УДК 681.04 DOI: 10.26565/2519-2310-2021-1-01

МЕТОД ВИКОНАННЯ ОПЕРАЦІЇ ДОДАВАННЯ ЗАЛИШКІВ ЧИСЕЛ ЗА МОДУЛЕМ

Віктор Краснобаев, Катерина Кузнецова, Михайло Багмут

Харківський національний університет імені В.Н. Каразіна, майдан Свободи, 4, Харків, 61022, Україна
v.a.krasnobaev@gmail.com, kate7smith12@gmail.com, mikhail56@ukr.net

Рецензент: В'ячеслав Калашников, д. ф.-м.н., проф., Технологічний університет Монтеррея, 64849 Монтеррей, Нуево-Леон, Мексика
kalash@itesm.mx

Надійшло: Листопад 2020.

Анотація: *Суматор двох чисел є одним з компонентів комп'ютерної системи (КС) в позиційній двійковій системі числення (ПСЧ). Зокрема, компонентами КС є також суматори за модулем m_i двох чисел. Даний тип суматори за модулем широко використовуються як в ПСЧ, так і в позиційній системі числення в залишкових класах (СЗК). Важливою і актуальною науково-прикладною задачею є завдання побудови суматорів, що працюють за довільним модулем m_i СЗК. Якщо залишки a_i і b_i чисел A і B в СЗК, представлені в двійковій ПСЧ, тоді акумулятор двох залишків a_i і b_i по модулю m_i є послідовна сукупність з двійкових однорозрядних суматорів (ДОС). Метою статті є розробка методу виконання операції модульного додавання $(a_i + b_i) \bmod m_i$ залишків двох залишків чисел, за довільним модулем на основі використання позиційного двійкового суматора за модулем $M = 2^n - 1$. Запропонований в статті метод виконання операції модульного додавання, заснований на використанні відомої структури позиційних двійкових суматорів за модулем $M = 2^n - 1$. Технічно, завдання побудови структури суматора полягає в необхідності забезпечити умови, при яких вихідний суматор в ПСЧ за модулем M, виконував би операцію складання за модулем m_i. Дана процедура здійснюється шляхом введення додаткових зв'язків виду $X_{\downarrow i \uparrow j}$ в позиційний суматор за модулем $M = 2^n - 1$, де вираз $X_{\downarrow i \uparrow j}$ позначає односторонню зв'язок між виходом j-го ДОС і входом i-го ДОС. Наведені приклади реалізації методу виконання операції модульного додавання для різних значень залишків a_i і b_i. Аналіз розглянутих прикладів показав практичну придатність запропонованого в статті методу. Він може бути використаний, як в ПСЧ, так і в СЗК.*

Ключові слова: *суматор двох чисел; суматор за довільним модулем; операція модульного додавання двох залишків; позиційна двійкова система числення (ПСЧ); непозиційних система числення в залишкових класах (СЗК).*

1 Вступ

Основою виконання арифметичної операції додавання двох чисел в непозиційній системі числення залишкових класів (СЗК) є операція $(a_i + b_i) \bmod m_i$ додавання відповідних залишків a_i та b_i по відповідним основам (модулям) m_i $(i = \overline{1,k})$ СЗК. Операція арифметичного додавання двох чисел в СЗК здійснюється незалежно від інших залишків і паралельно в часі по кожної i-ї основі СЗК [1-3]. Модульна операція складання $(a_i + b_i) \bmod m_i$ здійснюється на основі використання малоразрядних двійкових суматорів за модулем, на основі використання суматорів за модулем $M = 2^n - 1$. Даний підхід надає широкий вибір варіантів можливої реалізації внутрішньої структури такого суматору. Це дозволяє в повній мірі використовувати наявний теоретичний практичний досвід проектування двійкових суматорів [4-5]. Відомо, що одним з основних компонентів комп'ютерної системи (КС) в позиційній системі числення (ПСЧ) є суматор двох чисел. Зокрема, компонентами КС є також суматори двох чисел по модулю m_i [3-4]. Даний тип суматорів широко використовується, як в ПСЧ, так і в непозиційних системах числення [5]. Суматор чисел $A = (a_1 \| a_2 \| ... \| a_i \| ... \| a_k)$ та $B = (b_1 \| b_2 \| ... \| b_i \| ... \| b_k)$ в СЗК буде складатися з сукупності k $n = [\log_2 (m_i - 1) + 1]$ - розрядних суматорів за модулем m_i.

В цьому аспекті актуальною науково-прикладною задачею є задача побудови (*задача синтезу*) суматорів, які працюють за довільним модулем m_i, що виконані на логічних елементах з двома стійкими станами. Якщо залишки a_i та b_i, відповідно чисел A і B в СЗК, представлені в двійковій ПСЧ, тоді суматор двох залишків a_i та b_i по модулю m_i представляє собою послідовну сукупність з $n=[\log_2(m_i-1)+1]$ *двійкових однорозрядних суматорів* (ДОС), об'єднаних між собою зв'язками, подібно зв'язків позиційних двійкових суматорів.

Позиційні двійкові суматори мають фіксовану величину модуля $M=2^n-1$. Ця обставина не дає можливості їх безпосереднього застосування в якості модулів m_i СЗК. В ПСЧ найбільшого поширення набули два випадки. Для кожного випадку має місце наступні співвідношення модулів. *Перший випадок*. Має місце співвідношення модулів $M=m_i+1$. Для *другого випадку* має місце співвідношення модулів $M=m_i-1$. Для цих обох випадків реалізація операції модульного складання залишків здійснюється відносно просто. У той же час, в загальному випадку, операція модульного додавання двох залишків є досить трудомістким завданням, що обумовлює актуальність завдання синтезу суматорів за довільним модулем.

