



УКРАЇНА

(19) **UA** (11) **112034** (13) **C2**
(51) МПК

G06F 7/52 (2006.01)

G06F 7/72 (2006.01)

ДЕРЖАВНА СЛУЖБА
ІНТЕЛЕКТУАЛЬНОЇ
ВЛАСНОСТІ
УКРАЇНИ

(12) ОПИС ДО ПАТЕНТУ НА ВІНАХІД

<p>(21) Номер заявки: а 2015 07299</p> <p>(22) Дата подання заявки: 20.07.2015</p> <p>(24) Дата, з якої є чинними права на винахід: 11.07.2016</p> <p>(41) Публікація відомостей про заяву: 12.10.2015, Бюл.№ 19</p> <p>(46) Публікація відомостей про видачу патенту: 11.07.2016, Бюл.№ 13</p>	<p>(72) Винахідник(и): Краснобаєв Віктор Анатолійович (UA), Янко Аліна Сергіївна (UA), Курчанов Валерій Микитович (UA), Кошман Сергій Олександрович (UA)</p> <p>(73) Власник(и): Краснобаєв Віктор Анатолійович, вул. Астрономічна, 35-б, кв. 24, м. Харків, 61085 (UA), Янко Аліна Сергіївна, вул. Великотирнівська, 36, корп. 3, к. 122, м. Полтава, 36014 (UA), Курчанов Валерій Микитович, вул. Зінківська, 36-А, кв. 20, м. Полтава, 36009 (UA), Кошман Сергій Олександрович, вул. Енгельса, 19, к. 409, м. Харків, 61052 (UA)</p> <p>(56) Перелік документів, взятих до уваги експертизою: UA 91321 U, 25.06.2014 UA 106343 C2, 11.08.2014 UA 75965 C2, 15.06.2006 UA 75201 C2, 15.03.2006 SU 1015382 A1, 30.04.1983 SU 1756887 A1, 23.08.1992 RU 2310223 C2, 10.11.2007 US 2008114820 A1, 15.05.2008 EP 0601907 A2, 15.06.1994 FR 2775368 A1, 27.08.1999</p>
--	---

(54) ПРИСТРІЙ ДЛЯ РЕАЛІЗАЦІЇ ОПЕРАЦІЇ МНОЖЕННЯ ТА ДІЛЕННЯ ЧИСЕЛ У СИСТЕМІ ЗАЛИШКОВИХ КЛАСІВ

(57) Реферат:

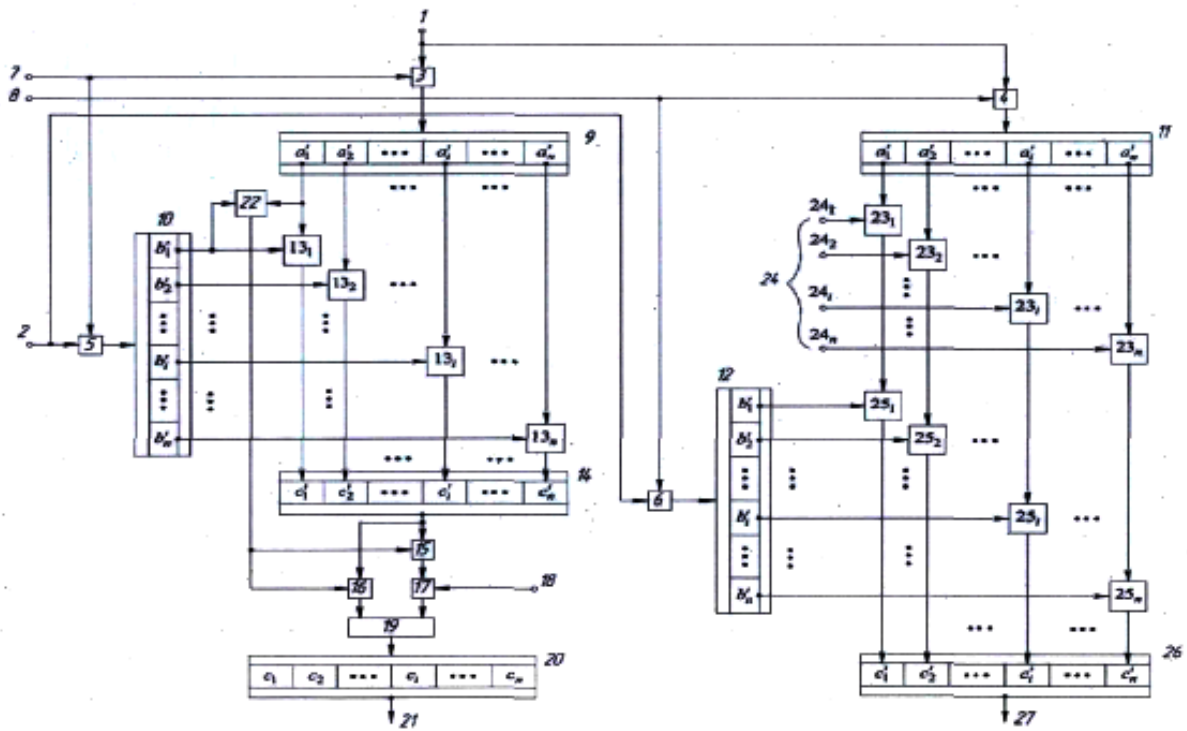
Пристрій для реалізації операції множення та ділення чисел у системі залишкових класів належить до обчислювальної техніки і призначено для множення та ділення двох чисел у непоозиційній системі числення залишкових класів (СЗК) як в додатному, так і у від'ємному числових діапазонах. У пристрій, що містить перший і другий вхідні та перший вихідний регістри, прийомний регістр, суматор за модулем два, групу елементів АБО, групу з n пристроїв для множення двох лишків a_i та b_i чисел $A'_{СЗК}$ та $B'_{СЗК}$ за модулями m_i ($i = \overline{1, n}$), де n -

кількість модулів СЗК, першу групу елементів I , групу вентилів, суматор за модулем $M = \prod_{i=1}^n m_i$,

додатково введені другий та третій вхідні регістри, другий вихідний регістр, другу, третю, четверту та п'яту групи елементів I , групу з n суматорів, групу з n пристроїв для ділення чисел. Технічним результатом є розширення функціональних можливостей пристрою за рахунок

UA 112034 C2

виконання, додатково до операції множення, операції ділення чисел у СЗК, у випадку, якщо ділене цілком ділиться на дільник.



