток теорії ДФ СЗК та визначення умов, які дозволяють побудувати всі можливі варіанти для заданої кількості модулів ДФ СЗК.

Розробка алгоритмів підбору модулів ДФ СЗК

Запишемо вираз (2) у вигляді системи:

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

Домноживши кожне рівняння на відповідний модуль, отримаємо:

$$\begin{cases} P \ mod \ p_1^2 = p_1 \\ \dots \\ P \ mod \ p_n^2 = p_n. \end{cases} \tag{4}$$

Розв'язуючи (4) стандартними методами теорії чисел згідно китайської теореми про залишки, матимемо:

$$P = \left(\sum_{i=1}^{n} p_i M_i^2 m_i^2 \right) mod \ M, \tag{5}$$

де $M = \prod_{i=1}^{n} p_i^2 = P^2$.

Врахувавши, що у ДФ СЗК m_i=1, та скоротивши модуль, ліву та праву частину (5) на їх спільний дільник $P = \prod_{i=1}^{n} p_i$, запишемо (5) таким чином:

$$\left(\sum_{i=1}^{n} M_i \right) mod \ P = 1. \tag{6}$$

Вираз (6) еквівалентний рівності:

$$\sum_{i=1}^{n} M_i = kP + 1, \tag{7}$$

де k=1, 2, 3, ...

Поділивши ліву та праву частини (7) на $P = p_1 \cdot p_2 \cdot p_3$, отримаємо остаточний вираз для пошуку набору модулів у ДФ СЗК:

$$\sum_{i=1}^{n} \frac{1}{p_i} = k + \frac{1}{\prod_{i=1}^{n} p_i}. \tag{8}$$

Елементарною підстановкою можна переконатися, що єдино можливою системою з трьох модулів ДФ СЗК є 2, 3, 5, оскільки при збільшенні будь–якого p_i ліва частина (8) стає меншою 1.

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.

Обмежимося найпростішим випадком, який відповідає значенню k=1. Крім того, слідуючи [11], виберемо кількість модулів n=6. Вираз (8) набуде такого вигляду:

$$\frac{1}{p_1} + \frac{1}{p_2} + \frac{1}{p_3} + \frac{1}{p_4} + \frac{1}{p_5} + \frac{1}{p_6} = 1 + \frac{1}{p_1 p_2 p_3 p_4 p_5 p_6}. \tag{9}$$

На даний час відомі тільки такі набори модулів ДФ СЗК, в яких p_1=2, p_2=3, тоді (9) перепишемо так:

$$\sum_{i=3}^{n} \frac{1}{p_i} = \frac{1}{6} + \frac{1}{\prod_{i=3}^{n} p_i}. \tag{10}$$

Модуль p_3 виберемо так, щоб при відніманні $\frac{1}{p_3}$ в правій частині (10) в чисельнику отримати 1. Видно, що p_3=7.Тоді маємо: $\sum_{i=4}^{n}\frac{1}{p_i}=\frac{1}{42}+\frac{1}{\prod_{i=4}^{n}p_i}$.

Аналогічно звідси випливає, що p_4=43:

$$\sum_{i=5}^{n}\frac{1}{p_i}=\frac{1}{1806}+\frac{1}{\prod_{i=4}^{n}p_i}. \tag{11}$$

Для останнього модуля p_n справедлива рівність:

$$\frac{1}{p_1p_2p_3\cdots p_{n-1}-1}=\frac{1}{p_1p_2p_3\cdots p_{n-1}}+\frac{1}{p_1p_2p_3\cdots p_{n-1}\left(p_1p_2p_3\cdots p_{n-1}-1\right)}. \tag{12}$$

Звідси випливає закономірність побудови системи модулів ДФ СЗК базису Крестенсона:

$$\begin{cases} p_1=2 \\ p_i=p_1p_2\cdots p_{i-1}+1,\ 1<i<n \\ p_n=p_1p_2\cdots p_{n-1}-1. \end{cases} \tag{13}$$

Слід зазначити, що запропонований метод не вичерпує всіх можливих наборів модулів ДФ СЗК при заданих .

