УКРАЇНА

(19) UA (11) 119904 (13) U

(51) МПК
G06F 11/08 (2006.01)
H03M 7/18 (2006.01)

МІНІСТЕРСТВО ЕКОНОМІЧНОГО РОЗВИТКУ І ТОРГІВЛІ УКРАЇНИ

(12) ОПИС ДО ПАТЕНТУ НА КОРИСНУ МОДЕЛЬ

(21) Номер заявки: **u 2017 04681**

(22) Дата подання заявки: **15.05.2017**

(24) Дата, з якої є чинними права на корисну модель: **10.10.2017**

(46) Публікація відомостей про видачу патенту: **10.10.2017, Бюл.№ 19**

(72) Винахідник(и):
Краснобаєв Віктор Анатолійович (UA),
Кошман Сергій Олександрович (UA),
Рассомахін Сергій Геннадійович (UA),
Кузнецов Олександр Олександрович (UA),
Янко Аліна Сергіївна (UA)

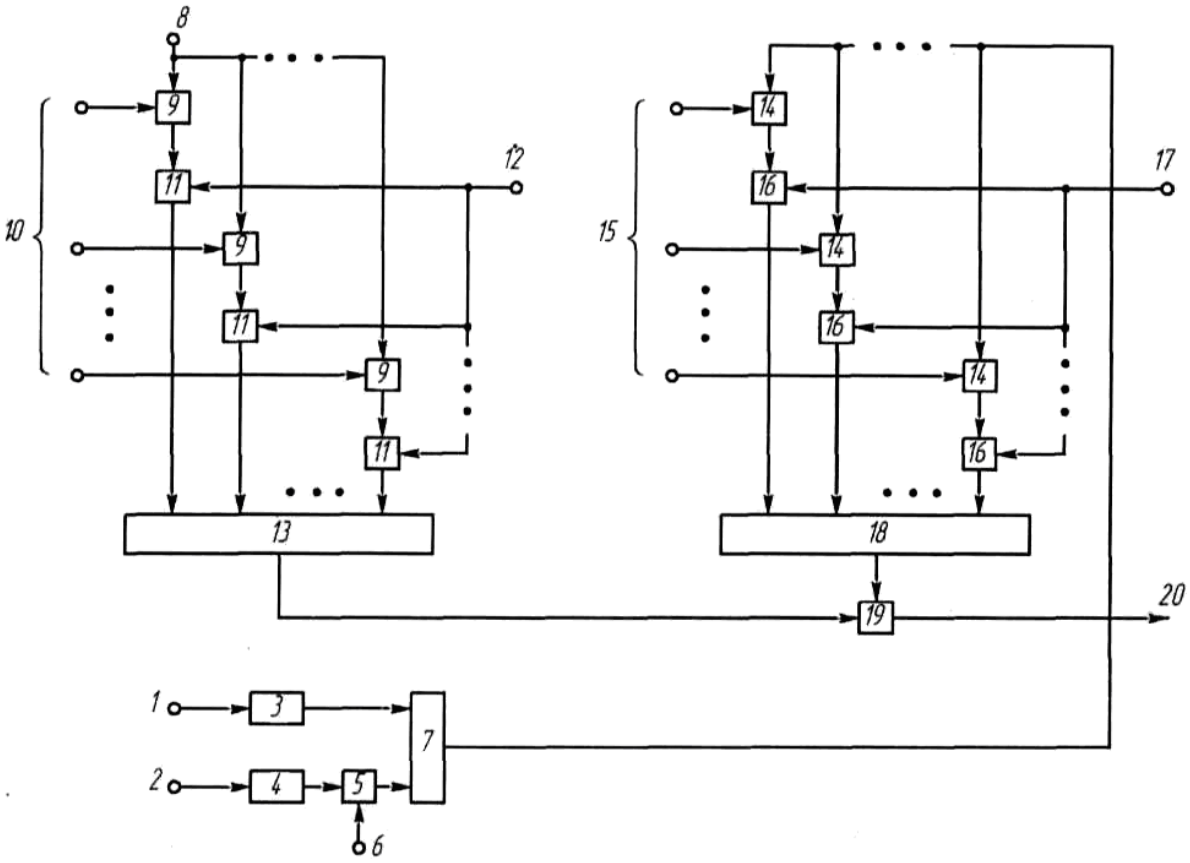
(73) Власник(и):
Краснобаєв Віктор Анатолійович,
вул. Астрономічна, 35-б, к. 24, м. Харків, 61085 (UA),
Кошман Сергій Олександрович,
вул. Різдвяна, 19, к. 409, м. Харків, 61012 (UA),
Рассомахін Сергій Геннадійович,
вул. Астрономічна, 35-г, к. 13, м. Харків, 61085 (UA),
Кузнецов Олександр Олександрович,
пров. Спартаківський, 3, к. 12, м. Харків, 61003 (UA),
Янко Аліна Сергіївна,
вул. Великотирнівська, 36, корп. 3, к. 122, м. Полтава, 36014 (UA)