2 Метод побудови суматорів за модулем

Розглянемо метод побудови суматорів модульного додавання $(a_i+b_i)\bmod m_i$ двох залишків чисел за довільним модулем m_i. Даний метод побудови суматорів за модулем СЗК, заснований на використанні відомих структур суматорів за модулем $M=2^n-1$ в ПСЧ. Завдання побудови суматора модульного додавання $(a_i+b_i)\bmod m_i$ вирішується шляхом запровадження та організації додаткових зв'язків $X_{\downarrow i\uparrow j}$ меж j-м та i-м двійковими розрядами суматора за модулем *M*.

Метод побудови суматорів за довільним модулем m_i СЗК складається з двох етапів. Перший етап складається з рішення задачі побудови структури суматора модульного додавання $(a_i+b_i)\bmod m_i$. Другий етап. На основі отриманої структури суматора і чисельного значення модуля m_i, що представлений двійковим кодом, визначається схема модульного додавання двох залишків a_i та b_i чисел, обумовлену наявністю і використанням додаткових зв'язків $X_{\downarrow i\uparrow j}$ меж j-м та i-м ДОС. Детально розглянемо кожен з етапів методу побудови суматорів за довільним модулем m_i СЗК.

Перший етап: *- створення структури суматора модульного додавання* $(a_i+b_i)\bmod m_i$

Нехай є структура n-розрядного двійкового суматора в ПСЧ по модулю $M=2^n-1$ (рис. 1). Потрібно створити структуру суматора модульного складання $(a_i+b_i)\bmod m_i$, інакше, необхідно створити структуру суматора для реалізації операції додавання двох залишків чисел за довільним модулем m_i СЗК.

Технічно завдання побудови структури суматора за модулем формулюється в такий спосіб. Необхідно забезпечити умови, при яких вихідний суматор в ПСЧ по модулю *M* виконував би операцію складання за модулем m_i. Дана процедура здійснюється шляхом введення додаткових зв'язків виду $X_{\downarrow i\uparrow j}$ в позиційному суматорі за модулем $M=2^n-1$, де вираз $X_{\downarrow i\uparrow j}$ позначає односторонній зв'язок між виходом j-го ДОС та входом i-го ДОС.

Для побудови непозиційних суматора за довільним модулем, в структурі позиційного суматора за модулем *M* необхідно між певною парою ДОС вихідного суматора за модулем *M* сформувати додаткові зв'язку виду $X_{\downarrow i\uparrow j}$.

Додаткові зв'язки $X_{\downarrow i\uparrow j}$ формуються таким чином, щоб створений суматор здійснював операцію $(a_i+b_i)\bmod m_i$.

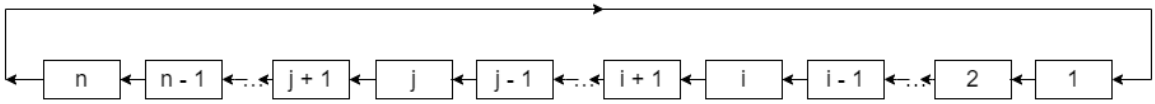

Рис. 1 – Схема розташування та нумерації ДОС

Схема організації в суматорі додаткового зв'язку $X_{\downarrow i \uparrow j}$ між виходом j-го ДОС та входом i-го ДОС відображено на рис. 2. Вочевидь, що завжди виконується умова $j > i$.

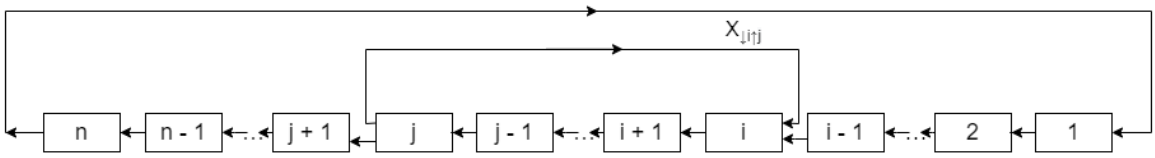

Рис. 2 – Схема двійкового суматора з одним додатковим зв'язком виду $X_{\downarrow i \uparrow j}$

<u>Другий етап</u>: *- визначення схеми додавання двох залишків a_i та b_i чисел*

В роботі [5] проведено дослідження впливу одного додаткового зв'язку $X_{\downarrow i \uparrow j}$, який встановлено між виходом j-го ДОС та входом i-го ДОС в структурі позиційного суматора по модулю $M = 2^n - 1$, на величину G_L вихідного вмісту суматора. Крім цього, показано, що числове значення $L = \{l_i\} = \{l_1, l_2, ..., l_m, ..., l_n\}$ $(i = \overline{1, n})$, що є вмістом G_L суматора, при введенні одного додаткового зв'язку $X_{\downarrow i \uparrow j}$ зменшується на величину $\Delta G_L = 2^{i-j-2} \cdot \sum_{m=j+1}^{n} 2^m \cdot l_m$. Введення і використання такого додаткового зв'язку $X_{\downarrow i \uparrow j}$ переводить обчислення чисел з двійкової системи числення (СЧ), в якій працює акумулятор по модулю M, в поліадичну СЧ з основами $\tau_1, \tau_2, ..., \tau_k$ с модулем $M = \tau_1 \cdot \tau_2 \cdot ... \cdot \tau_k - 1$. У цьому випадку число, наприклад $L = \{l_i\}$, $(i = \overline{1, k})$ представиться у вигляді (1):

$$G_L = \sum_{m=1}^{k} l_m \cdot \prod_{i=1}^{m-1} \tau_i = l_1 \cdot \tau_2 \cdot \tau_3 \cdot ... \cdot \tau_k + l_2 \cdot \tau_3 \cdot \tau_4 \cdot ... \cdot \tau_k + ... + l_{k-2} \cdot \tau_{k-1} \cdot \tau_k + l_{k-1} \cdot \tau_k + l_k . \quad (1)$$

