DOI 10.15276/imms.v14.no4.324
УДК 519.7

Informatics and Mathematical Methods in Simulation
Vol.14 (2024), No. 4, pp. 324-334

МЕТОДИ ПОБУДОВИ ДОСКОНАЛОЇ ФОРМИ СИСТЕМИ ЗАЛИШКОВИХ КЛАСІВ НА МНОЖИНІ ЦІЛИХ КОМПЛЕКСНИХ ЧИСЕЛ

А. М. Алілуйко

Західноукраїнський національний університет
11, Львівська вул., Тернопіль, 46009, Україна
Email: aliluyko82@gmail.com

На даний час велика увага приділяється задачам підвищення швидкодії алгоритмів виконання операцій модулярної арифметики. Досить перспективною для застосування в сучасній теорії чисел, прикладній та обчислювальній математиці, а також асиметричній криптографії, є непозиційна система залишкових класів. Запропонована стаття присвячена розробці методів знаходження набору модулів досконалої форми системи залишкових класів в області цілих комплексних чисел, яке є розширенням множини цілих чисел. Вирішено актуальне завдання знаходження довільної кількості модулів досконалої форми цілочисельної комплексної системи залишкових класів на основі дробових перетворень та факторизації добутку чисел. Використання даного методу дозволяє суттєво зменшити обчислювальну складність при виконанні арифметичних операцій над комплексними числами шляхом розпаралелення процесу обчислень та переведення чисел із системи залишкових класів за рахунок виключення процедури пошуку зворотного елемента за модулем та множенням на базисні числа. Вперше отримано набори трьохмодульної досконалої форми комплексної системи залишкових класів. Визначено умови для знаходження будь-якої кількості модулів, які утворюють досконалу форму комплексної системи залишкових класів, два з яких невідомі. Наведено приклади використання запропонованих методів для досконалої форми системи залишкових класів, у якому отримані всі можливі набори комплексних модулів при заданому найменшому модулі. Представлені табличні значення та проаналізовано графічні залежності норм одержаних модулів. 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. Використання запропонованого методу підбору модулів, які утворюють досконалу форму, дозволить збільшити швидкодію обчислювальних систем, що працюють у системі залишкових класів.

Ключові слова: система залишкових класів, комплексне число, досконала форма, факторизація, китайська теорема про залишки

Вступ. На сучасному етапі розвитку інформаційних технологій непозиційні системи числення привертають все більшу увагу з метою використання їх при вирішенні ряду проблем та науково-технічних задач [1, 2]. Це пояснюється тим, що при виконанні значних обсягів обчислень в реальному часі суттєво проявляються недоліки двійкової системи (наприклад, наявність міжрозрядних зв'язків та велика розрядність [3]), які суттєво зменшують швидкодію обчислювальних систем [4].

Перераховані недоліки відсутні, наприклад, в системі залишкових класів (СЗК). Зокрема, СЗК ефективно використовується при виконанні цілочисельних операцій модулярної арифметики над багаторозрядними числами: додавання, віднімання, множення, піднесення до степеня [5] і т.д., що особливо актуально в задачах криптографії [4, 6]. Але вона також має певні недоліки (відсутність операцій ділення та порівняння [7], труднощі у виявленні умов переповнення розрядної сітки, складність зворотного перетворення чисел у десяткову систему числення). Безсумнівною перевагою СЗК є можливість виконання операцій над числами, які менші за вибрані модулі, та розпаралелення процесу обчислень. Крім того, використання досконалої (ДФ) [8-10] та модифікованої досконалої форм (МДФ) [11] СЗК дозволяє суттєво

спростити переведення чисел у позиційну системи числення.

Іншим напрямком підвищення швидкодії алгоритмів виконання операцій модулярної арифметики і стійкості комп'ютерних систем до різного виду атак є застосування більш складних структур, зокрема, цілих комплексних чисел або чисел Гауса. Завдяки ізоморфізму між кільцями цілих та комплексних чисел комплексна модулярна арифметика є перспективною для застосування в багатьох системах асиметричної криптографії.

Аналіз досліджень та публікацій. Аналіз наукових досліджень показує, що модулярні операції над цілими комплексними числами можуть успішно застосовуватися в асиметричних криптоалгоритмах RSA, Ель-Гамаля, Рабіна та їх модифікаціях, які раніше були сформульовані для дійсних цілих чисел.

В [12] продемонстровано переваги використання модифікованого алгоритму Ель-Гамаля на множині цілих комплексних чисел щодо підвищення його надійності. В [13, 14] було показано для системи RSA, що можна досягти значного зниження складності обчислень з цілими числами Гауса, але при цьому можливе зниження надійності алгоритму. В [15] зазначено переваги використання гаусівських цілих чисел для генерації відкритого ключа криптосистеми Рабіна. Це дозволило розробити відповідну арифметику для теореми Вільсона і китайської теореми про залишки (КТЗ), а також для обчислення символів Лежандра і квадратичних залишків. Криптографічну еліптичну криву над цілими числами Гауса розглядали в [16]. Крім того, в програмах кодування над цілими числами Гауса використовують цілочисельну арифметику Гауса [17].

При застосуванні комплексної системи залишкових класів (КСЗК) в задачах криптографії доводиться мати справу із подібними труднощами, як і при застосуванні цілочисельної СЗК. Зокрема, при зворотному перетворенні комплексних чисел із КСЗК на основі КТЗ необхідно виконувати громіздку процедуру пошуку оберненого елемента за комплексним модулем [18].

Виходячи із сказаного, актуальною науковою задачею є створення аналітичних методів пошуку комплексних модулів, які задовольняли б умовам ДФ КСЗК.