Винахід (пристрій) належить до області обчислювальної техніки і призначено для множення та ділення двох чисел у непозиційній системі числення залишкових класів (СЗК) як в додатному, так і у від'ємному числових діапазонах.

Відомий пристрій (аналог) для множення по довільному модулю m_i СЗК (А.с. СРСР № 922731, кл. МПК G06F 7/39, Б. В. № 15, 1982 р.), що містить вхідні реєстри, дешифратори, групи елементів АБО, групи елементів І, суматор по модулю два, елементи І та АБО, комутатори та вихідний реєстр.

Недоліком відомого пристрою є низькі функціональні можливості, які полягають в тому, що даний пристрій не може реалізувати операцію ділення двох чисел у СЗК.

Відомий пристрій (аналог) для множення по довільному модулю w , СЗК є пристрій для множення по довільному модулю (Пат. № 60078, Україна, МПК (2011.01) G 06 F 7/00. Опубл. 10.06.2011, Бюл. № 11). Він містить вхідні реєстри, дешифратори, групи елементів АБО, групи елементів І, суматор по модулю два, елементи І та АБО, комутатори та вихідний реєстр.

Недоліком відомого пристрою є низькі функціональні можливості, які полягають в тому, що даний пристрій не може реалізувати операцію ділення двох чисел у СЗК.

Близьким (аналогом) за технічною суттю і результатом, що досягається, є табличний пристрій для множення двох чисел у СЗК (Пат. 70442 Україна, МПК G06F 7/52. Бюл. № 11 від 11.06.2012 р. (2006.01)). Табличний пристрій для множення двох чисел у класі лишків, який містить перший та другий входи пристрою, перший та другий вхідні реєстри, суматор за модулем два, групу елементів АБО, вихідний реєстр, вихід пристрою, при цьому перший та другий входи пристрою підключено до входів відповідно першого та другого вхідних реєстрів, а вихід вихідного реєстра є виходом пристрою.

Недоліком аналога є низькі функціональні можливості, які полягають в тому, що даний пристрій не може реалізувати операцію ділення двох чисел у СЗК.

Найбільш близьким аналогом (прототипом) за технічною суттю і результатом, що досягається, є пристрій для реалізації операції множення двох чисел у СЗК (Пат. 91321 Україна, МПК G06F 7/52. Бюл. № 12 від 25.06.2014 р. (2006.01)). Пристрій для реалізації операції модульного множення двох чисел у СЗК містить перший та другий вхідні прийомні реєстри, вихідний прийомний реєстр, реєстр результату операції, суматор за модулем два, першу групу елементів АБО, групу з n пристроїв для множення двох лишків a_i та b_i чисел $A'_{СЗК}$ та $B'_{СЗК}$ за модулями ($i = \overline{1, n}$; n - кількість модулів СЗК), першу групу елементів І, першу групу вентилів,

перший суматор за модулем $M = \prod_{i=1}^n m_i$, при цьому виходи i -х ($i = \overline{1, n}$) підреєстрів першого та

другого вхідних прийомних реєстрів підключено до входів i -го пристрою для множення лишків a_i та b_i , відповідно чисел $A'_{СЗК}$ та $B'_{СЗК}$, за модулем m_i СЗК, виходи групи пристроїв

множення лишків a_i та b_i за модулями m_i підключено до входів відповідних i -х підреєстрів вихідного прийомного реєстра, вихід якого підключено до перших входів елементів І першої групи та вентиляльних елементів першої групи, виходи елементів І першої групи підключено до

перших входів суматора за модулем $M = \prod_{i=1}^n m_i$, до других входів якого підключена шина подачі

значення $\frac{M}{2}$, виходи суматора за модулем $M = \prod_{i=1}^n m_i$ і вентиляльних елементів першої групи

через елементи АБО першої групи підключено до входу реєстра результату операції, виходи перших (за модулем m_1 СЗК) підреєстрів вхідних прийомних реєстрів підключено до входів суматора за модулем два, вихід якого підключено до других входів елементів І першої групи та до других (заборонених) входів вентиляльних елементів першої групи.

Недоліком прототипу є низькі функціональні можливості, які полягають в тому, що даний пристрій не може реалізувати операцію ділення двох чисел у СЗК.

В основу винаходу поставлено задачу - розширити функціональні можливості пристрою-прототипу за рахунок виконання, додатково до операції множення, операції ділення чисел у СЗК, у випадку, якщо ділене цілком ділиться на дільник.

Поставлена задача вирішується тим, що у пристрій-прототип, який містить перший і другий вхідні та перший вихідний реєстри, прийомний реєстр, суматор за модулем два, групу елементів АБО, групу з n пристроїв для множення двох лишків a_i та b_i чисел $A'_{СЗК}$ та $B'_{СЗК}$ за

модулями m_i ($i = \overline{1, n}$; n - кількість модулів СЗК), першу групу елементів I , групу вентилів, суматор за модулем $M = \prod_{i=1}^n m_i$, при цьому, виходи i -их ($i = \overline{1, n}$) підрегістрів першого та другого

вхідних реєстрів підключено до входів i -го пристрою групи для множення лишків a_i' та b_i' , відповідно чисел $A'_{СЗК}$ та $B'_{СЗК}$, за модулем m_i СЗК, виходи пристроїв множення групи лишків

5 a_i' та b_i' за модулями m_i підключено до входів відповідних i -их підрегістрів прийомного реєстра, вихід якого підключено до перших входів елементів I першої групи та вентиляльних елементів групи, виходи елементів I першої групи підключено до перших входів суматора за модулем

$M = \prod_{i=1}^n m_i$, до других входів якого підключена шина подачі значення $\frac{M}{2}$, виходи суматора за

модулем $M = \prod_{i=1}^n m_i$ і вентиляльних елементів групи через елементи АБО групи підключено до

10 входу вихідного реєстра, вихід якого є першим виходом пристрою, виходи перших (за модулем m_1 СЗК) підрегістрів вхідних реєстрів підключено до входів суматора за модулем два, вихід якого підключено до других (відкриваючих) входів елементів I першої групи та до других (заборонених) входів вентиляльних елементів групи, додатково введено другий та третій вхідні реєстри, другий вихідний реєстр, другу, третю, четверту та п'яту групи елементів I , групу з n