Очевидно, що за відсутності в суматорі додаткових зв'язків $X_{\downarrow i \uparrow j}$ величина G_L вмісту суматора буде дорівнювати

$$G_L = \sum_{m=1}^{n} l_m \cdot q_m , \quad (2)$$

де величина l_m в m–му розряді вмісту суматора може приймати два значення $l_m = 0$ або $l_m = 1$, а значення q_m – є вага m–го розряду вмісту суматора, який визначається місцем розташування двійкового розряду суматора, що представлений на рис. 1. Якщо є додатковий зв'язок $X_{\downarrow i \uparrow j}$, що поєднує в структурі КС ДОС з номерами від i до j в єдиний (*узагальнений*) розряд суматора за модулем

$$\tau_{ij} = 2^{j-(i-1)} - 1 = 2^{j-i+1} - 1, \quad (3)$$

то вага q_m кожного розряду суматора з номерами від $(i-1)$-го до першого (молодшого розряду суматора) буде дорівнювати значенню $q_m = 2^{m-1}$ $(m = \overline{1, i-1})$ (див. рис. 3).

Виходячи зі структури суматора по модулю (рис. 4) вага розрядів суматора з номерами від $(j+1)$-го до старшого розряду суматора, буде визначатися виразом

$$q_m = 2^{i-1} \cdot \tau_{ij} \cdot 2^{m-j-1} . \quad (4)$$

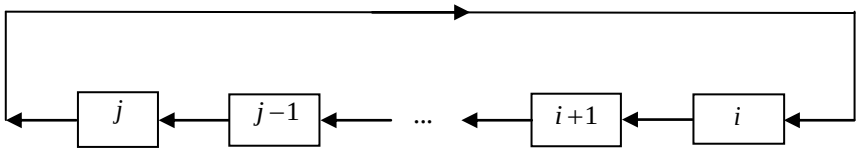

Рис. 3 – Схема узагальненого $(j-i+1)$-го розряду суматора за модулем τ_{ij}

З огляду на співвідношення (3), вираз (4) можна представити в наступному вигляді:

$$q_m = 2^{m+i-j-2} \cdot \tau_{ij} = 2^{m+i-j-2} \cdot (2^{j-i+1} - 1) = 2^{m-1} - 2^{m+i-j-2}. \quad (5)$$

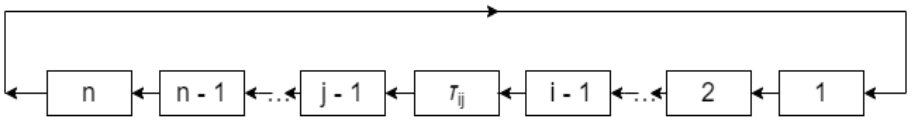

Рис. 4 – Еквівалентна схема суматора по модулю з додатковим зв'язком $X_{\downarrow i \uparrow j}$

В роботі [5] показано, що при введенні додаткової зв'язку виду $X_{\downarrow i \uparrow j}$, значення величини модулю $M = 2^n - 1$ позиційного суматора зменшується на величину

$$\Delta M = 2^{i-j-2} \cdot \sum_{m=j+1}^{n} S_m \cdot 2^m, \quad (6)$$

де S_m – значення m-го розряду числа, що міститься в суматорі. При цьому, природно, діапазон чисел, які представлені по модулю M, зменшується на величину ΔM. Дана обставина дає можливість, за рахунок введення в суматор за модулем M, додаткових зв'язків (або одного додаткового зв'язку), зменшити величину позиційного M модулю до необхідного значення модуля m_i СЗК.

Схема складання двох залишків визначається наступними правилами організації додаткових зв'язків $X_{\downarrow i \uparrow j}$.

1. Додатковий зв'язок суматора за модулем починається з виходу *n*-го (*старшого*) ДОС ($j = n$).

2. Додатковий зв'язок надходить на вхід ДОС, для якого $S_i = 0$.

3. В *n*-розрядному двійковому позиційному суматорі, що працює за модулем $M = 2^n - 1$, додатковий зв'язок $X_{\downarrow i \uparrow j}$ може мати місце лише в i-х двійкових розрядах S_i ($i = \overline{2, n}$), які відповідають нульовим значенням двійкової кодової комбінації модулю m_i.

4. У двійкових розрядах S_i позиційного суматора, котрі відповідають одиничним значенням, додаткові зв'язки $X_{\downarrow i \uparrow j}$ повинні бути відсутніми.

5. Визначаються двійкові розряди S_i позиційного суматора, для яких виконується умова $S_i = 0$. Процес визначення умови $S_i = 0$ проводиться виходячи з представлення модуля числа m_i в двійковому коді.

Розглянемо приклад побудови суматора, наприклад, по модулю $m_i = 11$ СЗК.

Приклад 1.

1. Згідно з величиною $m_i = 11$ модуля СЗК, визначимо кількість *n* ДОС. Для модулю $m_i = 11$ маємо, що $n = [\log_2(11-1)] + 1 = 4$. При цьому, вихідна (*без додаткових зв'язків*) структура позиційного суматора за модулем $M = 2^n - 1 = 15$ має вигляд, який представлений на рис. 5.

2. Для синтезу суматора по модулю $m_i = 11$ СЗК, попередньо визначимо значення двійкових розрядів S_i суматора, в запису значення модуля $m_i = 11$ котрих, містяться нулі (*тобто, коли* $S_i = 0$). Таким розрядом є третій розряд ($S_3 = 0$),так як в двійковому коді модуль $m_i = 11$ має вигляд: - 1011.

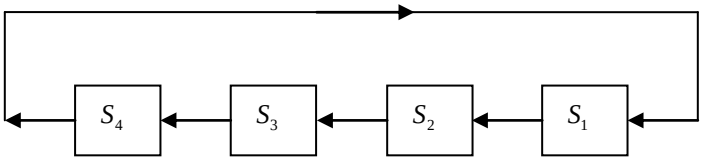

Рис. 5 – Вихідна структура суматора за модулем $M = 2^n - 1$

3. Так як $S_3 = 0$, то додатковий зв'язок в суматорі має вигляд $X_{\downarrow 3 \uparrow 4}$. Загальна кількість зв'язків дорівнює двом $X_{\downarrow 1 \uparrow 4}$ та $X_{\downarrow 3 \uparrow 4}$. Структура суматора за модулем $m_i = 11$ представлена на рис. 6.