(54) ПРИСТРІЙ ДЛЯ ВИЗНАЧЕННЯ ДІЙСНИХ ЛИШКІВ ДІЙСНИХ ТА КОМПЛЕКСНИХ ЧИСЕЛ ЗА МОДУЛЯМИ СИСТЕМИ ЗАЛИШКОВИХ КЛАСІВ

(57) Реферат:

Пристрій для визначення дійсних лишків дійсних та комплексних чисел за модулями системи залишкових класів містить перший та другий регістри, блок множення двох чисел, шину подачі значення константи множення, суматор, при цьому перший і другий входи пристрою підключено до входів відповідно першого та другого вхідних регістрів, вихід другого вхідного регістра підключено до першого входу блока множення, до другого входу якого підключена шина подачі значення константи множення, виходи першого регістра та блоку множення підключено до входів суматора. Додатково введено першу та другу групи суматорів, першу та другу групи схем порівняння, перший, другий та третій елементи АБО.

UA 119904 U


8
9
11
12
10
9
11
9
11
13
14
16
17
15
14
16
14
16
18
19
20
1
3
2
4
5
6
7

Корисна модель належить до області автоматики та обчислювальної техніки та може бути застосована в комп'ютерних системах та компонентах, що функціонують у системі залишкових класів (СЗК).

Відомий пристрій (аналог), цю застосовується для перетворення позиційного двійкового коду A у лишок за довільним модулем m_i КЛ (а.с. СРСР № 864278, МПК G06F 5/02, 1978). Пристрій містить блок множення, блок порівняння, регістри, комбінаційний суматор, елементи І та АБО.

Недолік аналога - низька швидкодія визначення лишків дійсних та комплексних чисел у системі залишкових класів.

Відомий пристрій (аналог), що застосовується для перетворення позиційного двійкового коду A у лишок за довільним модулем m_i, КЛ (а.с. СРСР № 1185339, МПК G06F 5/02, 1985). Даний пристрій містить блок порівняння, вхідний та вихідний регістри, суматор, елементи І та АБО.

Недолік аналога - низька швидкодія визначення лишків дійсних та комплексних чисел у системі залишкових класів.

Відомий пристрій (аналог), що застосовується для перетворення позиційного двійкового коду A у лишок за довільним модулем m_i КЛ (а.с. СРСР № 1105895, МПК G06F 11/08, 1983). Пристрій для перетворення позиційного двійкового коду у лишок за довільним модулем m_i, містить лічильник, до першого входу якого підключено перший (установчий) вхід пристрою, блок порівняння та перший елемент І, причому перший вхід першого елемента І є другим (тактовим) входом пристрою, вихід першого елемента І підключено до другого (рахункового) входу лічильника, перший вхід блока порівняння є входом подачі значення модуля m_i.