Мета роботи. Метою даної роботи є подальший розвиток теорії ДФ СЗК. Для досягнення поставленої мети в роботі вирішуються наступні задачі:

– розробка методів побудови ДФ СЗК в комплексній числовій області;

– визначення умов побудови всіх можливих варіантів для заданої кількості модулів ДФ КСЗК.

Основна частина. Теоретичні основи виконання арифметичних модулярних операцій на множині комплексних чисел заклав Гаус [19]. Аналогічно до традиційної асиметричної криптографії, доцільно розглядати тільки цілі комплексні числа (їх ще називають гаусовими), в яких дійсна та уявна частини є цілими. Будь-яке ціле комплексне число $\dot{A} = a + bi,\ a,b \in Z$ записується в СЗК єдиним способом у вигляді набору своїх найменших або абсолютно найменших комплексних залишків $\dot{b}_j$ від ділення $\dot{A}$ на кожен із системи $\dot{M}$ попарно взаємно простих комплексних модулів $\dot{m}_1, \dot{m}_2, \ldots, \dot{m}_n$:

$$\dot{b}_j = \dot{A} \bmod \dot{m}_j, \quad j = \overline{1,n}.$$

При цьому для подання числа $\dot{A}$ в системі $\dot{M}$ найменших залишків, необхідно і достатньо, щоб виконувалися нерівності

$$0 \le ap_M + bq_M < N(\dot{M}),\ \ 0 \le bp_M - aq_M < N(\dot{M}),$$

а в системі $\dot{M}$ абсолютно найменших залишків –

$$\left|ap_M + bq_M\right| \le \frac{1}{2} N(\dot{M}),\ \ \left|bp_M - aq_M\right| \le \frac{1}{2} N(\dot{M}), \qquad (1)$$

де $N(\dot{M})$ – норма комплексного числа $\dot{M} = \prod_{j=1}^{n} \dot{m}_j = p_M + q_M i$.

Відновлення числа $\dot{A}$ з СЗК можна здійснити на основі КТЗ в комплексній числовій області:

$$\dot{A} = \left(\sum_{j=1}^{n} \dot{b}_j \dot{M}_j \dot{f}_j \right) \bmod \dot{M}, \tag{2}$$

де $\dot{M}_j = \dfrac{\dot{M}}{\dot{m}_j}$, $\dot{f}_j$ шукається з виразу $\left(\dot{M}_j \dot{f}_j\right) \bmod \dot{m}_j = 1,\ j = \overline{1,n}$.

Слід зазначити, що пошук обернених мультиплікативних елементів $\dot{f}_j = \dot{M}_j^{-1} \bmod \dot{m}_j$ становить значну обчислювальну складність, який реалізується, наприклад, з допомогою алгоритму Евкліда або використання аналогу функції Ейлера в комплексній числовій області [18]. У роботах [8, 9] було запропоновано ДФ цілочисельної СЗК, у якій здійснювався підбір цілих модулів таким чином, щоб їм відповідали одиничні коефіцієнти $f_j = 1,\ j = \overline{1,n}$.

За аналогією розглянемо побудову ДФ КСЗК, у якій підбір комплексних модулів такий, що

$$\dot{M}_j \bmod \dot{m}_j = 1,\ j = \overline{1,n}, \tag{3}$$

тобто $\dot{f}_j = 1$. Це дозволяє уникнути пошуку обернено елемента і множення в (2) на $\dot{f}_j$. Вираз (2) в цьому випадку спрощується: $\dot{A} = \left(\sum_{j=1}^{n} \dot{b}_j \dot{M}_j \right) \bmod \dot{M}$.

Запишемо вираз (3) у вигляді системи:

$$\begin{cases} \dot{M}_1 \bmod \dot{m}_1 = 1, \\ \cdots \\ \dot{M}_n \bmod \dot{m}_n = 1. \end{cases} \tag{4}$$

Спочатку дослідимо систему з трьох модулів. Для цього задамо модулі $\dot{m}_1$, $\dot{m}_2$ у вигляді: $\dot{m}_2 = a\dot{m}_1 + b$, $\dot{m}_3 = c\dot{m}_1\dot{m}_2 + d = c\dot{m}_1(a\dot{m}_1 + b) + d$, де a і c – натуральні числа, b і d – цілі числа, причому вважаємо, що $N(\dot{m}_1) < N(\dot{m}_2) < N(\dot{m}_3)$. Тоді з (4) отримуємо:

$$\begin{cases} ((a\dot{m}_1 + b)(c\dot{m}_1(a\dot{m}_1 + b) + d)) \bmod \dot{m}_1 = 1, \\ (\dot{m}_1(c\dot{m}_1(a\dot{m}_1 + b) + d)) \bmod (a\dot{m}_1 + b) = 1, \\ (\dot{m}_1(a\dot{m}_1 + b)) \bmod (c\dot{m}_1(a\dot{m}_1 + b) + d) = 1. \end{cases} \tag{5}$$

Третє рівняння системи (5) має місце, якщо, зокрема, добуток $\dot{m}_1(a\dot{m}_1 + b)$ на одиницю більший від значення модуля $c\dot{m}_1(a\dot{m}_1 + b) + d$. Звідси слідує, що $c = 1$, $d = -1$. З другого рівняння бачимо, що $(\dot{m}_1(a\dot{m}_1 + b) - 1) \bmod (a\dot{m}_1 + b) = -1$, тому повинна виконуватися умова $\dot{m}_1 \bmod (a\dot{m}_1 + b) = -1$. Це можливо, якщо $a = 1$, $b = 1$. Тоді система (5) набуде такого вигляду:

$$\begin{cases} ((\dot{m}_1 + 1)(\dot{m}_1(\dot{m}_1 + 1) - 1)) \bmod \dot{m}_1 = 1, \\ (\dot{m}_1(\dot{m}_1(\dot{m}_1 + 1) - 1)) \bmod (\dot{m}_1 + 1) = 1, \\ (\dot{m}_1(\dot{m}_1 + 1)) \bmod (\dot{m}_1(\dot{m}_1 + 1) - 1) = 1. \end{cases} \tag{6}$$

З першого рівняння системи (6) видно, що $(\dot{m}_1(\dot{m}_1 + 1) - 1)) \bmod \dot{m}_1 = -1$. Тоді має виконуватися умова $(\dot{m}_1 + 1) \bmod \dot{m}_1 = -1$ або $1 \bmod \dot{m}_1 = -1$.