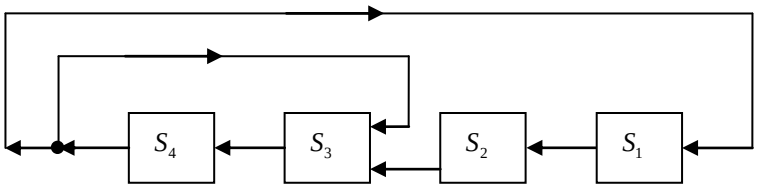

Рис. 6 – Структура суматора за модулем $m_i = 11$

Для перевірки ідентичності отриманої структури суматора за модулем $m_i = 11$ (рис. 6), попередньо, розглянемо частину (див. рис. 7) структури суматора виду

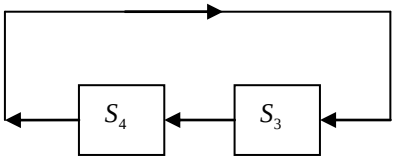

Рис. 7 – Частина структури суматора за модулем 11

Для цієї частини (рис. 7) структури суматора значення модуля M_1 визначиться як $M_1 = \tau_4 \cdot \tau_3 - 1$. Значення модуля СЗК суматора (рис. 6) визначається наступним чином (див. рис. 8): $m_i = M_1 \cdot \tau_2 \cdot \tau_1 - 1 = (\tau_4 \cdot \tau_3 - 1) \cdot \tau_2 \cdot \tau_1 - 1 = = (2 \cdot 2 - 1) \cdot 2 \cdot 2 - 1 = 11$.

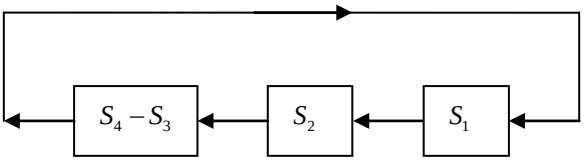

Рис. 8 – Фрагмент структури суматора для визначення значення модуля СЗК

Таким чином, синтез суматора за модулем $m_i = 11$ проведений вірно.

3 Приклади виконання операції додавання, залишків чисел за модулем

Існуючий [5] метод додавання $(a_i + b_i) \bmod m_i$ залишків a_i та b_i чисел за модулем m_i, базується на використанні двійкових суматорів, складається з сукупності таких дій, операцій і процедур:

1. Синтез суматора по заданому модулю m_i СЗК;
2. Визначається результат $S_n S_{n-1} \ldots S_2 S_1$ порозрядного додавання по модулю два залишків a_i та b_i чисел за модулем m_i, що представлені двійковим кодом;
3. Вміст двійкових розрядів, отриманої модульної суми $S_n S_{n-1} \ldots S_2 S_1$, заноситься до відповідних ДОС структури суматора по модулю m_i СЗК;
4. На підставі синтезованої структури суматора за модулем СЗК, реалізується алгоритм додавання двох залишків a_i та b_i чисел.

Однак в деяких випадках існуючий метод має обмежене застосування при додаванні двох залишків чисел за модулем m_i СЗК. Зокрема, в разі рівності двох залишків, тобто коли $a_i = b_i$, результат додавання $(a_i + b_i) \bmod m_i$ не у всіх випадках буде правильним. Це обумовлено тим, що отримана модульна сума $S_n S_{n-1} ... S_2 S_1$, яка використовується при визначенні результату модульного додавання $(a_i + b_i) \bmod m_i$ залишків a_i та b_i чисел, не враховує співвідношення між величинами значень модулів m_i, M і значенням $a_i + b_i$ позиційного додавання. В даному випадку для отримання правильного результату операції $(a_i + b_i) \bmod m_i$ необхідно враховувати величини значень m_i, M та $a_i + b_i$.

Очевидно, що при розробці методу додавання $(a_i + b_i) \bmod m_i$ залишків a_i та b_i необхідно враховувати варіанти співвідношення між величинами значень модулів m_i, M і значенням $a_i + b_i$ результату позиційного додавання залишків чисел. У таблиці 1 представлені можливі співвідношення між величинами модулів m_i, M та значенням $a_i + b_i$ позиційного додавання залишків чисел.

Таблиця 1 - Співвідношення значень величин

№ з.п.	***Співвідношення значень*** m_i, $a_i + b_i$ ***та*** $M = 2^n - 1 (n = 4, m_i = 11, M = 15)$		***Режим виконання операції додавання***
1	$a_i + b_i < m_i$	$a_i + b_i < 11$	Перший режим
2	$a_i + b_i = m_i$	$a_i + b_i = 11$	
3	$m_i < a_i + b_i < 2^n - 1$	$11 < a_i + b_i < 15$	Другий режим
4	$a_i + b_i = 2^n - 1$	$a_i + b_i = 15$	
5	$2^n - 1 < a_i + b_i$	$15 < a_i + b_i$	

Розглянемо запропонований метод на *прикладах* виконання операції $(a_i + b_i) \bmod m_i$ додавання залишків a_i та b_i чисел за модулем m_i. Узагальнюючи все вищевикладене для заданого значення модуля m_i, метод реалізації операції додавання $(a_i + b_i) \bmod m_i$ двох залишків a_i та b_i чисел буде складатися з сукупності таких дій, операцій і процедур:

1. Спочатку, для заданого значення модулю m_i, здійснюється побудова суматора за модулем m_i СЗК;

2. Формується результат позиційного підсумовування $a_i + b_i$ двох залишків a_i та b_i;

3. Проводиться порівняння значень $a_i + b_i$ та m_i;

4. Якщо $a_i + b_i \le m_i$, тоді значення $a_i + b_i$ – результат операції $(a_i + b_i) \bmod m_i$;

5. Якщо $a_i + b_i > m_i$, то для всіх можливих режимів виконання операції додавання (*див. табл. 1*), отриманий результат $a_i + b_i$ позиційного підсумовування двох залишків a_i та b_i, порозрядно заноситься до відповідних *n* ДОС, послідовна сукупність яких, становить структуру суматора по модулю m_i СЗК;

6. На підставі синтезованої, для заданого значення модуля m_i СЗК, структури суматора двох залишків a_i і b_i чисел (*див. п. 1*), реалізується алгоритм додавання двох залишків a_i та b_i чисел за модулем.