Недолік аналога - низька швидкодія визначення лишків дійсних та комплексних чисел у системі залишкових класів.

Близьким аналогом за технічною суттю до запропонованої корисної моделі є пристрій для перетворення позиційного двійкового коду у лишок за довільним модулем m (патент України № 92155, МПК G06F 11/08, 2014 р.). Пристрій для перетворення позиційного двійкового коду у лишок за довільним модулем m_i, що містить: лічильник, до першого входу якого підключено перший установчий вхід пристрою, блок порівняння та перший елемент І, при цьому перший вхід першого елемента І є другим тактовим входом пристрою, вихід першого елемента І підключено до другого (рахункового) входу лічильника, перший вхід блока порівняння є входом подачі значення модуля m_i, другий елемент І, блок пам'яті констант, блок множення, суматор і регістр, при цьому вихід суматора підключено до першого інформаційного входу регістра, вихід якого є виходом пристрою, який підключено до першого входу суматора та до другого входу блока порівняння, вихід якого є виходом ознаки кінця перетворення позиційного двійкового коду у лишок за довільним модулем m_i, вихід лічильника підключено до входу блока пам'яті констант, вихід якого підключено до першого входу блока множення, до другого якого підключена шина подачі значення модуля m_i, вихід блока множення підключено до другого входу суматора, другий вихід якого підключено до другого входу першого елемента І і до першого входу другого елемента І, вихід якого підключено до другого входу регістра, другий вхід другого елемента І підключено до другого входу пристрою, шина подачі числа, що перетворюється, підключена до третього входу регістра.

Недолік аналога - низька швидкодія визначення лишків дійсних та комплексних чисел у системі залишкових класів.

Найближчим аналогом до запропонованої корисної моделі є пристрій для визначення лишків дійсних та комплексних чисел у системі залишкових класів (патент України № 114063, МПК G06F 7/72, H03M 7/18, 2017, Бюл. № 7). Пристрій містить перший вхідний регістр, перший суматор, лічильник, перший блок пам'яті констант (БПК), блок порівняння (БП), при цьому перший (тактовий) вхід пристрою підключено до входу лічильника, а вихід першого регістра підключено до перших входів першого суматора. В пристрій додатково введено першу, другу та третю групи елементів АБО, другий БПК, першу, другу та третю групи елементів І, другий і третій вхідні регістри, блок множення, другий суматор, перший та другий елементи І, вентильний елемент, при цьому вихід лічильника підключено до першого входу вентильного елемента, вихід якого підключено до перших входів першого та другого елементів І, до других входів яких підключено відповідно перша та друга керуючі шини пристрою (шини подачі сигналів

ознак відповідно першого та другого режимів роботи пристрою). Виходи першого та другого елементів І підключено до входів відповідно першого та другого БПК, виходи яких через елементи АБО першої групи підключено до других входів першого суматора, вихід якого підключено до перших входів БП і до перших входів елементів І першої групи, виходи яких є виходом пристрою. Другий (інформаційний) вхід пристрою через елементи АБО другої групи підключено до входу першого регістра. Третій і четвертий (інформаційні) входи пристрою підключено до входів відповідно другого та третього вхідних регістрів, вихід третього вхідного регістра підключено до першого входу блока множення, до другого входу якого підключена шина подачі значення константи ρ множення, виходи другого регістра та блока множення підключено до входів другого суматора, вихід якого підключено до входів елементів АБО другої групи. До перших входів елементів І другої та третьої груп підключено шини подачі значень відповідно першого та другого модулів пристрою, до других (відкриваючих) входів елементів І другої та третьої груп підключено відповідно перша та друга керуючі шини пристрою, виходи елементів І другої та третьої груп через елементи АБО третьої групи підключено до других входів БП, перший вихід якого підключено до других (відкриваючих) входів елементів І першої групи, а другий вихід БП підключено до другого (забороненого) входу вентильного елемента.