Якщо позначити $\dot{m}_1 = x + yi$, то отримаємо таку систему рівнянь

$$\begin{cases} x \bmod (x^2 + y^2) = -x, \\ y \bmod (x^2 + y^2) = -y, \end{cases} \tag{7}$$

яка має розв'язок при $x = \pm 1$, $y = \pm 1$. Отже, вірним є співвідношення $i^k \bmod \dot{m}_1 = i^l$, де $k, l = \overline{0,3}$ при $\dot{m}_1 = \{1+i; 1-i; -1+i; -1-i\}$.

Враховуючи нерівність $N(\dot{m}_1) < N(\dot{m}_2) < N(\dot{m}_3)$, отримуємо такі два єдині набори трьох модулів для ДФ КСЗК: $\{1+i; 2+i; 3i\}$ та $\{1-i; 2-i; -3i\}$.

Метод побудови ДФ КСЗК на основі дробових перетворень. Помноживши кожне рівняння (4) на відповідний модуль, отримаємо:

$$\begin{cases} \dot{M} \bmod \dot{m}_1^2 = \dot{m}_1, \\ \quad \cdots \\ \dot{M} \bmod \dot{m}_n^2 = \dot{m}_n. \end{cases} \tag{8}$$

Використовуючи властивості конгруенцій до системи (8) та КТЗ в комплексній числовій області, матимемо:

$$\dot{M} = \left(\sum_{j=1}^{n} \dot{m}_j \dot{M}_j \dot{f}_j^2 \right) \bmod \dot{P}, \tag{9}$$

де $\dot{P} = \prod_{j=1}^{n} \dot{m}_j^2 = \dot{M}^2$.

Врахувавши, що у ДФ КСЗК $\dot{f}_j = 1$, та скоротивши модуль, ліву та праву частини (8) на їх спільний дільник $\dot{M} = \prod_{j=1}^{n} \dot{m}_j$, перепишемо (9) таким чином:

$$\left(\sum_{j=1}^{n} \dot{M}_j \right) \bmod \dot{M} = 1. \tag{10}$$

Вираз (10) еквівалентний рівності:

$$\sum_{j=1}^{n} \dot{M}_j = \dot{\gamma} \dot{M} + 1, \tag{11}$$

де $\dot{\gamma}$ – ціле комплексне число.

Поділивши ліву та праву частини (11) на $\dot{M}$, отримаємо остаточний вираз для пошуку набору модулів у ДФ КСЗК:

$$\sum_{j=1}^{n} \frac{1}{\dot{m}_j} = \dot{\gamma} + \frac{1}{\prod_{j=1}^{n} \dot{m}_j}. \tag{12}$$

Дослідження рівняння (12) для великої кількості модулів та великого $\dot{\gamma}$ є досить громіздким.

В (12) перенесемо доданок $\frac{1}{m_1}$ вправо. Тоді маємо

$$\frac{1}{\dot{m}_2} + \frac{1}{\dot{m}_3} + \ldots + \frac{1}{\dot{m}_n} = \dot{\gamma} - \frac{1}{\dot{m}_1} + \frac{1}{\dot{m}_1 \dot{m}_2 \dot{m}_3 \ldots \dot{m}_n}. \tag{13}$$

Нехай

$$\dot{\gamma} - \frac{1}{\dot{m}_1} = \frac{s}{\dot{m}_1}, \tag{14}$$

де s – натуральне число, вибір якого дозволяє знайти модуль $\dot{m}_1$ з найменшою нормою.

Знов в (13) перенесемо доданок $\frac{1}{\dot{m}_2}$ вправо. Тоді маємо

$$\frac{1}{\dot{m}_3}+\ldots+\frac{1}{\dot{m}_n}=\dot{\gamma}-\frac{1}{\dot{m}_1}-\frac{1}{\dot{m}_2}+\frac{1}{\dot{m}_1\dot{m}_2\dot{m}_3\ldots\dot{m}_n}. \tag{15}$$

Нехай

$$\dot{\gamma}-\frac{1}{\dot{m}_1}-\frac{1}{\dot{m}_2}=\frac{s}{\dot{m}_1\dot{m}_2}. \tag{16}$$

З (14) та (16) маємо співвідношення:

$$\dot{\gamma}=\frac{s+1}{\dot{m}_1} \text{ та } \dot{m}_2=\frac{s+\dot{m}_1}{s}. \tag{17}$$

Якщо прийняти, що модулі $\dot{m}_1$, $\dot{m}_2$ та $\dot{\gamma}$ є натуральними, то із (17) слідує, що одночасно $\dot{m}_1$ кратне s і $s+1$ кратне $\dot{m}_1$. Це можливо лише при $\dot{m}_1=2$, $s=1$, $\gamma=1$. Такий випадок, детально описано в [10]. Зокрема, отримано ДФ СЗК з цілими модулями при $n=6$ (2, 3, 7, 43, 1807, 3263441, $M=1,0650050423922\times10^{13}$).