15 суматорів, групу з n пристроїв для ділення чисел, при цьому перший вхід пристрою підключено до перших входів елементів I другої та третьої груп, а другий вхід пристрою підключено до перших входів елементів I четвертої та п'ятої груп, до других входів елементів I другої та четвертої груп підключена шина подачі сигналу ознаки операції множення, а до других входів елементів I третьої та п'ятої груп підключена шина подачі сигналу ознаки операції ділення,

20 виходи елементів I другої, третьої, четвертої та п'ятої груп підключено до входів відповідно першого, другого, третього та четвертого вхідних реєстрів, виходи i -их ($i = \overline{1, n}$) підрегістрів

третього вхідного реєстра підключено до перших входів i -их суматорів, до других входів яких підключені шини подачі відповідних значень констант, виходи суматорів підключено до перших входів відповідних пристроїв для ділення, до других входів яких підключено відповідні виходи

25 підрегістрів четвертого вхідного реєстру, а виходи пристроїв для ділення підключені до входів відповідних підрегістрів другого вихідного реєстра, вихід якого є другим виходом пристрою.

Введення вказаних ознак дозволяє розширити функціональні можливості прототипу за рахунок, додатково до виконання операцій множення, реалізувати процес виконання і операції ділення двох чисел у СЗК у випадку, якщо ділене цілком ділиться на дільник.

30 Як і у прототипу, у винаході для реалізації процесу виконання операції множення та ділення у СЗК як у додатному, так і у від'ємному числових діапазонах, вхідні числа A і B представлені у штучній формі (ШФ)

$$\begin{cases} A'(B') = \frac{M}{2} + |A|(B), \text{ якщо } A(B) \geq 0 \\ A'(B') = \frac{M}{2} - |A|(B), \text{ якщо } A(B) < 0 \end{cases},$$

тобто, для додатних чисел маємо, що $A' = \frac{M}{2} + |A|$, а для від'ємних - $A' = \frac{M}{2} - |A|$, де

35 $M = \prod_{i=1}^n m_i$.

Алгоритм виконання операції множення у СЗК визначається наступним чином

$$(A \cdot B)' = f(A', B') = \begin{cases} A' \cdot B', \text{ якщо } A' \text{ і } B' \text{ однакової парності,} \\ A' \cdot B' + \frac{M}{2}, \text{ якщо } A' \text{ і } B' \text{ різної парності.} \end{cases} \quad (1)$$

Алгоритм виконання операції ділення у СЗК визначається наступним чином.

40 Якщо задано числа A' та B' у СЗК, тоді при тому, що ділене A' цілком ділиться на дільник B' , маємо

$$\frac{A'}{B'} = \left(\frac{a'_1 \parallel a'_2 \parallel \dots \parallel a'_n}{b'_1 \parallel b'_2 \parallel \dots \parallel b'_n} \right) = (c'_1 \parallel c'_2 \parallel \dots \parallel c'_n).$$

При цьому

$$c'_i = (c'_1 \parallel c'_2 \parallel \dots \parallel c'_n) = \left[\left(\frac{a'_1 + k_{1j_1} \cdot m_1}{b'_1} \right) \parallel \left(\frac{a'_2 + k_{2j_2} \cdot m_2}{b'_2} \right) \parallel \dots \parallel \left(\frac{a'_n + k_{nj_n} \cdot m_n}{b'_n} \right) \right].$$

Для довільного модуля m_i СЗК залишок c'_i визначається наступним співвідношенням

5

$$c'_i = \frac{a'_i + k_{ij_j} \cdot m_i}{b'_i}, \quad (2)$$

де: $k_{ij_j} = \overline{1, m_i - 1}$ - натуральне число, що може дорівнювати тільки одному з чисел $1, 2, \dots, m_i - 1$; $i = \overline{1, n}$; $j_j = \overline{1, m_i - 1}$ - чисельне значення індексу k_{ij_j} . Так, для $m_1 (i = 1)$ маємо, що

$$k_{1j_1} = \begin{cases} k_{11} = 1, \\ k_{12} = 2, \\ \vdots \\ k_{1(m_1-1)} = m_1 - 1. \end{cases}$$

10

І так далі. Для $m_n (i = n)$ маємо

$$k_{nj_n} = \begin{cases} k_{n1} = 1, \\ k_{n2} = 2, \\ \vdots \\ k_{n(m_n-1)} = m_n - 1. \end{cases}$$

Таким чином у винаході залишок c'_i визначається у відповідності до алгоритму (2).

Вираз (2) для $i = \overline{1, n}$ однозначно визначає частку $\frac{A'}{B'}$, якщо $b'_i \neq 0$. Ділення чисел за алгоритмом (2) розуміється у тому сенсі, що якщо значення a'_i цілком не ділиться на b'_i , тоді до a'_i послідовно додається значення m_i доти, поки сума $a'_i + k_{ij_j} \cdot m_i$ не буде цілком ділитися на дільник b'_i .

15

20

25

На фіг. 1 представлена блок-схема пристрою для реалізації операції множення та ділення двох чисел для довільної СЗК, де: 1, 2 - перший та другий входи пристрою; 3, 4, 5 та 6 - перша, друга, третя та четверта групи елементів I; 7 - шина подачі сигналу ознаки операції множення; 8 - шина подачі сигналу ознаки операції ділення; 9, 10, 11 та 12 - перший, другий, третій та четвертий вхідні регістри; 13₁-13_n група пристроїв множення лишків a'_i та b'_i за модулями $m_i, i = \overline{1, n}$; 14 - прийомний регістр; 15 - п'ята група елементів I; 16 - група вентильних елементів; 17 - суматор за модулем $M = \prod_{i=1}^n m_i$; 18 - шина подачі значення $\frac{M}{2}$; 19 - група елементів АБО; 20 - перший вихідний регістр; 21 - перший вихід пристрою; 22 - суматор за модулем два; 23₁-23_n - група суматорів, призначених для виконання операції $a'_i + k_{ij_j} \cdot m_i, i = \overline{1, n}$; 24 (24₁-24_n) - шини подачі відповідних значень констант $k_{ij_j} \cdot m_i, i = \overline{1, n}$; 25₁-25_n - група пристроїв для ділення $\frac{a'_i + k_{ij_j} \cdot m_i}{b'_i}$; 26 - другий вихідний регістр; 27 - другий вихід пристрою.