Недолік найближчого аналога - низька швидкодія визначення дійсних лишків дійсних та комплексних чисел у СЗК. Цей недолік обумовлено послідовним за порядком отриманням дійсних лишків дійсних та комплексних чисел, а також чітко послідовним функціонуванням суматорів і схем порівняння.

Задача корисної моделі - підвищення швидкодії визначення дійсних лишків дійсних та комплексних чисел у СЗК.

Поставлена задача вирішується тим, що в пристрій для визначення дійсних лишків дійсних та комплексних чисел за модулями системи залишкових класів, що містить перший та другий регістри, блок множення двох чисел, шину подачі значення константи множення, суматор, при цьому перший і другий входи пристрою підключено до входів відповідно першого та другого вхідних регістрів, вихід другого вхідного регістра підключено до першого входу блока множення, до другого входу якого підключена шина подачі значення константи множення, виходи першого регістра та блока множення підключено до входів суматора, додатково введено першу та другу групи суматорів, першу та другу групи схем порівняння (СП), перший, другий та третій елементи АБО, при цьому, третій вхід пристрою підключено до перших входів суматорів першої групи, до других входів яких підключено відповідні шини подачі констант першої групи, виходи суматорів першої групи підключено до перших входів відповідних СП першої групи, до других входів яких підключено шину подачі модуля m_i, а виходи СП першої групи підключено до входів першого елемента АБО, вихід суматора підключено до перших входів суматорів другої групи, до других входів яких підключено відповідні шини подачі констант другої групи, виходи суматорів другої групи підключено до перших входів відповідних СП другої групи, до других входів яких підключено шину подачі модуля N, а виходи СП другої групи підключено до входів другого елемента АБО, виходи першого та другого елементів АБО підключено до входів третього елемента АБО, вихід якого є виходом пристрою.

Введення вказаних ознак дозволяє підвищити швидкодію операції визначення дійсних лишків $\alpha \equiv A(\mathrm{mod}\, m_i)$ дійсних чисел A за довільним дійсним модулем m_i СЗК, а також операції визначення дійсних лишків h комплексних чисел $\dot{A} = a + bi$ за довільним комплексним модулем $\dot{m} = p + qi$ СЗК.

Відповідно до наслідків першої фундаментальної теореми Гауса, за заданим комплексним модулем $\dot{m} = p + qi$, норма N якого дорівнює $N = p^2 + q^2$, та при найбільшому загальному дільнику (НЗД) чисел p і q $(p,q) = 1$, комплексне число $\ddot{A} = a + bi$ порівняно з одним і лише одним лишком з ряду $0,1,2,\ldots,N-2,N-1$ чисел. Тобто, $\dot{A} \equiv h(\mathrm{mod}\, \dot{m})$, де h - дійсне ціле число. Ізоморфізм між комплексними числами та їх дійсними лишками дає можливість реалізувати процес визначення лишків комплексних чисел за допомогою алгоритму визначення лишків числа у дійсній області.

З теорії чисел відомо, що для двох чисел p і q таких, що НЗД $(p,q) = 1$, знайдуться два цілих числа u та v, такі, що виконується умова

$$u \cdot p + v \cdot q = 1. \quad (1)$$

Крім цього відомо, що існує таке число h, що визначається з наступного порівняння

$[a+(u\cdot q-v\cdot p)\cdot b]\equiv h(\mathrm{mod}N)$ (2)

або

$(a+b\cdot\rho)\equiv h(\mathrm{mod}N)$, (3)

де вираз

$\rho=u\cdot q-v\cdot p$ (4)

за допомогою якого установлюється відповідність між комплексними та дійсними лишками чисел, називають коефіцієнтом ізоморфізму. В цьому випадку дійсний лишок h комплексного числа $\dot{A}$ визначається за алгоритмом визначення дійсного лишку α дійсного числа A, тобто