Аналітичний пошук модулів ДФ СЗК

Для вирішення даної задачі трансформуємо (9) так:

$$6p_3p_4\left(p_5+p_6\right)=\left(p_4\left(p_3-6\right)-6p_3\right)p_5p_6+1. \tag{14}$$

Введемо позначення:

$$p_{5,6}=\frac{6p_3p_4+a,b}{p_4\left(p_3-6\right)-6p_3}. \tag{15}$$

Підставивши (15) в (14), матимемо умову, яка повинна виконуватися для визначення набору модулів для ДФ СЗК:

$$\left(6p_3p_4\right)^2-\left(p_4\left(p_3-6\right)-6p_3\right)=ab. \tag{16}$$

Це означає, що ліва частина (16) повинна бути факторизована, на основі чого визначаються параметри a та b. Крім того, як випливає з (15), модулі p_5 та p_6 мають бути цілими числами, тобто

$$\left(6p_3p_4+a,b\right)mod\left(p_4\left(p_3-6\right)-6p_3\right)=0. \tag{17}$$

Отже, вирази (16) та (17) визначають умови знаходження будь-якого варіанту набору модулів ДФ СЗК.

Часткові випадки

Перевіривши можливі значення p_3, можна побачити, що даний модуль може дорівнювати 7 або 11. Розглянемо ці випадки детальніше:

1) p_3=7. Вирази (16) та (17) відповідно трансформуються:

$$\left(42p_4\right)^2-\left(p_4-42\right)=ab,$$
$$\left(42p_4+a,b\right)mod\left(p_4-42\right)=0. \tag{18}$$

Модуль p_4 має бути не менше 43, оскільки набір 2, 3, 7, 41 утворює ДФ СЗК. Тоді друга умова (18) зникає, а з першої будемо мати:

$$ab=\left(42\cdot43\right)^2-1=1805\cdot1807=5\cdot19\cdot19\cdot13\cdot139. \tag{19}$$

Використавши все можливі перестановки множників у (19), можна отримати 12 можливих варіантів наборів з 6 модулів ДФ СЗК при заданих 2, 3, 7, 43, які представлені в табл. 1.

При p_4=47 отримаємо: $p_{5,6}=\frac{1974+a,b}{5}$, $ab=\left(42\cdot47\right)^2-5=9041\cdot431$.

Можливі два варіанти, які представлені у табл. 2.

При p_4=53 рівності (15) та (16) набудуть вигляду: $p_{5,6}=\frac{2226+a,b}{11}$, $ab=\left(42\cdot53\right)^2-11=5\cdot151\cdot6563$. Оскільки, $2226\bmod11=4$, $5\bmod11=5$, $151\bmod11=8$, $6563\bmod11=7$, то

умову (17) задовольняє тільки значення a=5·151. Відповідно b=6563 і p_5=271, p_6=799.

Аналогічно можна знайти ще тільки один набір модулів: p_4=71, p_5=103, p_6=61429.

1) p_3=11. Вирази (16) та (17) набудуть вигляду:

$$(66p_4)^2 - (5p_4 - 66) = ab;\ (66p_4 + a, b) mod(5p_4 - 66) = 0 \quad (20)$$

Умову (20) задовольняють значення p_4=23, p_5=31, p_6=47057.

Таблиця 1

Можливі варіанти наборів з 6 модулів ДФ СЗК при заданих 2, 3, 7, 43

№	a	b	p_5	p_6
1	1	5·19·19·13·139	1807	3263441
2	5	19·19·13·139	1811	654133
3	13	5·19·19·139	1819	252701
4	19	5·19·13·139	1825	173471
5	5·13	19·19·139	1871	51985
6	5·19	19·13·139	1901	36139
7	139	5·19·19·13	1945	25271
8	19·13	5·19·139	2053	15011
9	19·19	5·13·139	2167	10841
10	5·139	19·19·13	2501	6499
11	5·13·19	19·139	3041	4447
12	5·19·19	13·139	3611	3613

Таблиця 2

Можливі варіанти наборів з 6 модулів ДФ СЗК при заданих 2, 3, 7, 47

№	a	b	p_5	p_6
1	1	9041·431	395	779729
2	431	9041	481	2203

Отже, значення елементів таблиці, отримані в [11] методом підбору, обчислені за допомогою аналітичних розрахунків.

На рисунку 1 представлений характер зміни значень модулів p_5 та p_6 залежно від номера модуля, згідно з таблицею 1 у логарифмічній шкалі.