В таблиці 1 представлено алгоритм функціонування суматора 22 за модулем два.

Алгоритм функціонування суматора 22

Входи суматора 22		Виходи суматора 22 $(a'_1 + b'_1) \bmod 2$
a'_1	b'_1	
0	0	0
0	1	1
1	0	1
1	1	0

Перший 1 та другий 2 входи пристрою підключено до перших входів елементів I відповідно першої 3 та другої 4 груп і до перших входів елементів I відповідно третьої 5 та другої 6 груп. До других входів елементів I першої 3 та третьої 5 груп підключена шина 7 подачі сигналу ознаки операції множення, а до других входів елементів I другої 4 та четвертої 6 груп підключена шина 8 подачі сигналу ознаки операції ділення. Виходи елементів I першої 3 і третьої 5 груп підключені до входам відповідно першого 9 та другого 10 вхідних регістрів, а виходи елементів I другої 4 і четвертої 6 груп підключені до входам відповідно третього 11 та четвертого 12 вхідних регістрів. Виходи i-их ($i = \overline{1, n}$) підрегистрів першого 9 та другого 10 вхідних регістрів підключено до входів i-го пристрою групи 13₁-13_n для множення лишків a'_1 та b'_1 , відповідно чисел $A'_{СЗК}$ та $B'_{СЗК}$, за модулем m_i СЗК. Виходи пристроїв множення групи 13₁-13_n лишків a'_i та b'_i за модулями m_i підключено до входів відповідних i-их підрегистрів прийомного 14 регістра, вихід якого підключено до перших входів елементів I п'ятої 15 групи та вентильних елементів 16 групи, виходи елементів I п'ятої 15 групи підключено до перших входів суматора 17 за модулем $M = \prod_{i=1}^n m_i$, до других входів якого підключена шина 18 подачі значення $\frac{M}{2}$.

Виходи суматора 17 за модулем $M = \prod_{i=1}^n m_i$, і вентильних елементів 16 групи через елементи АБО 19 групи підключено до входу першого 20 вихідного регістра, вихід 21 якого є першим виходом пристрою. Виходи перших (за модулем m_1 СЗК) підрегистрів вхідних регістрів 9 і 10 підключено до входів суматора 22 за модулем два, вихід якого підключено до других (відкриваючих) входів елементів I п'ятої 15 групи та до других (заборонених) входів вентильних елементів 16 групи. Виходи i-х ($i = \overline{1, n}$) підрегистрів третього 11 вхідного регістра підключено до перших входів відповідних суматорів 23₁-23_n, до других входів яких підключені шини 24 (24₁-24_n) подачі відповідних значень $k_{i_j} \cdot m_i$ констант. Виходи суматорів 23₁-23_n підключено до перших входів відповідних пристроїв 25₁-25_n, для ділення, до других входів яких підключено відповідні виходи підрегистрів четвертого 12 вхідного регістра, а виходи пристроїв 25₁-25_n для ділення підключені до входів відповідних підрегистрів другого 26 вихідного регістра, вихід 27 якого є другим виходом пристрою.

Роботу пристрою доцільно розглянути у двох режимах. Перший режим роботи - реалізація операції множення двох чисел $A'_{СЗК}$ і $B'_{СЗК}$, а другий режим - реалізація операції ділення двох чисел $A'_{СЗК}$ і $B'_{СЗК}$.

Перший режим роботи пристрою (існує сигнал шини 7). За першим 1 та другим 2 входами пристрою через елементи I 3 і 5 до першого 9 та другого 10 вхідних регістрів поступають значення чисел у СЗК, що представлені у ШФ, тобто $A'_{СЗК} = (a'_1 \parallel a'_2 \parallel \dots \parallel a'_i \parallel \dots \parallel a'_n)$ і $B'_{СЗК} = (b'_1 \parallel b'_2 \parallel \dots \parallel b'_i \parallel \dots \parallel b'_n)$. З виходу регістрів 9 і 10 пара лишків a'_i та b'_i ($i = \overline{1, n}$) надходить до входів відповідного i-го пристрою 13_i для множення лишків a'_i та b'_i , з виходу якого значення $c'_i = (a'_i \cdot b'_i) \bmod m_i$ надходить до входу i-го під регістра прийомного регістра 14, з виходу якого значення $C'_{СЗК} = (c'_1 \parallel c'_2 \parallel \dots \parallel c'_i \parallel \dots \parallel c'_n)$ надходить до перших входів елементів I 15 п'ятої групи та вентильних елементів 16 групи, до других входів яких, з виходу суматора 22, надходить

значення $(a'_1 + b'_1) \bmod 2$. Якщо $(a'_1 + b'_1) \bmod 2 = 1$ (присутній вихідний сигнал суматора 22), тоді через відкриті елементи І 15 групи значення $C'_{СЗК} = (c'_1 \parallel c'_2 \parallel \dots \parallel c'_i \parallel \dots \parallel c'_n)$ поступає до перших входів суматора 17 за модулем $M = \prod_{i=1}^n m_i$, на другі входи якого за шиною 18 надходить

значення $\frac{M}{2}$. З виходу суматора 17 значення $(C' + \frac{M}{2}) \bmod M$ через елементи АБО групи 19

5 надходить до входу першого вихідного регістра 20. Якщо $(a'_1 + b'_1) \bmod 2 = 0$ (відсутній вихідний сигнал суматора 22), тоді через відкриті вентильні елементи групи 16 (відсутній сигнал заборони) значення $C'_{СЗК} = (c'_1 \parallel c'_2 \parallel \dots \parallel c'_i \parallel \dots \parallel c'_n)$ через елементи АБО групи 19 надходить до входу першого вихідного регістра 20.