Знайдемо можливі комплексні значення $\dot{m}_i$, $\dot{\gamma}$ та натурального s, для яких можуть виконуватися співвідношення (17).

Нехай $\dot{m}_1=x+yi$, $y\neq0$. Тоді $\dot{\gamma}=\frac{s+1}{x+yi}=\frac{s+1}{x^2+y^2}(x-yi)$. Вираз $\frac{s+1}{x^2+y^2}$ повинен мати ціле значення, тому $|s+1|\geq x^2+y^2$.

Друге співвідношення в (17) матиме вигляд $\dot{m}_2=\frac{s+x+yi}{s}=1+\frac{x}{s}+\frac{y}{s}i$. Оскільки $\frac{x^2}{s^2}\geq0$, $\frac{y^2}{s^2}\geq1$, то $x^2+y^2\geq s^2$. Таким чином отримали подвійну нерівність $|s+1|\geq x^2+y^2\geq s^2$, яка виконується лише для одного натурального значення $s=1$ та одного з чотирьох комплексних чисел $\dot{m}_1=\pm1\pm i$ з нормою $N(\dot{m}_1)=2$. Тоді для кожного $\dot{m}_1=\{1+i;1-i;-1+i;-1-i\}$ є відповідне значення $\dot{\gamma}=\frac{2}{\dot{m}_1}=\{1-i;1+i;-1-i;-1+i\}$. Взявши $s=1$, отримаємо $\dot{m}_2=1+\dot{m}_1$.

Якщо в (15) знову перенести доданок $\frac{1}{\dot{m}_3}$ вправо, то з співвідношень $\dot{\gamma}-\frac{1}{\dot{m}_1}-\frac{1}{\dot{m}_2}-\frac{1}{\dot{m}_3}=\frac{1}{\dot{m}_1\dot{m}_2\dot{m}_3}$ та $\dot{\gamma}=\frac{2}{\dot{m}_1}$ $(s=1)$ отримаємо формулу $\dot{m}_3=1+\dot{m}_1\dot{m}_2$. При перенесенні кожного разу в праву частину (11) доданка $\frac{1}{\dot{m}_j}$ вважаємо, що у виразі $\dot{\gamma}-\frac{1}{\dot{m}_1}-\frac{1}{\dot{m}_2}-\frac{1}{\dot{m}_3}-\ldots-\frac{1}{\dot{m}_j}=\frac{s}{\dot{m}_1\dot{m}_2\dot{m}_3\ldots\dot{m}_j}$ завжди $s=1$.

Для останнього модуля $\dot{m}_n$ справедлива рівність

$$\frac{1}{\dot{m}_n}=\frac{1}{\prod_{j=1}^{n-1}\dot{m}_j}+\frac{1}{\dot{m}_n\cdot\prod_{j=1}^{n-1}\dot{m}_j}.$$

Звідси отримуємо, що $\dot{m}_n=\prod_{j=1}^{n-1}\dot{m}_j-1$.

Отже, остаточний вираз для побудови системи модулів ДФ КСЗК при $N(\dot{m}_1) < N(\dot{m}_2) < \ldots < N(\dot{m}_n)$ має такий вигляд:

$$\begin{cases} \dot{m}_1 = 1 \pm i, \\ \dot{m}_k = \prod_{j=1}^{k-1} \dot{m}_j + 1,\ 1 < k < n, \\ \dot{m}_n = \prod_{j=1}^{n-1} \dot{m}_j - 1. \end{cases} \tag{18}$$

Зауважимо, що запропонований в (18) метод не вичерпує всіх можливих наборів модулів ДФ КСЗК при заданих n. Наприклад, при $n = 5$ набір комплексних модулів, отриманий за допомогою (18), буде такий: $1+i$, $2+i$, $2+3i$, $-6+9i$, $-40-117i$. Але можна навести інші набори, зокрема: $1+i$, $2+i$, $2+3i$, $-10+9i$, $4+51i$.

Побудова ДФ КСЗК методом факторизації. Вважаючи, що два останні модулі в рівності (12) невідомі, після відповідних математичних перетворень отримаємо наступне співвідношення:

$$(\dot{m}_{n-1} + \dot{m}_n) \prod_{j=1}^{n-2} \dot{m}_j + \dot{m}_{n-1}\dot{m}_n \prod_{j=1}^{n-2} \dot{m}_j \left(\sum_{k=1}^{n-2} \frac{1}{\dot{m}_k} - \dot{\gamma} \right) = 1. \tag{19}$$

Введемо заміну:

$$\dot{m}_{n-1}, \dot{m}_n = \frac{\dot{a}, \dot{b} - \prod_{j=1}^{n-2} \dot{m}_j}{\prod_{j=1}^{n-2} \dot{m}_j \left(\sum_{k=1}^{n-2} \frac{1}{\dot{m}_k} - \dot{\gamma} \right)}. \tag{20}$$

Після підстановки (20) в (19) отримуємо умову, яка виконується для заданих наборів модулів ДФ КСЗК:

$$\dot{a}\dot{b} = \prod_{j=1}^{n-2} \dot{m}_j \left(\sum_{k=1}^{n-2} \frac{1}{\dot{m}_k} - \dot{\gamma} + \prod_{j=1}^{n-2} \dot{m}_j \right). \tag{21}$$

Для знаходження параметрів $\dot{a}$ і $\dot{b}$ потрібно факторизувати праву частину співвідношення (21). Оскільки модулі $\dot{m}_{n-1}$ та $\dot{m}_n$ цілі комплексні, то з (20) слідують наступні рівності:

$$\left(\dot{a}, \dot{b} - \prod_{j=1}^{n-2} \dot{m}_j \right) \bmod \left(\prod_{j=1}^{n-2} \dot{m}_j \left(\sum_{k=1}^{n-2} \frac{1}{\dot{m}_k} - \dot{\gamma} \right) \right) = 0. \tag{22}$$

Отже, вирази (21) та (22) визначають умови для знаходження довільної кількості модулів ДФ КСЗК, два з яких невідомі.