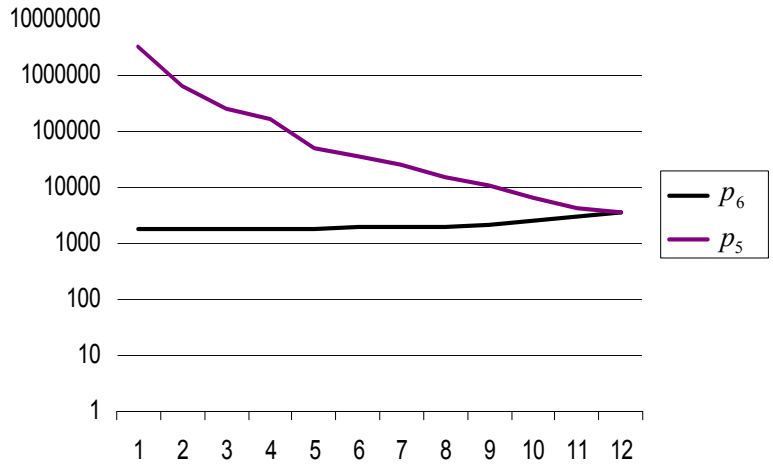

Рис. 1. Характер зміни значень модулів p_5 та p_6 залежно від номера модуля

Як видно з рисунка, модуль p_5 зростає повільно. В той же час, графік для p_6 істотно спадає із збільшенням номера модуля.

Застосування досконалої форми системи залишкових класів в задачах захисту інформації

ДФ СЗК може успішно використовуватися в асиметричних криптосистемах, зокрема, в криптосистемі Рабіна, яка ґрунтується на застосуванні КТЗ [9]. Вона зводиться до розв'язання такої системи конгруенцій:

$$\begin{cases} x \bmod p_1 = b_1 \\ x \bmod p_2 = b_2 \\ ..... \\ x \bmod p_n = b_n . \end{cases} \quad (21)$$

Розв'язок даної системи представлений в (1.8). Як уже зазначалося, пошук обернених елементів для коефіцієнтів $m_i = M_i^{-1} \bmod p_i$ становить значну обчислювальну складність. Однак якщо модулі p_1, p_2, … , p_n утворюють ДФ СЗК, тоді можна уникнути цієї громіздкої операції.

Нехай p_1=2, p_2=3, p_3=7, p_4=43, p_5=3611, p_6=3613 і потрібно розв'язати таку систему конгруенцій:

$$\begin{cases} x \bmod 2 = 1 \\ x \bmod 3 = 2 \\ x \bmod 7 = 5 \\ x \bmod 43 = 20 \\ x \bmod 3611 = 100 \\ x \bmod 3613 = 1000. \end{cases} \quad (22)$$

В загальному випадку $x = \left(\sum_{i=1}^{6} b_i M_i m_i \right) \bmod P$, де $m_i = M_i^{-1} \bmod p_i$. В ДФ СЗК $m_i = 1$,. звідси: x=(3·7·43·3611·3613·1 + 2·7·43·3611·3613·2 + 2·3·43·3611·3613·5 + 2·3·7·3611·3613·20 + 2·3·7·43·3613·100+ +2·3·7·43·3611·1000) mod 5225745 = (11781028329 + 15708037772 + 16830040470 + 10959096120 + 652507800+ +6521466000) mod 23562056658= (62452176491) mod 23562056658 = 15328063175.

Отже, шукане значення x отримане за допомогою китайської теореми про залишки без виконання громіздкої операції пошуку оберненого елемента за модулем, а використовуючи додавання та множення, методи спрощення яких описані в [4].

Оцінка та порівняльний аналіз обчислювальних складностей відомих та запропонованих алгоритмів.

При перетвореннях згідно КТЗ використовуються такі основні модульні операції: знаходження оберненого елемента; знаходження залишків; операції множення та додавання.

Тому при визначенні обчислювальних складностей відомого та запропонованого методу, які дозволяють виконувати перетворення КТЗ, потрібно враховувати складності вищезазначених операцій, наведені у табл. 3.

Таблиця3

Обчислювальні складності основних операцій КТЗ

№	Основні операції	Обчислювальна складність операцій у запропонованому алгоритмі	Обчислювальна складність операцій у класичному алгоритмі
1.	Пошук оберненого елемента	відсутня	$O1(17{,}5k \cdot ((n+1)^2 + n^2 + n)$
2.	Пошук залишків	$O\left(\log_2 n/2\right)$	$O1((n+1)^2 + n)$
3.	Операція множення і додавання	$O\left(\log_2 k \cdot (2 \cdot \log_2{}^2 n + n\right)$	$O1(k \cdot (2n^2 + n))$

де k – кількість взаємно простих модулів.

Враховуючи табличні дані, алгоритмічна складність КТЗ з використанням запропонованого методу становить $O\left(\left(log_2 k \cdot (2 \cdot log_2{}^2 n + n\right) + \left(log_2 n/2\right)\right) \approx O(log_2 k \cdot (2 \cdot log_2{}^2 n + n))$, а з використанням класичного алгоритму – $O1(37k \cdot n^2 + 53{,}5k \cdot n + 17{,}5k + n^2 + 3n + 1)) \approx O1(37k \cdot n^2)$.