Розглянемо конкретні приклади виконання операції додавання $(a_i + b_i) \bmod m_i$ для двох довільних залишків a_i та b_i чисел розглянутим вище методом.

Приклади виконання операції додавання розглянемо в двох режимах (*див. табл. 1*).

Перший режим виконання операції додавання: - виконується умова $(a + b) \le m_i$ (*див. табл. 1*).

Приклад 2. Нехай залишки дорівнюють $a_i = 5$ та $b_i = 4$. Суматор реалізує операцію позиційного додавання залишків $a_i = 0101$ та $b_i = 0100$ у вигляді:

$$\begin{array}{r} a_i = 0101 \\ + \\ b_i = 0100 \\ \hline a_i + b_i = 1001 \end{array}.$$

Значення суми $a_i + b_i = 1001$ визначає результат операції.

Перевірка: $(0101 + 0100) = 1001 (\mathrm{mod} 11)$.

2-й режим виконання операції додавання. Виконується умова $(a+b) > m_i$ (*табл. 1*).

Приклад 3. Нехай $a_i = 5$ і $b_i = 6$. Суматор реалізує операцію позиційного додавання залишків $a_i = 0101$ та $b_i = 0110$ у вигляді:

$$\begin{array}{r} a_i = 0101 \\ + \\ b_i = 0110 \\ \hline a_i + b_i = 1011 \end{array}.$$

Значення позиційної суми $a_i + b_i = 1011$ залишків $a_i = 0101$ та $b_i = 0110$ порозрядно надходить на відповідні входи ДОС $5_4 - 5_1$. Таким чином, ДОС $5_4 - 5_1$ суматора містить значення 1011. Операція модульного додавання реалізується за схемою модульного додавання за модулем $m_i = 11$ (див. рис. 6). Алгоритм реалізації модульної операції представлений в таблиці 2 та на рис. 9. Одиниця двійкового розряду надходить на вхід ДОС 5_3 і 5_1.

Таблиця 2 - Алгоритм виконання результату операції

ДОС $5_4 - 5_1$	Вміст ДОС $5_4 - 5_1$	Наявність одиниці на входах ДОС $5_4 - 5_1$	Результат операції модульного додавання
5_1	1	+1	0
5_2	1	–	0
5_3	0	+1	0
5_4	1	–	0

На рис. 9 представлена схема додавання залишків $a_i = 0101$ та $b_i = 0110$ за модулем $m_i = 11$.

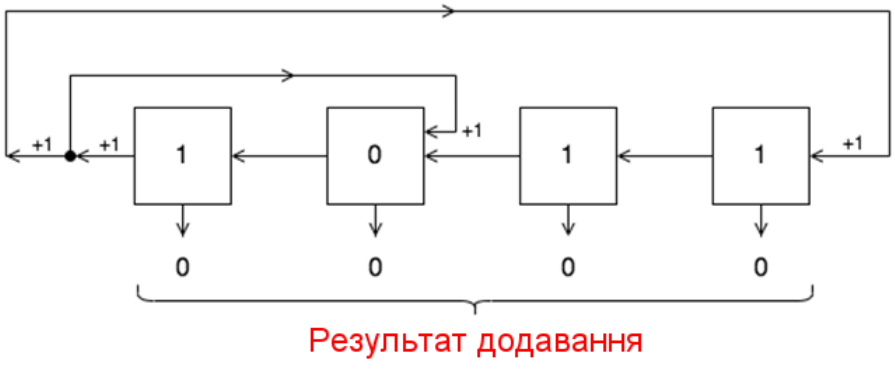

Рис. 9 – Схема додавання залишків $a_i = 0101$ та $b_i = 0110$ за модулем $m_i = 11$

Перевірка: $(0101 + 0110) = 0000 (\mathrm{mod} 11)$.

Приклад 4. Нехай $a_i = 5$ і $b_i = 7$. Суматор реалізує операцію позиційного додавання залишків $a_i = 0101$ та $b_i = 0111$ у вигляді:

$$\begin{array}{r} a_i = 0101 \\ + \\ b_i = 0111 \\ \hline a_i + b_i = 1100 \end{array}.$$

Значення позиційної суми $a_i + b_i = 1100$ залишків $a_i = 0101$ і $b_i = 0111$ порозрядно надходить на відповідні входи ДОС $5_4 - 5_1$. Таким чином, ДОС $5_4 - 5_1$ суматора містить значення 1100. Операція модульного додавання реалізується за схемою модульного додавання за модулем $m_i = 11$ (*див. рис. 6*).

Алгоритм реалізації модульної операції представлений в таблиці 3 і на рис. 10. Одиниця двійкового розряду надходить на вхід ДОС 5_3 і 5_1.