Нехай $n = 5$, $\dot{\gamma} = 1 - i$ і $\dot{m}_1 = 1+i$, $\dot{m}_2 = 2+i$, $\dot{m}_3 = 2+3i$, отримані з (18). Тоді вирази (20) та (21) будуть мати вигляд:

$$\dot{m}_4 = -7 + 9i - \dot{a},\ \dot{m}_5 = -7 + 9i - \dot{b},\ \dot{a}\dot{b} = -33 - 126i. \tag{23}$$

Права частина останньої рівності в (23) має бути факторизована, на основі чого визначаються параметри $\dot{a}$ та $\dot{b}$. Оскільки $\dot{m}_4$ та $\dot{m}_5$ цілі комплексні числа, то $\dot{a}$ та $\dot{b}$ також мають бути цілими комплексними числами.

Для знаходження $\dot{a}$ та $\dot{b}$ скористаємося властивістю мультиплікативності норми комплексного числа. Тоді має місце розклад:

$$N(\dot{a}) \cdot N(\dot{b}) = N(\dot{a} \cdot \dot{b}) = 16965 = 3 \cdot 3 \cdot 5 \cdot 13 \cdot 29. \tag{24}$$

Використавши всеможливі перестановки множників у (24), можна отримати 12

можливих варіантів наборів для $N(\dot{a})$, $N(\dot{b})$ (табл. 1).

Для знаходження параметра $\dot{a}$ потрібно враховувати, що $N(\dot{a})$ дорівнює сумі квадратів дійсної та уявної частин цілого комплексного числа $\dot{a}$. А з теорії чисел відомо, що числа виду $4k+1$, $k \in N$ можна розкласти в суму двох квадратів. Відповідно до цього можливі значення параметра $\dot{a}$ наведено в таблиці 1.

Таблиця 1.

Можливі значення для $\dot{a}$, $N(\dot{a})$, $N(\dot{b})$

$N(\dot{a})$	$\dot{a}$	$N(\dot{b})$	$N(\dot{a})$	$\dot{a}$	$N(\dot{b})$
1	$\pm 1; \pm i$	$3\cdot3\cdot5\cdot13\cdot29 = 16965$	29	$\pm 2 \pm 5i;$ $\pm 5 \pm 2i$	$3\cdot3\cdot5\cdot13 = 585$
3		$3\cdot5\cdot13\cdot29 = 5655$	$3\cdot13 = 39$		$3\cdot5\cdot29 = 435$
5	$\pm 1 \pm 2i;$ $\pm 2 \pm i$	$3\cdot3\cdot13\cdot29 = 3393$	$3\cdot3\cdot5 = 45$	$\pm 3 \pm 6i;$ $\pm 6 \pm 3i$	$13\cdot29 = 377$
$3\cdot3 = 9$	$\pm 3; \pm 3i$	$5\cdot13\cdot29 = 1885$	$5\cdot13 = 65$	$\pm 1 \pm 8i;$ $\pm 8 \pm i;$ $\pm 4 \pm 7i;$ $\pm 7 \pm 4i$	$3\cdot3\cdot29 = 261$
13	$\pm 2 \pm 3i;$ $\pm 3 \pm 2i$	$3\cdot3\cdot5\cdot29 = 1305$	$3\cdot29 = 87$		$3\cdot5\cdot13 = 195$
$3\cdot5 = 15$		$3\cdot13\cdot29 = 1131$	$3\cdot3\cdot13 = 117$	$\pm 6 \pm 9i;$ $\pm 9 \pm 6i$	$5\cdot29 = 145$

Використовуючи співвідношення в (24) та умову цілочисельності параметра $\dot{b}$, отримуємо 32 можливих наборів з 5 модулів ДФ КСЗК при заданих $1+i$, $2+i$, $2+3i$, які наведені в таблиці 2. Причому, одному і тому ж значенню $N(\dot{a})$ відповідають різні модулі $\dot{m}_4$ та $\dot{m}_5$, що дозволяє змінювати діапазон комплексних чисел.

На рисунку 1 показано характер зміни максимальних та мінімальних значень норм $N(\dot{m}_4)$ та $N(\dot{m}_5)$ залежно від номера норми $N(\dot{a})$, відповідно до таблиці 2 у логарифмічній шкалі. Як видно з рисунка, максимальні значення норм $N(\dot{m}_4)$ зростають, а мінімальні $N(\dot{m}_4)$ спадають приблизно з однаковою інтенсивністю. В той же час, мінімальні значення $N(\dot{m}_5)$ із збільшенням номера норми спадають інтенсивніше, ніж максимальні $N(\dot{m}_5)$.