На рис. 2 показано графіки залежності обчислювальних складностей від розрядності чисел n в логарифмічній шкалі.

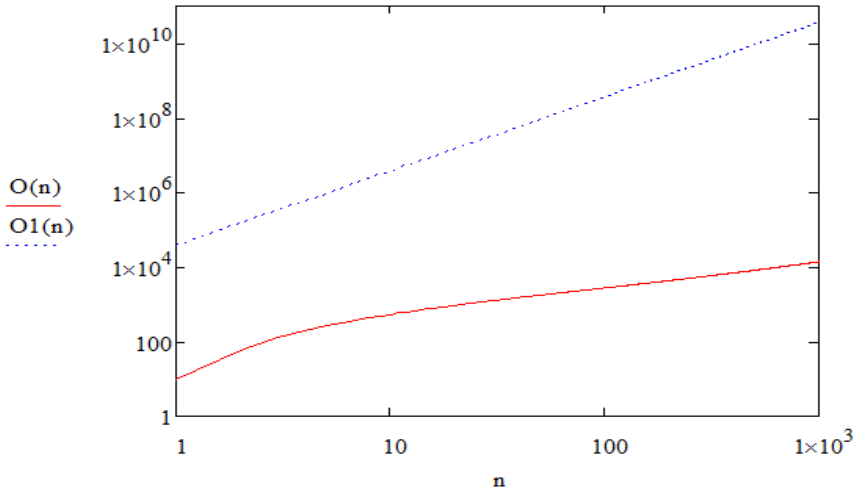

Рис. 2. Графіки залежності обчислювальних складностей від розрядності чисел n запропонованим методом $O(n)$ та класичним $O1(n)$

З рисунка видно, що використання запропонованого методу, який дозволяє аналітично обчислювати модулі ДФ СЗК і уникати операції пошуку оберненого елемента за модулем істотно зменшує обчислювальну складність КТЗ відносно класичного.

Висновки

У роботі показано, що СЗК є досить перспективною для застосування у сучасних обчислювальних системах, особливо під час виконання операцій над багаторозрядними числами. Уперше отримано аналітичні вирази та визначено умови, які дозволяють обчислити усі варіанти систем модулів для заданої їх кількості у ДФ СЗК. Показано, що використання запропонованого методу, який дозволяє аналітично обчислювати модулі ДФ СЗК і уникати операції пошуку оберненого елемента за модулем істотно зменшує обчислювальну складність КТЗ відносно класичного.

Література

1. Николайчук Я.М. Теорія джерел інформації / Я.М. Николайчук. – Тернопіль : ТзОВ „Терно–граф”, 2010. – 536 с.

2. Николайчук Я.М.Теоретичні основи побудови та структура спец процесорів в базисі Крестенсона / Я.М. Николайчук, О.І. Волинський, С.В. Кулина // Вісник Хмельницького національного університету. – 2007. – № 3. Т.1. – С. 85–90.

3. Акушский И.Я. Машинная арифметика в остаточных классах / И.Я. Акушский, Д.И. Юдицкий. – М. : Сов.радио, 1968. – 440 с.

4. Kasyanchuk M., Yakymenko I., Nykolaychuk Ya. Matrix Algorithms of Processing of the Information Flow in Computer Systems Based on Theoretical and Numerical Krestenson’s Basis. Proceedings of the X-th International Conference ”Modern Problems of Radio Engineering, Telecommunications and Computer Science” (TCSET–2010). L’viv–Slavske. 2010. P. 241.

5. Задірака В.К. Комп’ютерна арифметика багаторозрядних чисел / В.К. Задірака, О.С. Олексюк // Наукове видання. – К., 2003. – 264 с.

6. Касянчук М.М. Теорія алгоритмів RSA та Ель-Гамаля в розмежованій системі числення Радемахера – Крестенсона / М.М. Касянчук, І.З. Якименко, О.І. Волинський, І.Р. Пітух // Вісник Хмельницького національного університету. Технічні науки. – 2011. – № 3. – С. 265–273.

7. Su Jun, Yatskiv V. Method and Device for Image Coding & Transferring Based on Residue Number System.Journal Sensors & Transducers. Vol.18, Special Issue, 2013. P. 60–65.