Таблиця 3 - Алгоритм виконання результату операції

ДОС $5_4 - 5_1$	Вміст ДОС $5_4 - 5_1$	Наявність одиниці на входах ДОС $5_4 - 5_1$	Результат операції модульного додавання
5_1	0	+1	1
5_2	0	–	0
5_3	1	+1	0
5_4	1	–	0

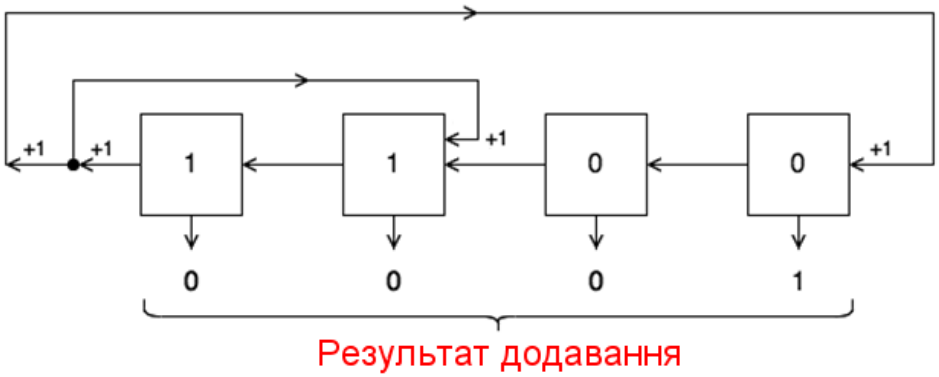

Рис. 10 – Схема додавання залишків $a_i = 0101$ і $b_i = 0111$ за модулем $m_i = 11$

Перевірка: $(0101 + 0111) = 0001 (\text{mod} 11)$.

Приклад 5. Нехай $a_i = 5$ і $b_i = 9$. Суматор реалізує операцію позиційного додавання залишків $a_i = 0101$ и $b_i = 1001$ у вигляді:

$$\begin{array}{r} a_i = 0101 \\ + \quad b_i = 1001 \\ \hline a_i + b_i = 1110 \end{array}.$$

Значення позиційної суми $a_i + b_i = 1110$ залишків $a_i = 0101$ и $b_i = 1001$ порозрядно надходить до відповідних входів ДОС $5_4 - 5_1$. Таким чином, ДОС $5_4 - 5_1$ суматора, містить значення 1110. Операція модульного додавання реалізується за схемою модульного додавання за модулем $m_i = 11$ (рис. 6).

Алгоритм реалізації модульної операції представлений в таблиці 4 і схемі на рис. 11. Одиниця двійкового розряду надходить на вхід ДОС 5_3 та 5_1.

Перевірка: $(0101 + 1001) = 0011 (\text{mod} 11)$.

Таблиця 4 - Алгоритм виконання результату операції

ДОС $5_4 - 5_1$	Вміст ДОС $5_4 - 5_1$	Наявність одиниці на входах ДОС $5_4 - 5_1$	Результат операції модульного додавання
5_1	0	+1	1
5_2	1	–	1
5_3	1	+1	0
5_4	1	–	0

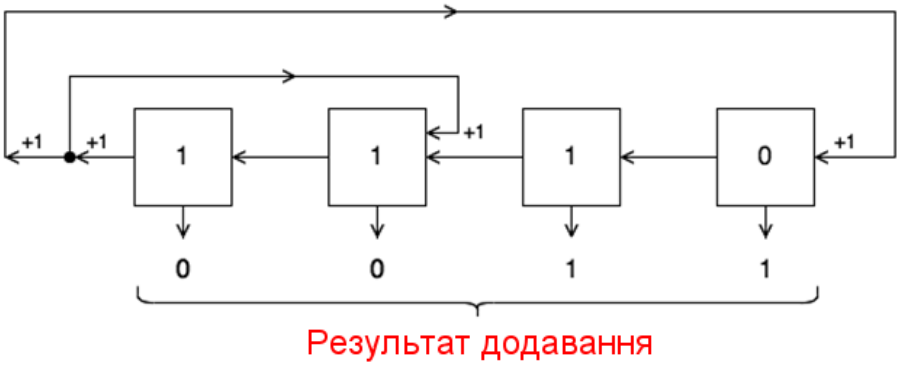

Рис. 11 – Схема додавання залишків $a_i = 0101$ і $b_i = 1001$ за модулем $m_i = 11$

Приклад 6. Нехай $a_i = 6$ і $b_i = 10$. Суматор реалізує операцію позиційного додавання залишків $a_i = 0110$ та $b_i = 1010$ у вигляді:

$$\begin{array}{r} a_i = 0110 \\ + \\ b_i = 1010 \\ \hline a_i + b_i = 10000 \end{array}.$$

Значення чотирьох 0000 молодших двійкових розрядів позиційної суми $a_i + b_i = 10000$ залишків $a_i = 0110$ і $b_i = 1010$, порозрядно надходить до відповідних входів ДОС $5_4 - 5_1$. Таким чином, ДОС $5_4 - 5_1$ суматора, містить значення 0000. Операція модульного додавання реалізується за схемою модульного додавання (рис. 6) за модулем $m_i = 11$.

Алгоритм реалізації модульної операції представлений в таблиці 5, а схема додавання на рис. 12. Одиниця двійкового розряду надходить на вхід ДОС 5_3 та 5_1.

Таблиця 5 - Алгоритм виконання результату операції

ДОС $5_4 - 5_1$	Вміст ДОС $5_4 - 5_1$	Наявність одиниці на входах ДОС $5_4 - 5_1$	Результат операції модульного додавання
5_1	0	+1	1
5_2	0	–	0
5_3	0	+1	1
5_4	0	–	0

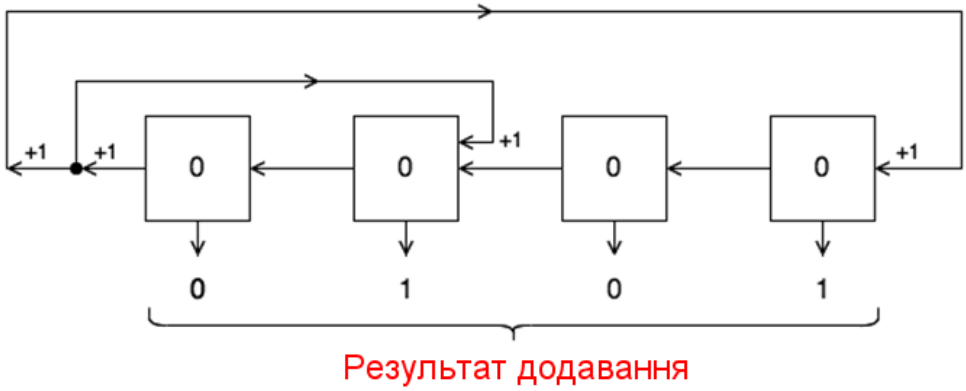

Рис. 12 – Схема додавання залишків

Перевірка: $(0110 + 1010) = 0101 (\mathrm{mod} 11)$.