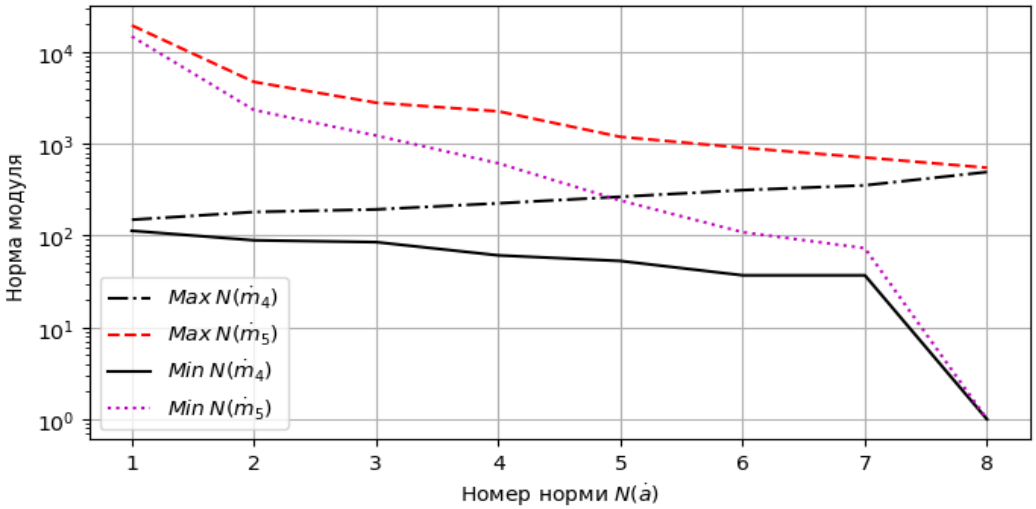

Рис. 1. Характер зміни значень норм $N(\dot{m}_4)$ та $N(\dot{m}_5)$ залежно від номера норми $N(\dot{a})$

Таблиця 2.

Можливі варіанти наборів з 5 модулів ДФ КСЗК при заданих $1+i,\ 2+i,\ 2+3i$

№	$N(\dot{a})$	$\dot{a}$	$\dot{b}$	$\dot{m}_4$	$N(\dot{m}_4)$	$\dot{m}_5$	$N(\dot{m}_5)$
1	1	1	– 33 – 126*i*	– 8 + 9*i*	145	26 + 135*i*	18901
		– 1	33 + 126*i*	–6 + 9*i*	117	– 40 – 117*i*	15289
		i	– 126 + 33*i*	– 7 + 8*i*	113	119 – 24*i*	14737
		– *i*	126 – 33*i*	– 7 + 10*i*	149	– 133 + 42*i*	19453
2	5	1 + 2*i*	– 57 – 12*i*	– 8 + 7*i*	113	50 + 21*i*	2941
		– 1 – 2*i*	57 + 12*i*	– 6 +11*i*	157	– 64 – 3*i*	4105
		2 – *i*	12 – 57*i*	– 9 +10*i*	181	– 19 + 66*i*	4717
		– 2 + *i*	– 12 + 57*i*	– 5 + 8*i*	89	5 – 48*i*	2329
3	9	3	– 11 – 42*i*	– 10 + 9*i*	181	4 + 51*i*	2617
		– 3	11 + 42*i*	– 4 + 9*i*	97	– 18 – 33*i*	1413
		3*i*	– 42 + 11*i*	– 7 + 6*i*	85	35 – 2*i*	1229
		– 3*i*	42 – 11*i*	– 7 + 12*i*	193	– 49 + 20*i*	2801
4	13	2 – 3*i*	24 – 27*i*	– 9 + 12*i*	225	– 31 + 36*i*	2257
		– 2 + 3*i*	– 24 + 27*i*	– 5 + 6*i*	61	17 – 18*i*	613
		3 + 2*i*	– 27 – 24*i*	– 10 + 7*i*	149	20 + 33*i*	1489
		– 3 – 2*i*	27 + 24*i*	– 4 + 11*i*	137	– 34 – 15*i*	1381
5	29	2 + 5*i*	– 24 – 3*i*	– 9 +4*i*	97	17 + 12*i*	433
		– 2 – 5*i*	24 + 3*i*	– 5 + 14*i*	221	– 31 + 6*i*	997
		5 – 2*i*	3 – 24*i*	– 12 + 11*i*	265	– 10 + 33*i*	1189
		– 5 + 2*i*	– 3 + 24*i*	– 2 + 7*i*	53	– 4 – 15*i*	241
6	45	3 + 6*i*	– 19 – 4*i*	– 10 + 3*i*	109	12 + 13*i*	313
		– 3 – 6*i*	19 + 4*i*	– 4 + 15*i*	241	– 26 + 5*i*	701
		6 – 3*i*	4 – 19*i*	– 13 + 12*i*	313	– 11 + 28*i*	905
		– 6 + 3*i*	– 4 + 19*i*	– 1 + 6*i*	37	– 3 – 10*i*	109
7	65	1 – 8*i*	15 – 6*i*	– 8 + 17*i*	353	– 22 + 15*i*	709
		– 1 + 8*i*	– 15 + 6*i*	– 6 + *i*	37	8 + 3*i*	73
		8 + *i*	– 6 – 15*i*	– 15 + 8*i*	289	– 1 + 24*i*	577
		– 8 – *i*	6 + 15*i*	1 + 10*i*	101	– 13 – 6*i*	205
8	117	6 – 9*i*	8 – 9*i*	– 13 + 18*i*	493	– 15 + 18*i*	549
		– 6 + 9*i*	– 8 + 9*i*	– 1	1	1	1
		9 + 6*i*	– 9 – 8*i*	– 16 + 3*i*	265	2 + 17*i*	293
		– 9 – 6*i*	9 + 8*i*	2 + 15*i*	229	– 16 + *i*	257

На рисунку 1 показано характер зміни максимальних та мінімальних значень норм $N(\dot{m}_4)$ та $N(\dot{m}_5)$ залежно від номера норми $N(\dot{a})$, відповідно до таблиці 2 у логарифмічній шкалі. Як видно з рисунка, максимальні значення норм $N(\dot{m}_4)$ зростають, а мінімальні $N(\dot{m}_4)$ спадають приблизно з однаковою інтенсивністю. В той же час, мінімальні значення $N(\dot{m}_5)$ із збільшенням номера норми спадають інтенсивніше, ніж максимальні $N(\dot{m}_5)$.