8. Nykolaychuk Ya. M., Humennij P. V. Theoretical Bases, Methods, and Processors for Transforming Information in Galois Field Codes on the Basis of the Vertical Information Technology. Cybernetics and Systems Analysis. Vol.50, Issue 3, 2014. P. 338–347.

9. Бухштаб А.А. Теория чисел / А.А. Бухштаб. – М. : Просвещение, 1966. – 384 с.

10. Nykolaychuk Ya. M., Kasianchuk M. M., Yakymenko I. Z. Theoretical Foundations for the Analytical Computation of Coefficients of Basic Numbers of Krestenson’s Transformation. Cybernetics and Systems Analysis. Vol. 50, Issue 5, 2014. P. 649–654.

11. Касянчук М. Концепція теоретичних положень досконалої форми перетворення Крестенсона та його практичне застосування / М. Касянчук // Оптико-електронні інформаційно-енергетичні технології. – 2010. – № 2(20). – С. 43–48.

12. Касянчук М.М. Теорія та математичні закономірності досконалої форми системи залишкових класів / М.М. Касянчук // Праці Міжнародного симпозіуму „Питання оптимізації обчислень (ПОО–XXXV)”.

– Київ–Кацивелі. – 2009. – Т. 1.– С. 306–310.

References

1. Nykolaichuk Ya.M. Teoriia dzherel informatsii. Ternopil: TzOV„Terno–hraf", 2010, 536 c.

2. Nykolaichuk Ya.M., Volynskyi O.I., Kulyna S.V. Teoretychni osnovy pobudovy ta struktura spets protsesoriv v bazysi Krestensona. Visnyk Khmelnytskoho natsionalnoho universytetu. Technical Science. Khmelnytsky. 2007. Issue 3. pp.85-90.

3. Akushskyi Y.Ya, Yudytskyi D.Y. Mashynnaia aryfmetyka v ostatochnykh klassakh. M: Sov.radyo, 1968, 440 c.

4. Kasianchuk M., Yakymenko I., Nykolaychuk Ya. Matrix Algorithms of Processing of the Information Flow in Computer Systems Based on Theoretical and Numerical Krestensons Basis. Proceedings of the X–th International Conference "Modern Problems of Radio Engineering, Telecommunications and Computer Science" (TCSET–2010), Lviv–Slavske, 2010, pp. 241.

5. Zadiraka V.K., Oleksiuk O.S. Kompiuterna aryfmetyka bahatorozriadnykh chysel: Naukove vydannia – K., 2003. – 264 c.

6. Kasianchuk M.M., Yakymenko I.Z., Volynskyi O.I., Pitukh I.R. Teoriia alhorytmiv RSA ta El–Hamalia v rozmezhovanii systemi chyslennia Rademakhera – Krestensona. Visnyk Khmelnytskoho natsionalnoho universytetu. Technical Science. Khmelnytsky. 2011. Issue 3. pp.265-273.

7. Jun Su, Yatskiv V. Method and Device for Image Coding & Transferring Based on Residue Number System. Journal Sensors & Transducers, 2013, Vol.18, Special Issue, pp.60-65.

8. Nykolaychuk Ya. M., Humennij P. V. Theoretical Bases, Methods, and Processors for Transforming Information in Galois Field Codes on the Basis of the Vertical Information Technology. Cybernetics and Systems Analysis, 2014, Vol.50, No. 3, pp. 338-347.

9. Bukhshtab A.A. Teoryia chysel. M.:Prosveshchenye, 1966, 384 c.

10. Nykolaychuk Ya. M., Kasianchuk M. M., Yakymenko I. Z. Theoretical Foundations for the Analytical Computation of Coefficients of Basic Numbers of Krestensons Transformation. Cybernetics and Systems Analysis, 2014, Vol. 50, No 5, pp. 649-654.

11. Kasianchuk M. Kontseptsiia teoretychnykh polozhen doskonaloi formy peretvorennia Krestensona ta yoho praktychne zastosuvannia. Optyko-elektronni informatsiino-enerhetychni tekhnolohii, 2010, No 2 (20), pp. 43-48.

12. Kasianchuk M.M. Teoriia ta matematychni zakonomirnosti doskonaloi formy systemy zalyshkovykh klasiv. Pratsi Mizhnarodnoho sympoziumu „Pytannia optymizatsii obchyslen (POO–XXXV)", Vol. 1, Kyiv–Katsyveli, 2009, pp. 306–310.

Рецензія/Peer review : 26.1.2015 р. Надрукована/Printed :26.1.2015 р.
Рецензент: д.т.н., проф. Березький О.М.