Приклад 7. Пусть $a_i = b_i = 10$.

Суматор реалізує операцію позиційного додавання залишків $a_i = 1010$ та $b_i = 1010$ у вигляді:

$$\begin{array}{r} a_i = 1010 \\ + \quad b_i = 1010 \\ \hline a_i + b_i = 10100 \end{array}.$$

Значення 4-х 0100 молодших двійкових розрядів позиційної суми $a_i + b_i = 10100$ залишків $a_i = 1010$ і $b_i = 1010$ порозрядно надходить до відповідних входів ДОС $5_4 - 5_1$. Таким чином, ДОС $5_4 - 5_1$ суматора, містить значення Операція модульного додавання реалізується за схемою модульного додавання за модулем $m_i = 11$ (рис. 6).

Алгоритм реалізації модульної операції представлений в таблиці 6, а схема на рис. 13. Одиниця двійкового розряду надходить на вхід ДОС 5_3 та 5_1.

Таблиця 6 - Алгоритм виконання результату операції (*для* $a_i = b_i = 10$)

ДОС $5_4 - 5_1$	Вміст ДОС $5_4 - 5_1$	Наявність одиниці на входах ДОС $5_4 - 5_1$	Результат операції модульного додавання
5_1	0	+1	1
5_2	0	–	0
5_3	1	+1	0
5_4	0	–	1

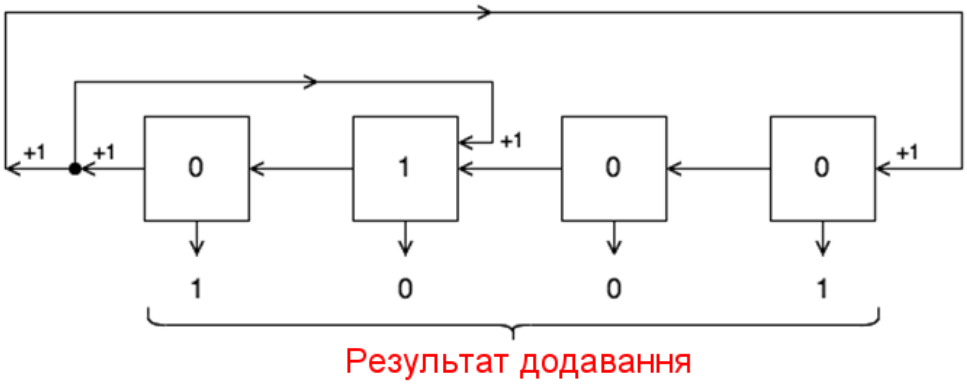

Рис. 13 – Схема додавання залишків $a_i = 1010$ та $b_i = 1010$ за модулем $m_i = 11$

Перевірка: $(1010 + 1010) = 1001 (\mathrm{mod} 11)$.

4 Висновки

У даній роботі представлений метод додавання залишків a_i та b_i двох чисел за довільним модулем m_i в СЗК. Для реалізації даного методу додавання за модулем, була модифікована структура модульного суматора за довільним модулем СЗК. В основу цих змін була покладена структура позиційного суматора за модулем $M = 2^n - 1$, яка складається із сукупності послідовних двійкових однорозрядних суматорів з 1-м зворотним зв'язком.

Для побудови зазначеного типу суматора, необхідно використовувати додаткові зв'язки $X_{\downarrow i \uparrow j}$ між j-м та i-м двійковими розрядами суматору за модулем *M*.

Розроблений метод виконання операції додавання $(a_i + b_i) \bmod m_i$ двох залишків a_i і b_i чисел за модулем m_i, ґрунтується на структурі двійкового суматору за довільним модулем m_i СЗК та схемою додавання залишків a_i та b_i двох чисел.

Розглянуті приклади реалізації методу модульного складання для залишків a_i і b_i для різних значень модуля m_i СЗК, підтверджують практичну реалізованість запропонованого методу.

Посилання

[1] Bayoumi M.A., Jullien G.A., Miller W.C. A VLSI Implementation of Residue. Adders IEEE Trans. on Circuits and Systems. 1987. V. 34, № 3. pp. 284-288.

[2] P.V. Ananda Mohan. Residue Number Systems: Theory and Applications. Birkhäuser Basel: Springer International Publishing Switzerland, 2016. 351 P.

[3] Krasnobayev V. A. and Koshman S. A. Method for implementing the arithmetic operation of addition in residue number system based on the use of the principle of circular shift // Cybernetics and Systems Analysis. – July, 2019. – Vol. 55, Is. 4, pp. 692-698.

[4] Krasnobayev V. A., Yanko A. S., Koshman S. A. A Method for arithmetic comparison of data represented in a residue number of system // Cybernetics and Systems Analysis. – January 2016. – Vol. 52, Is. 1, pp. 145-150.

[5] V. A. Krasnobayev, A. A. Kuznetsov, S. A. Koshman, and K. O. Kuznetsova "A method for implementing the operation of modulo addition of the residues of two numbers in the residue number system", Cybernetics and Systems Analysis, Vol. 56, No. 6, November, 2020, 1029-1038. https://doi.org/10.1007/s10559-020-00323-9.