10 Другий режим роботи пристрою (існує сигнал шини 8). За першим 1 та другим 2 входами пристрою через елементи І 4 і 6 до третього 11 та четвертого 12 вхідних регістрів надходять значення чисел у СЗК, що представлені у ШФ, тобто $A'_{СЗК} = (a'_1 \parallel a'_2 \parallel \dots \parallel a'_i \parallel \dots \parallel a'_n)$ і $B'_{СЗК} = (b'_1 \parallel b'_2 \parallel \dots \parallel b'_i \parallel \dots \parallel b'_n)$. З виходу і-го під регістра третього регістра 11 значення лишку a'_i надходить до першого входу і-го ($i = \overline{1, n}$) суматора 23_i, на другий вхід якого за шиною 24_i надходить значення відповідної константи $k_{i_j} \cdot m_i$. З виходу суматора 23_i значення $a'_i + k_{i_j} \cdot m_i$

15 надходить до першого входу і-го ($i = \overline{1, n}$) пристрою 25_i для ділення, до другого входу якого, з виходу і-го під регістра четвертого регістра 12, надходить значення лишку b'_i . З виходів пристроїв 25 результат $C'_{СЗК} = (c'_1 \parallel c'_2 \parallel \dots \parallel c'_i \parallel \dots \parallel c'_n)$ ділення, якщо ділене цілком ділиться на дільник, надходить до входу другого 26 вихідного регістра.

20 Розглянемо приклади процесу функціонування винаходу для конкретних СЗК у двох режимах роботи. Перший режим роботи - реалізація операції множення двох чисел $A'_{СЗК}$ і $B'_{СЗК}$ а другий режим - реалізація операції ділення двох чисел $A'_{СЗК}$ і $B'_{СЗК}$.

Перший режим. Розглянемо процес функціонування винаходу для СЗК, що задано основами $m_1=2, m_2=3, m_3=5$. При цьому $M=30, \frac{M}{2} = 15$. В таблиці 2 представлено кодові слова для даної СЗК, що задана основами $m_1=2, m_2=3, m_3=5$.

25 Приклад 1. Для чисел у позиційній системі числення (ПСЧ) $A_{ПСЧ}=-3, B_{ПСЧ}=-4$ сформуємо у СЗК їх ШФ А' і В' у вигляді (див. табл. 2):

$$A'_{СЗК} = \frac{M}{2} - A_{СЗК} = (1 \parallel 0 \parallel 0) - (1 \parallel 0 \parallel 3) = (0 \parallel 0 \parallel 2),$$

$$B'_{СЗК} = \frac{M}{2} - B_{СЗК} = (1 \parallel 0 \parallel 0) - (1 \parallel 0 \parallel 4) = (1 \parallel 2 \parallel 1).$$

30 У регістр 9 заноситься число $A'_{СЗК} = (0 \parallel 0 \parallel 2)$, а у регістр 10 - $B'_{СЗК} = (1 \parallel 2 \parallel 1)$. З виходів групи 13₁+13₃ пристроїв множення отримуємо наступні значення: $13_1 \cdot (0 \cdot 1) \bmod 2 = 0$; $13_2 \cdot (0 \cdot 2) \bmod 3 = 0$ і $13_3 \cdot (2 \cdot 1) \bmod 5 = 2$. Таким чином до входу регістра 14 надходить значення $C'_{СЗК} = (0 \parallel 0 \parallel 2)$. Так, як $(a'_1 + b'_1) \bmod 2 = (0 + 1) \bmod 2 = 1$, тоді вихідний сигнал суматора 22 присутній. Він відкриває елементи І п'ятої групи 15, через які значення $C'_{СЗК} = (0 \parallel 0 \parallel 2)$

35 $\frac{M}{2} = (1 \parallel 0 \parallel 0)$. З виходу суматора 17 значення $C_p = (C'_{СЗК} + \frac{M}{2}) = (0 \parallel 0 \parallel 2) + (1 \parallel 0 \parallel 0) = (1 \parallel 0 \parallel 2)$ через елементи АБО 19 надходить до входу першого вихідного регістра 20. (Результат значення $C_p = (1 \parallel 0 \parallel 2)$ у ПСЧ дорівнює 27).

Кодові слова у СЗК

A(B) у ПСЧ	A'(B') у ПСЧ	A'(B') у СЗК		
		m ₁ =2	m ₂ =3	m ₃ =5
-15	0	0	0	0
-14	1	1	1	1
-13	2	0	2	2
-12	3	1	0	3
-11	4	0	1	4
-10	5	1	2	0
-9	6	0	0	1
-8	7	1	1	2
-7	8	0	2	3
-6	9	1	0	4
-5	10	0	1	0
-4	11	1	2	1
-3	12	0	0	2
-2	13	1	1	3
-1	14	0	2	4
0	15	1	0	0
1	16	0	1	1
2	17	1	2	2
3	18	0	0	3
4	19	1	1	4
5	20	0	2	0
6	21	1	0	1
7	22	0	1	2
8	23	1	2	3
9	24	0	0	4
10	25	1	1	0
11	26	0	2	1
12	27	1	0	2
13	28	0	1	3
14	29	1	2	4

Перевірка (див. табл. 2). $[(-3) \cdot (-4)]' = 15 + (-3) \cdot (-4) = 15 + 12 = 27 = C_p$.

5 Приклад 2. Для чисел у ПСЧ $A_{ПСЧ}=3$, $B_{ПСЧ}=4$ сформуємо у СЗК їх ШФ A' і B' у вигляді (див. табл. 2):

$$A'_{ПСЧ} = \frac{M}{2} + A_{ПСЧ} \text{ і } B'_{ПСЧ} = \frac{M}{2} + B_{ПСЧ}, \text{ або}$$

$$A'_{СЗК} = \frac{M}{2} + A_{СЗК} = (1 \parallel 0 \parallel 0) + (1 \parallel 0 \parallel 3) = (0 \parallel 0 \parallel 3),$$

$$B'_{СЗК} = \frac{M}{2} + B_{СЗК} = (1 \parallel 0 \parallel 0) + (0 \parallel 1 \parallel 4) = (1 \parallel 1 \parallel 4).$$