$h\equiv Z(\mathrm{mod}N)$, (5)

де

$Za+b\cdot\rho;\ N=p^2+q^2$. (6)

На кресленні представлена блок-схема корисної моделі, де: 1, 2 - перший (шина подачі дійсної частині а комплексного числа $\dot{A}=a+bi$) та другий (шина подачі уявної частини b комплексного числа) входи пристрою; 3, 4 - перший та другий вхідні регістри; 5 - блок множення двох чисел b і ρ; 6 - шина подачі значення константи $\rho=u\cdot q-v\cdot p$ множення; 7 - суматор; 8 - шина третього входу пристрою; 9 - перша група суматорів; 10 - шини подачі констант першої групи; 11 - перша група схем порівняння (СП); 12 - шина подачі модуля m_i; 13 - перший елемент АБО; 14 - друга група суматорів; 15 - шини подачі констант другої групи; 16 - друга група СП; 17 - шина подачі модуля N; 18 - другий елемент АБО; 19 - третій елемент АБО; 20 - вихід пристрою.

Перший 1 і другий 2 входи пристрою підключено до входів відповідно першого 3 та другого 4 вхідних регістрів, вихід другого 4 вхідного регістра підключено до першого входу блока 5 множення, до другого входу якого підключена шина 6 подачі значення ρ константи множення. Виходи першого 3 регістра та блока 5 множення підключено до входів суматора 7. Третій 8 вхід пристрою підключено до перших входів суматорів першої 9 групи, до других входів яких підключено відповідні шини 10 подачі констант першої групи. Виходи суматорів першої 11 групи підключено до перших входів відповідних СП першої 9 групи, до других входів яких підключено шину 12 подачі модуля m_i. Виходи СП першої 11 групи підключено до входів першого 13 елемента АБО. Вихід суматора 7 підключено до перших входів суматорів другої 14 групи, до других входів яких підключено відповідні шини 15 подачі констант другої групи. Виходи суматорів другої 14 групи підключено до перших входів відповідних СП другої 16 групи, до других входів яких підключено шину 17 подачі модуля N, а виходи СП другої 16 групи підключено до входів другого 18 елемента АБО. Виходи першого 13 та другого 18 елементів АБО підключено до входів третього 19 елемента АБО, вихід 20 якого є виходом пристрою.

Пристрій для визначення дійсних лишків дійсних та комплексних чисел у системі залишкових класів функціонує у двох режимах.

Перший режим. Визначення дійсного лишку $\alpha\equiv A(\mathrm{mod}\ m_i)$ дійсного числа A за дійсним модулем m_i.

За третім 8 входом пристрою дійсне число A надходить до перших входів суматорів першої 9 групи, до других вході яких надходять відповідні значення $0\cdot m_i,1\cdot m_i,\ldots,k\cdot m_i$ констант 10. Суматори 9 виконують операцію $A-k\cdot m_i\ \ (k=0,1,2,\ldots)$, результат якої надходить до перших входів СП 11, до других входів за шиною 12 надходить значення модуля m_i. З виходу однієї СП 11, для якої виконується умова, $\alpha=A-k\cdot m_i\le m_i$, лишок $\alpha\equiv A(\mathrm{mod}\ m_i)$ через елементи АБО 13 і 19 надходить до виходу 20 пристрою.

Другий режим. Визначення дійсного лишку $h\equiv\dot{A}(\mathrm{mod}\ \dot{m})$ комплексного числа $\dot{A}=a+bi$ за комплексним модулем $\dot{m}=p+qi$.

За першим 1 та другим 2 входами відповідно до першого 3 (дійсна a частина комплексного числа) і другого 4 (уявна b частина комплексного числа) регістрів надходить значення комплексного числа $\dot{A}=a+bi$. На перші та другі входи суматора 7 відповідно надходять значення a і $b\cdot\rho$ (див. співвідношення (4) та (6)). З виходу суматора 7 значення Z (див.