[6] Azadeh Safari, James Nugent, Yinan Kong. Novel implementation of full adder based scaling in Residue Number Systems. IEEE 56th International Midwest Symposium on Circuits and Systems (MWSCAS). 4-7 Aug. 2013. pp. 657–660.

[7] Shugang Wei. Fast signed-digit arithmetic circuits for residue number systems. IEEE International Conference on Electronics, Circuits, and Systems (ICECS). 6-9 Dec. 2015. pp. 344 – 347.

Reviewer: Vyacheslav Kalashnikov, Doctor of Sciences (Physics and Mathematics), Full Prof., Department of Systems and Industrial Engineering, Campus Monterrey, Monterrey, Mexico.
E-mail: kalash@itesm.mx

Received on November 2020.

Authors:
Victor Krasnobaev, Doctor of Sciences (Engineering), Full Prof., Academician of the Academy of Applied Radioelectronics Sciences, Kharkiv National University named after V.N. Karazin, Kharkiv, Ukraine.
E-mail: v.a.krasnobaev@gmail.com

Kateryna Kuznetsova, student of the Department of Security of Information Systems and Technologies, Kharkiv National University named after V.N. Karazin, Kharkiv, Ukraine.
E-mail: kate7smith12@gmail.com

Mykhaylo Bagmut, graduate student of the Department of Security of Information Systems and Technologies, Kharkiv National University named after V.N. Karazin, Kharkiv, Ukraine.
E-mail: Mikhail56@ukr.net

Method for performing the operation of adding the remainder of numbers modulo.

Abstract. One of the components of a computer system (CS) in a positional binary number system (PNS) is an adder of two numbers. In particular, adders modulo m_i of two numbers are also components of the CS. This type of modulo adders is widely used both in the PNS and in the non-positional number system in the residual classes (RNS). An important and urgent scientific and applied problem is the problem of constructing the adders, which operate by modulus m_i, that is an arbitrary RNS modulo. If the remainders a_i and b_i of both numbers A and B in RNS are represented in a binary PNS, then the adder of two residuals a_i and b_i by modulus m_i is a sequential set of n binary one-bit adders (BOBA). The purpose of the article is to develop a method for performing the operation of modular addition $(a_i + b_i) \bmod m_i$ of two remainders of numbers by an arbitrary modulo m_i based on the use of a positional binary adder modulo $M = 2^n - 1$. The proposed method is based on the use of the well-known structure of positional binary adders modulo $M = 2^n - 1$. Technically, the problem of creating the structure of the modular adder is formulated as follows. It is necessary to provide conditions under which the initial adder in PNS modulo M performs the addition operation modulo m_i. This procedure is carried out by introducing additional connections as $X_{\downarrow i \uparrow j}$ in the positional adder modulo $M = 2^n - 1$, where the expression $X_{\downarrow i \uparrow j}$ denotes one-way connection between the output of the j-th BOBA and the input of the i-th BOBA.

Keywords*:* adder of two numbers; adder for any module; operation of modular addition of two residues; positional binary number system (PNS); non-positional number system in residual classes (RNS).

Рецензент: Вячеслав Калашников, д.ф.-м.н., проф., Технологический университет Монтеррея, Монтеррей, Мексика.
E-mail: kalash@itesm.mx

Поступила: Ноябрь 2020.

Авторы:
Виктор Краснобаев, д.т.н., проф., академик Академии наук прикладной радиоэлектроники, Харьковский национальный университет имени В. Н. Каразина, Харьков, Украина.
E-mail: v.a.krasnobaev@gmail.com

Екатерина Кузнецова, студентка факультета компьютерных наук, Харьковский национальный университет имени В. Н. Каразина, Харьков, Украина.
E-mail: kate7smith12@gmail.com

Михаил Багмут, аспирант каф. Безопасности информационных систем и технологий, Харьковский национальный университет имени В. Н. Каразина, Харьков, Украина.
E-mail: Mikhail56@ukr.net

Метод выполнения операции сложения остатков чисел по модулю.

Аннотация. Сумматор двух чисел является одним из компонентов компьютерных систем (КС) в позиционной двоичной системе счисления (ПСС). В частности, компонентами КС являются, также, сумматоры по модулю m_i двух чисел. Данный тип сумматоров по модулю широко используются как в ПСС, так и в непозиционной системе счисления в остаточных классах (СОК). Важной и актуальной научно-прикладной задачей является задача построения сумматоров, работающих по произвольному модулю m_i СОК. Если остатки a_i и b_i чисел A и B в СОК, представлены в двоичной ПСС, тогда сумматор двух остатков a_i и b_i по модулю m_i есть последовательная совокупность из n двоичных одноразрядных сумматоров (ДОС). Целью статьи является, разработка метода выполнения операции модульного сложения $(a_i + b_i) \bmod m_i$ двух остатков чисел, по произвольному модулю, на основе использования позиционного двоичного сумматора по модулю $M = 2^n - 1$. Предложенный в работе метод выполнения операции модульного сложения, основан на использовании известной структуры позиционных двоичных сумматоров по модулю $M = 2^n - 1$. Технически, задача построения структуры сумматора, состоит в необходимости обеспечить условия при которых, исходный сумматор в ПСС по модулю М, выполнял бы операцию сложения по модулю m_i. Данная процедура осуществляется путем введения дополнительных связей вида $X_{\downarrow i \uparrow j}$ в позиционном сумматоре по модулю $M = 2^n - 1$, где выражение $X_{\downarrow i \uparrow j}$ обозначает одностороннюю связь между выходом j-го ДОС и входом i-го ДОС. Приведены примеры реализации метода выполнения операции модульного сложения для различных значений остатков a_i и b_i. Анализ рассмотренных примеров показал практическую реализуемость предложенного метода. Он может быть использован, как в ПСС, так и в СОК.

Ключевые слова: сумматор двух чисел; сумматор по произвольному модулю; операция модульного сложения двух остатков; позиционная двоичная система счисления (ПСС); непозиционная система счисления в остаточных классах (СОК).