10 За входами 1 і 2 пристрою в регістри 9 і 10 відповідно надходять наступні значення: $13_1 - 0 \cdot 1) \bmod 2 = 0$; $13_2 - (0 \cdot 1) \bmod 3 = 0$ і $13_3 - (3 \cdot 4) \bmod 5 = 2$. Таким чином до входу регістра 14 надходить значення $C'_{СЗК} = (0 \parallel 0 \parallel 2)$. Так як $(a'_1 + b'_1) \bmod 2 = (0 + 1) \bmod 2 = 1$ (табл. 1), тоді вихідний сигнал суматора 22 відкриває елементи I групи 15 (вентильні елементи групи 16 закриті). У цьому випадку з регістра 14 значення $C'_{СЗК} = (0 \parallel 0 \parallel 2)$ через відкриті елементи I групи 15 надходить до перших входів суматора 17, до других входів якого по шині 18 надходить

15 значення $\frac{M}{2} = (1 \parallel 0 \parallel 0)$. З виходу суматора 17 результат C_p множення двох чисел $A'_{СЗК}$ і $B'_{СЗК}$,

представлений у вигляді $C_p = (C'_{СЗК} + \frac{M}{2}) = (0 \parallel 0 \parallel 2) + (1 \parallel 0 \parallel 0) = (1 \parallel 0 \parallel 2)$ через елементи АБО групи 19 надходить до входу регістра 20.

Перевірка (табл. 2). Зробимо перевірку правильності отриманого результату множення двох чисел $A'_{СЗК} = (0 \parallel 0 \parallel 3)$ (у ПСЧ $A'_{ПСЧ} = 18$ і $A'_{ПСЧ} = 3$) та $V'_{СЗК} = (1 \parallel 1 \parallel 4)$ (у ПСЧ буде $V'_{ПСЧ} = 19$ і $V'_{ПСЧ} = 4$). Результат множення $C_p = (1 \parallel 0 \parallel 2)$ у ПСЧ дорівнює значенню 27.

У відповідності з ознакою ШФ чисел у СЗК для перевірки отриманого результату маємо наступну умову, що представлена рівнянням:

$$(A_{ПСЧ} \cdot V_{ПСЧ})' = \left[\frac{M}{2} + (A_{ПСЧ} \cdot V_{ПСЧ}) \right] \bmod M = C_p,$$

$$\text{або } (A_{ПСЧ} \cdot V_{ПСЧ})' = [15 + (A_{ПСЧ} \cdot V_{ПСЧ})] \bmod 30 = C_p.$$

Таким чином маємо (див. табл. 2) $(3 \cdot 4)' = 15 + 3 \cdot 4 = 27 = C_p$.

Приклад 3. Для чисел ПСЧ $A_{ПСЧ} = -3$, $V_{ПСЧ} = 4$ сформуємо у СЗК їх ШФ A' і V' у вигляді (див. табл. 2):

$$A'_{СЗК} = \frac{M}{2} - A_{СЗК} = (1 \parallel 0 \parallel 0) - (1 \parallel 0 \parallel 3) = (0 \parallel 0 \parallel 2),$$

$$V'_{СЗК} = \frac{M}{2} + V_{СЗК} = (1 \parallel 0 \parallel 0) - (0 \parallel 1 \parallel 4) = (1 \parallel 1 \parallel 4).$$

У регістр 9 заноситься число $A'_{СЗК} = (0 \parallel 0 \parallel 2)$, а у регістр 10 - $V'_{СЗК} = (1 \parallel 1 \parallel 4)$. З виходів групи $13_1 \div 13_3$ пристроїв множення отримуємо наступні значення: $13_1 - (0 \cdot 1) \bmod 2 = 1$; $13_2 - (0 \cdot 1) \bmod 3 = 0$ і $13_3 - (2 \cdot 4) \bmod 5 = 3$. Таким чином до входу регістра 14 надходить значення $C'_{СЗК} = (0 \parallel 0 \parallel 3)$. Так, як $(a'_1 + b'_1) \bmod 2 = (0 + 1) \bmod 2 = 1$, тоді вихідний сигнал суматора 22 присутній. Він відкриває елементи I групи 15, через які значення $C'_{СЗК} = (0 \parallel 0 \parallel 3)$ надходить до

перших входів суматора 17, до других входів якого по шині 18 поступає значення $\frac{M}{2} = (1 \parallel 0 \parallel 0)$.

З виходу суматора 17 значення $C_p = (C'_{СЗК} + \frac{M}{2}) = (0 \parallel 0 \parallel 3) + (1 \parallel 0 \parallel 0) = (1 \parallel 0 \parallel 3)$ через елементи АБО 19 надходить до входу регістра 20 (значення $C_p = (1 \parallel 0 \parallel 3)$ у ПСЧ дорівнює 3).

Перевірка (див. табл. 2). $[(-3) \cdot 4]' = 15 + (-3) \cdot 4 = 15 - 12 = 3 = C_p$. Приклад 4. Для чисел ПСЧ $A_{ПСЧ} = 3$, $V_{ПСЧ} = -4$ сформуємо у СЗК їх ШФ A' і V' у вигляді (див. табл. 2):

$$A'_{СЗК} = \frac{M}{2} + A_{СЗК} = (1 \parallel 0 \parallel 0) - (1 \parallel 0 \parallel 3) = (0 \parallel 0 \parallel 3),$$

$$V'_{СЗК} = \frac{M}{2} - V_{СЗК} = (1 \parallel 0 \parallel 0) - (0 \parallel 1 \parallel 4) = (1 \parallel 2 \parallel 1).$$

У регістр 9 заноситься число $A'_{СЗК} = (0 \parallel 0 \parallel 3)$, а у регістр 10 - $V'_{СЗК} = (1 \parallel 2 \parallel 1)$. З виходів групи $13_1 \div 13_3$ пристроїв множення отримуємо наступні значення: $13_1 - (0 \cdot 1) \bmod 2 = 0$; $13_2 - (0 \cdot 2) \bmod 3 = 0$ і $13_3 - (3 \cdot 1) \bmod 5 = 3$. Таким чином до входу регістра 8 надходить значення $C'_{СЗК} = (0 \parallel 0 \parallel 3)$. Так, як $(a'_1 + b'_1) \bmod 2 = (0 + 1) \bmod 2 = 1$, тоді вихідний сигнал суматора 22 присутній. Він відкриває елементи I групи 15, через які значення $C'_{СЗК} = (0 \parallel 0 \parallel 3)$ надходить до

перших входів суматора 17, до других входів якого по шині 18 надходить значення $\frac{M}{2} = (1 \parallel 0 \parallel 0)$. З виходу суматора 17 значення $C_p = (C'_{СЗК} + \frac{M}{2}) = (0 \parallel 0 \parallel 3) + (1 \parallel 0 \parallel 0) = (1 \parallel 0 \parallel 3)$ через елементи АБО 19 надходить до входу регістра 20 (значення $C_p = (1 \parallel 0 \parallel 3)$ у ПСЧ дорівнює 3).