Застосування ДФ КСЗК у китайській теоремі про залишки. Застосуємо КТЗ до взаємно простих комплексних чисел $\dot{m}_1 = 1+i,\ \dot{m}_2 = 2+i,\ \dot{m}_3 = 2+3i,\ \dot{m}_4 = -6+9i,$ $\dot{m}_5 = -40-117i$, які є основами системи $\dot{M} = \dot{m}_1 \cdot \dot{m}_2 \cdot \dot{m}_3 \cdot \dot{m}_4 \cdot \dot{m}_5 = -12129+9243i$. Спочатку число $\dot{A} = -7+2i$ запишемо в СЗК у вигляді своїх абсолютно найменших комплексних залишків:

$$\dot{b}_1 = \dot{A} \bmod \dot{m}_1 = i,\quad \dot{b}_2 = \dot{A} \bmod \dot{m}_2 = -1,\quad \dot{b}_3 = \dot{A} \bmod \dot{m}_3 = 1+i,$$

$$\dot{b}_4 = \dot{A} \bmod \dot{m}_4 = -1-7i\,,\ \ \dot{b}_5 = \dot{A} \bmod \dot{m}_5 = -7-2i\,.$$

Для $\dot{M}_1 = \dfrac{\dot{M}}{\dot{m}_1} = -1443+10686i$, $\dot{M}_2 = \dfrac{\dot{M}}{\dot{m}_2} = -3003+6123i$, $\dot{M}_3 = \dfrac{\dot{M}}{\dot{m}_3} = 267+4221i$, $\dot{M}_4 = \dfrac{\dot{M}}{\dot{m}_4} = 1333+459i$, $\dot{M}_5 = \dfrac{\dot{M}}{\dot{m}_5} = -39-117i$ обернені елементи за відповідними модулями відомі $\dot{f}_j = \dot{M}_j^{-1} \bmod \dot{m}_j = 1$, $j = \overline{1,5}$. Тут $N(\dot{M}) = 232545690$ і виконуються обмеження (1): $ap_M + bq_M = 103389 < 116272845,\ bp_M - aq_M = 40443 < 116272845$.

Число $\dot{A}$ відновлюється з СЗК за формулою (2):

$$\dot{A} = (i(-1443+10686i) - 1(-3003+6123i) + (1+i)(267+4221i) + (-1-7i)(1333+459i) +$$
$$+(-7-2i)(-39-117i) \bmod(-12129+9243\mathrm{i}) = (-9250-12124i) \bmod(-12129+9243\mathrm{i}) = -7+2i.$$

Отже, число $\dot{A}$ з СЗК відновлюється за допомогою КТЗ без виконання громіздкої операції пошуку оберненого елемента за модулем, а використовуючи операції цілочисельного додавання, множення, та модулярних обчислень в комплексній числовій області.

Висновки. У роботі розв'язано задачу побудови досконалої форми системи залишкових класів на множині цілих комплексних чисел, де відсутня процедура пошуку зворотного елемента по модулю.

Наукова новизна результатів, одержаних у статті, полягає в тому, що вперше запропоновано метод побудови досконалої форми комплексної системи залишкових класів на основі дробових перетворень та факторизації, в якій відсутні операції пошуку оберненого елемента за модулем і множення на базисні числа. Оскільки такі операції характеризуються великою обчислювальною складністю, то отримані методи дозволяють спростити виконання арифметичних операцій над цілими комплексними числами шляхом розпаралелювання процесу обчислень та переведення чисел із системи залишкових класів.

Практична значимість одержаних результатів полягає в тому, що використання запропонованого методу підбору модулів, що утворюють досконалу форму, дозволить збільшити швидкодію обчислювальних систем, що працюють у системі залишкових класів.

Перспективи подальших досліджень полягають у тому, щоб визначити умови для знаходження модулів модифікованої досконалої форми системи залишкових класів, а також програмна та апаратна реалізація запропонованих та запланованих методів.

Список літератури

1. Ananda Mohan P. V. Residue Number Systems: Theory and Applications, Birkhäuser, Basel, 2016. 351 p. URL: http://www.springer.com/978-3-319-41383-9
2. Краснобаєв В., Кошман С., Никольський С., Ковальчук Д. Математична модель надійності комп'ютерної системи у залишкових класах. *Сучасні інформаційні системи*. 2022. Т.6, №4. С. 19–24. URL: https://doi.org/10.20998/2522-9052.2022.4.03
3. Касянчук М., Карпінський М., Казмірчук С. Методологія опрацювання багаторозрядних чисел в асиметричних криптосистемах. *Захист інформації*. 2019. Т.21, №2. С. 65–73. URL: http://dx.doi.org/10.18372/2410-7840.21.13764
4. Adki V., Hatkar S. A Survey on Cryptography Techniques. *International Journal of Advanced Research in Computer Science and Software Engineering*. 2016. V.6, No.6. P. 469–475.
5. Задірака В.К., Терещенко А.М. Комп'ютерна арифметика багаторозрядних чисел у послідовній та паралельній моделях обчислень : монографія. Київ : Наук. думка, 2021. 136 с.