Перевірка (див. табл. 2). $[3 \cdot (-4)]' = 15 + 3 \cdot (-4) = 15 - 12 = 3 = C_p$.

Приклад 5. Другий режим. Розглянемо процес функціонування винаходу для СЗК,

М що задано основами $m_1 = 2$, $m_2 = 11$, $m_3 = 13$ і $m_4 = 17$. При цьому $M = 4862$, $\frac{M}{2} = 2431$. Нехай задано вихідні числа $A'_{СЗК21} = (1 \parallel 10 \parallel 8 \parallel 4)$, $V'_{СЗК7} = (1 \parallel 7 \parallel 7 \parallel 7)$.

За першим 1 та другим 2 входами пристрою через елементи 1 4 і 6 до третього 11 та четвертого 12 вхідних регістрів надходять значення вихідних чисел у СЗК, що представлені у ШФ, тобто $A'_{СЗК21} = (1 \parallel 10 \parallel 8 \parallel 4)$, $B'_{СЗК7} = (1 \parallel 7 \parallel 7 \parallel 7)$. З виходів підрегістрів третього регістра 11 значення лишків $a'_1 = 1$, $a'_2 = 10$, $a'_3 = 8$ і $a'_4 = 4$ надходять до перших входів першого, 5 другого, третього і четвертого суматорів 23, на другий вхід яких відповідно за першою, другою, третьою і четвертою шинами 24 надходять відповідні значення констант $k_{ij} \cdot m_i$: $k_{10} \cdot m_1 = 0 \cdot 2 = 0$ (табл. 3), $k_{21} \cdot m_2 = 1 \cdot 11 = 11$ (табл. 4), $k_{31} \cdot m_3 = 1 \cdot 13 = 13$ (табл. 5) і $k_{41} \cdot m_4 = 1 \cdot 17 = 17$ (табл. 6). З виходу суматорів 23 значення $a_i + k_{ij} \cdot m_i$: $a'_1 + k_{10} \cdot m_1 = 1 + 0 = 1$, $a'_2 + k_{21} \cdot m_2 = 10 + 11 = 21$, $a'_3 + k_{31} \cdot m_3 = 8 + 13 = 21$ і $a'_4 + k_{41} \cdot m_4 = 4 + 17 = 21$ надходять до 10 перших входів пристроїв 25 для ділення, до другого входу якого, з виходів підрегістрів четвертого регістра 12, надходять значення лишків b'_i : $b'_1 = 1$, $b'_2 = 7$, $b'_3 = 7$ і $b'_4 = 7$. З виходів пристроїв 25 результат

$$C'_{СЗК} = (c'_1 \parallel c'_2 \parallel \dots \parallel c'_i \parallel \dots \parallel c'_n) = (c'_1 \parallel c'_2 \parallel c'_3 \parallel c'_4) =$$

$$c = \left[\left(\frac{a'_1 + k_{1j_1} \cdot m_1}{b'_1} \right) \parallel \left(\frac{a'_2 + k_{2j_2} \cdot m_2}{b'_2} \right) \parallel \left(\frac{a'_3 + k_{3j_3} \cdot m_3}{b'_3} \right) \parallel \left(\frac{a'_4 + k_{4j_4} \cdot m_4}{b'_4} \right) \right] =$$

$$= \left[\left(\frac{1 + 0 \cdot 2}{1} \right) \parallel \left(\frac{10 + 1 \cdot 11}{7} \right) \parallel \left(\frac{8 + 1 \cdot 13}{7} \right) \parallel \left(\frac{4 + 1 \cdot 17}{7} \right) \right] = (1 \parallel 3 \parallel 3 \parallel 3)$$

операції ділення, якщо ділене цілком ділиться на дільник, надходить до входу другого 26 вихідного регістра. Ця величина у ПСЧ дорівнює значенню 3. 15

Перевірка, $\frac{A'_{СЗК21}}{B'_{СЗК7}} = C'_{СЗК}$, тобто $\frac{21}{7} = 3$.

Таблиця 3

Значення констант для k_{1j_1} , $m_1 = 2$, $a'_1 = 1$

j_1	$k_{1j_1} \cdot m_1$	$a'_1 + k_{1j_1} \cdot m_1$
1	1	3

Таблиця 4

Значення констант для k_{2j_2} , $m_2 = 11$, $a'_2 = 10$

j_2	$k_{2j_2} \cdot m_2$	$a'_2 + k_{2j_2} \cdot m_2$
1	11	21
2	22	32
3	33	43
4	44	54
5	55	65
6	66	76
7	77	87
8	88	98
9	99	109
10	110	120

Таблиця 5

Значення констант для $k_{3_{j_3}}$, $m_3 = 13$, $a_2' = 8$

j_3	$k_{3_{j_3}} \cdot m_3$	$a_3' + k_{3_{j_3}} \cdot m_3$
1	13	21
2	26	34
3	39	47
4	52	60
5	65	73
6	78	86
7	91	99
8	104	112
9	117	125
10	130	138
11	143	151
12	156	164

Таблиця 6

Значення констант для $k_{4_{j_4}}$, $m_4 = 17$, $a_4' = 4$

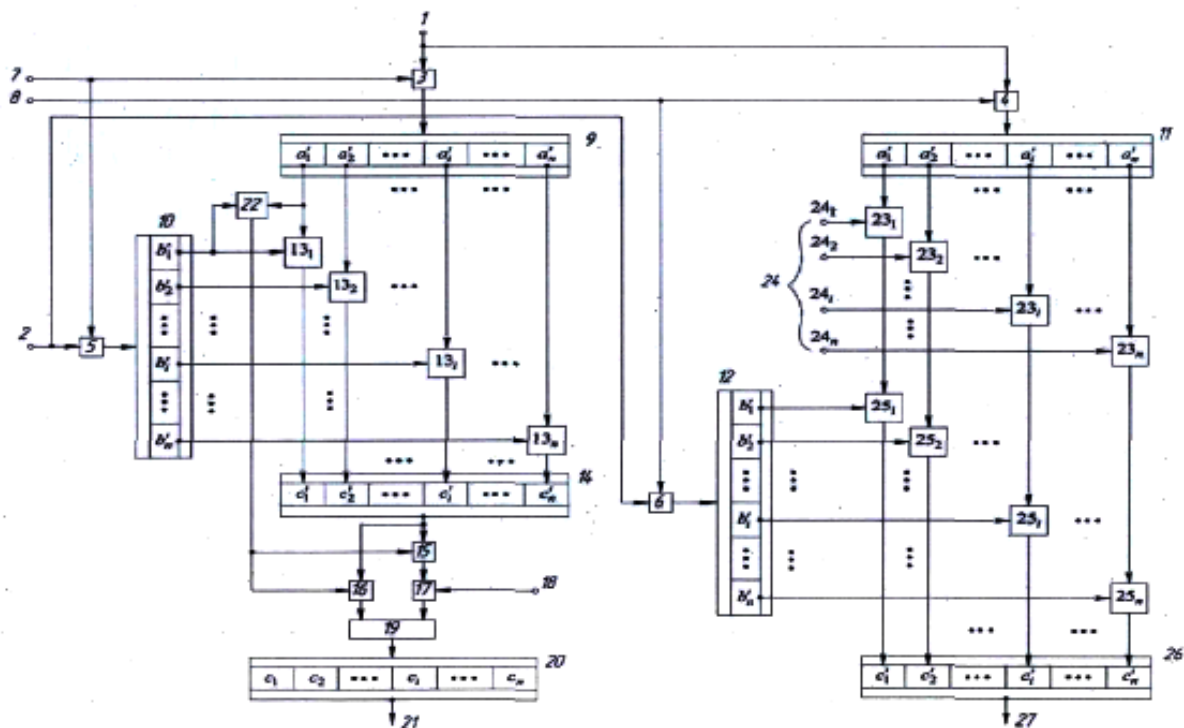
j_3	$k_{4_{j_4}} \cdot m_4$	$a_4' + k_{4_{j_4}} \cdot m_4$
1	17	21
2	34	38
3	51	55
4	68	72
5	85	89
6	102	106
7	119	123
8	136	140
9	153	157
10	170	174
11	187	191
12	204	208
13	221	225
14	238	242
15	255	259
16	272	276

5 Таким чином, запропонований винахід дозволяє суттєво розширити функціональні можливості пристрою-прототипу. Даний ефект досягається шляхом організації, додатково до виконання операції модульного множення двох чисел $A'_{СЗК}$ і $B'_{СЗК}$, процесу виконання операції модульного ділення двох чисел $A'_{СЗК}$ і $B'_{СЗК}$ у СЗК у випадку, якщо ділене цілком ділиться на дільник. Наведені приклади практичного застосування винаходу для конкретної СЗК підтверджують доцільність і цінність отриманих результатів.

10

ФОРМУЛА ВИНАХОДУ

- 5 Пристрій для реалізації операції множення та ділення чисел у системі залишкових класів (СЗК), який містить перший і другий вхідні та перший вихідний реєстри, прийомний реєстр, суматор за модулем два, групу елементів АБО, групу з n пристроїв для множення двох лишків a_i та b_i чисел $A'_{СЗК}$ та $B'_{СЗК}$ за модулями m_i ($i = \overline{1, n}$), де n - кількість модулів СЗК, першу групу елементів І, групу вентилів, суматор за модулем $M = \prod_{i=1}^n m_i$, при цьому виходи i -х ($i = \overline{1, n}$) підреєстрів першого та другого вхідних реєстрів підключено до входів i -го пристрою групи для множення лишків a_i та b_i , відповідно чисел $A'_{СЗК}$ та $B'_{СЗК}$, за модулем m_i СЗК, виходи пристроїв множення групи лишків a_i та b_i за модулями m_i підключено до входів відповідних i -их підреєстрів прийомного реєстра, вихід якого підключено до перших входів елементів І першої групи та вентильних елементів групи, виходи елементів І першої групи підключено до перших входів суматора за модулем $M = \prod_{i=1}^n m_i$, до других входів якого підключена шина подачі значення $\frac{M}{2}$, виходи суматора за модулем $M = \prod_{i=1}^n m_i$ і вентильних елементів групи через елементи АБО групи підключено до входу першого вихідного реєстра, вихід якого є першим виходом пристрою, виходи перших, за модулем m_1 СЗК, підреєстрів вхідних реєстрів підключено до входів суматора за модулем два, вихід якого підключено до других, відкриваючих, входів елементів І першої групи та до других, заборонених, входів вентильних елементів групи, який **відрізняється** тим, що додатково введено другий та третій вхідні реєстри, другий вихідний реєстр, другу, третю, четверту та п'яту групи елементів І, групу з n суматорів, групу з n пристроїв для ділення чисел, при цьому перший вхід пристрою підключено до перших входів елементів І другої та третьої груп, а другий вхід пристрою підключено до перших входів елементів І четвертої та п'ятої груп, до других входів елементів І другої та четвертої груп підключена шина подачі сигналу ознаки операції множення, а до других входів елементів І третьої та п'ятої груп підключена шина подачі сигналу ознаки операції ділення, виходи елементів І другої, третьої, четвертої та п'ятої груп підключено до входів відповідно першого, другого, третього та четвертого вхідних реєстрів, виходи i -х ($i = \overline{1, n}$) підреєстрів третього вхідного реєстра підключено до перших входів i -их суматорів, до других входів яких підключені шини подачі відповідних значень констант, виходи суматорів підключено до перших входів відповідних пристроїв для ділення, до других входів яких підключено відповідні виходи підреєстрів четвертого вхідного реєстра, а виходи пристроїв для ділення підключені до входів відповідних підреєстрів другого вихідного реєстра, вихід якого є другим виходом пристрою.
- 10
- 15
- 20
- 25
- 30



Комп'ютерна верстка Л. Ціхановська

Державна служба інтелектуальної власності України, вул. Василя Липківського, 45, м. Київ, МСП, 03680, Україна

ДП "Український інститут інтелектуальної власності", вул. Глазунова, 1, м. Київ – 42, 01601