6. Касянчук М.М., Якименко І.З., Івасьєв С.В. Криптосистема Рабіна на основі операції додавання. *Математичне та комп'ютерне моделювання: Технічні науки*. 2019. Вип.19. С.145-150. URL: https://doi.org/10.32626/2308-5916.2019-19.145-150
7. Krasnobayev V.A., Yanko A.S., Koshman S.A. A Method for Arithmetic Comparison of Data Represented in a Residue Number System. *Cybernetics and Systems Analysis*. 2016. V. 52, No. 1. P. 145–150. URL: https://doi.org/10.1007/s10559-016-9809-2
8. Касянчук М. М. Теорія та математичні закономірності досконалої форми системи залишкових класів // Питання оптимізації обчислень. *XXXV Міжнародний симпозіум, Кацивелі*. Київ: Інститут кібернетики ім. В. М. Глушкова. 2009. С. 306–310.
9. 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*. 2014. V. 50, No. 5. P. 649–654. URL: https://doi.org/10.1007/s10559-014-9654-0
10. Касянчук М. М., Якименко І. З., Паздрій І. Р., Николайчук Я.М. Аналітичний пошук модулів досконалої форми системи залишкових класів та їх використання в китайській теоремі про залишки. *Вісник Хмельницького національного університету : технічні науки*. 2015. Т. 221, № 1. С. 170–176. URL: http://journals.khnu.km.ua/vestnik/pdf/tech/2015_1/(221)%202015-1-t.pdf
11. Kasianchuk M., Nykolaychuk Ya., Yakymenko I. Theory and Methods of Constructing of Modules System of the Perfect Modified Form of the System of Residual Classes. *Journal of Automation and Information Sciences*. 2016. V. 48, No 8. P. 56-63. URL: https://doi.org/10.1615/JAUTOMATINFSCIEN.V48.I8.60
12. El-Kassar A., Rizk M., Mirza N., Awad Y. El-Gamal Public-Key Cryptosystem in the Domain of Gaussian Integers. *International Journal of Applied Mathematics*. 2001. V. 7, No. 4. P. 405–412. URL: https://www.researchgate.net/publication/266001078_El-Gamal_public_key_cryptosystem_in_the_domain_of_Gaussian_integers
13. Koval A., Verkhovsky B.S. Analysis of RSA over Gaussian Integers Algorithm. *Fifth International Conference on Information Technology: New Generations (ITNG)*, Las Vegas, NV, USA, 2008. P. 101–105. URL: https://doi.org/10.1109/ITNG.2008.44
14. Koval A. Algorithm for Gaussian Integer Exponentiation. In Information Technology: New Generations. Berlin/Heidelberg: Springer International Publishing, 2016. P. 1075–1085. URL: https://doi.org/10.1007/978-3-319-32467-8_93
15. Awad Y., El-Kassar A.N., Kadri T. Rabin Public-Key Cryptosystem in the Domain of Gaussian Integers. *Proceedings of the International Conference on Computer and Applications (ICCA)*, Beirut, Lebanon. 2018. P. 336–340. URL: https://doi.org/10.1109/COMAPP.2018.8460338
16. Safieh M., Thiers J., Freudenberger J. A Compact Coprocessor for the Elliptic Curve Point Multiplication over Gaussian Integers. *Electronics*. 2020, V. 9, P. 1–21. URL: https://doi.org/10.3390/electronics9122050
17. Rohweder D., Freudenberger J., Shavgulidze S. Low-Density Parity-Check Codes over Finite Gaussian Integer Fields. *Proceedings of the 2018 IEEE International Symposium on Information Theory (ISIT)*, Vail, CO, USA. 2018. P. 481–485. https://doi.org/10.1109/ISIT.2018.8437456
18. Алілуйко А.М., Касянчук М.М. Арифметика асиметричних криптосистем в полі комплексних чисел. *Захист інформації*. 2024. Т. 26, № 1. С. 35–43. URL: https://doi.org/10.18372/2410-7840.26.18825
19. Gauss C. F., Theoria Residuorum Biquadraticorum, Commentatio Secunda, in Werke, Band II. Koniglichen Gesellschaft der Wissenschaften zu Göttingen, 1876. P. 93-148. URL: https://archive.org/details/117771763_002/page/n103/mode/2up

METHODS FOR CONSTRUCTING THE PERFECT FORM OF RESIDUE NUMBER SYSTEM ON THE SET OF COMPLEX INTEGERS

Aliluiko A. M.

West Ukrainian National University
11, Lvivska str., Ternopil, 46009, Ukraine
Email: aliluyko82@gmail.com

So much attention is paid to the tasks of increasing the speed of algorithms for performing modular arithmetic operations. The non-positional residue number system is quite promising for application in modern number theory, applied and computational mathematics, and asymmetric cryptography. This article is focused on the development of methods for finding a set of modules of a perfect-form residue number system in the domain of complex integers, which is an extension of the set of integers. A relevant problem has been solved: finding an arbitrary number of modules of the perfect form of an integer complex residue number system based on fractional transformations and factorization of the product of numbers. The use of this method allows for a significant reduction in computational complexity during arithmetic operations on complex numbers by parallelizing the computation process and converting numbers within the residue number system, eliminating the procedure of finding the inverse element modulo and multiplication by base numbers. Sets of three-module perfect form of the complex residue number system were obtained for the first time. Conditions have been determined for finding any number of modules of modified perfect form of a complex residue number system, with two of them are unknown. Examples of the application of the proposed methods for the perfect form of the residue number system are provided, in which all possible sets of complex modules are obtained for a given smallest module. Tabular values of the obtained modulus norms are presented and their graphical dependencies are analyzed. The results of the conducted research demonstrate that the proposed method significantly reduces the computational complexity of the Chinese Remainder Theorem by avoiding the operation of finding the inverse element modulo. The use of the proposed method for selecting modules that form a perfect form will increase the performance of computational systems operating within the residue number system.

Keywords: residue number system, complex number, perfect form, factorization, the Chinese Remainder Theorem