співвідношення (6)) надходить до перших входів суматорів 14, до других входів яких за шинами 15 надходять відповідні значення $0 \cdot N, 1 \cdot N, 2 \cdot N, \ldots$. Суматори 14 виконують операцію $Z - l \cdot N$, результати якої надходять до перших входів СП 16, до других входів яких за шиною 17 надходить значення $N = p^2 + q^2$. В цьому випадку з виходу однієї СП 16 значення лишку $h \equiv Z(\mathrm{mod} N)$ через елементи АБО 18 і 19 надходить до виходу 20 пристрою.

Розглянемо процес функціонування корисної моделі для двох режимів роботи пристрою при конкретних значеннях модулів СЗК.

Перший режим. Нехай $A = 20$ і $m_i = 3$. У таблиці 1 представлено спрощений алгоритм визначення дійсного лишку $\alpha \equiv A(\mathrm{mod}\ m_i)$ дійсного числа $A = 20$ за дійсним модулем $m_i = 3$.

За третім 8 входом пристрою дійсне число $A = 20$ надходить до перших входів суматорів першої 9 групи, до других входів яких надходять відповідні значення $0 \cdot 3, 1 \cdot 3, \ldots, k \cdot 3$ констант 10. Суматори 9 виконують операцію $20 - k \cdot 3$ $(k = 0,1,2,\ldots)$, результат якої надходить до перших входів СП 11, до других входів за шиною 12 надходить значення модуля $m_i = 3$. З виходу однієї СП 11, для якої виконується умова, $\alpha = 20 - k \cdot 3_i \le 3_i$, $(A - 6 \cdot m_i = 20 - 18 = 2)$, лишок $2 \equiv 20(\mathrm{mod} 3)$ (табл. 1) через елементи АБО 13 і 19 надходить до виходу 20 пристрою.

Таблиця 1

Перший режим при $A = 20$, $m_i = 3$

Значення констант $k \cdot m_i$ шин 10	Виходи перших суматорів 9	Результати порівняння СП 11
0	20-0=20	20>3
3	20-3=17	17>3
6	20-6=14	14>3
9	20-9=11	11>3
12	20-12=8	8>3
15	20-15=5	5>3
18	20-18=2	2<3 (α=2)

Другий режим. Визначення дійсного лишку $h \equiv \dot{A}(\mathrm{mod}\ \dot{m})$ комплексного числа $\dot{A} = a + bi$ за комплексним модулем $\dot{m} = p + qi$. У таблиці 2 представлено спрощений алгоритм визначення дійсного лишку дійсного лишку $h \equiv \dot{A}(\mathrm{mod}\ \dot{m})$ комплексного числа $\dot{A} = 3 + 4i$ за комплексним модулем $\dot{m} = 1 + 2i$.

На основі співвідношень (1) - (6) визначимо необхідні числові значення. Так на основі співвідношення (1) визначимо значення $\rho = 2$. Маємо, що

$$u \cdot p + v \cdot q = 1,$$

$$u \cdot 1 + v \cdot 2 = 1.$$

Таблиця 2

Другий режим при $Z = 11$, $N = 5$

Значення констант $l \cdot N$ шин 15	Значення $Z = a + b \cdot \beta$ на виході суматора 7	Виходи суматорів 14 $Z - l \cdot N$	Результат порівняння СП 16
0	$Z = 11$	11-0=11	11>5
5		11-5=6	6>5
10		11-10=1	1<5

Ця рівність справедлива при наступних значеннях: $u = -1$, $v = 1$. Дійсно

$(-1)\cdot 1+1\cdot 2=1$.

В цьому випадку визначимо константу (коефіцієнт ізоморфізму) множення ρ, що подається до входу 6 блока 5 множення (див. (4))

$\rho = u\cdot q - v\cdot p = (-1)\cdot 1 - 1\cdot 2 = -3$,

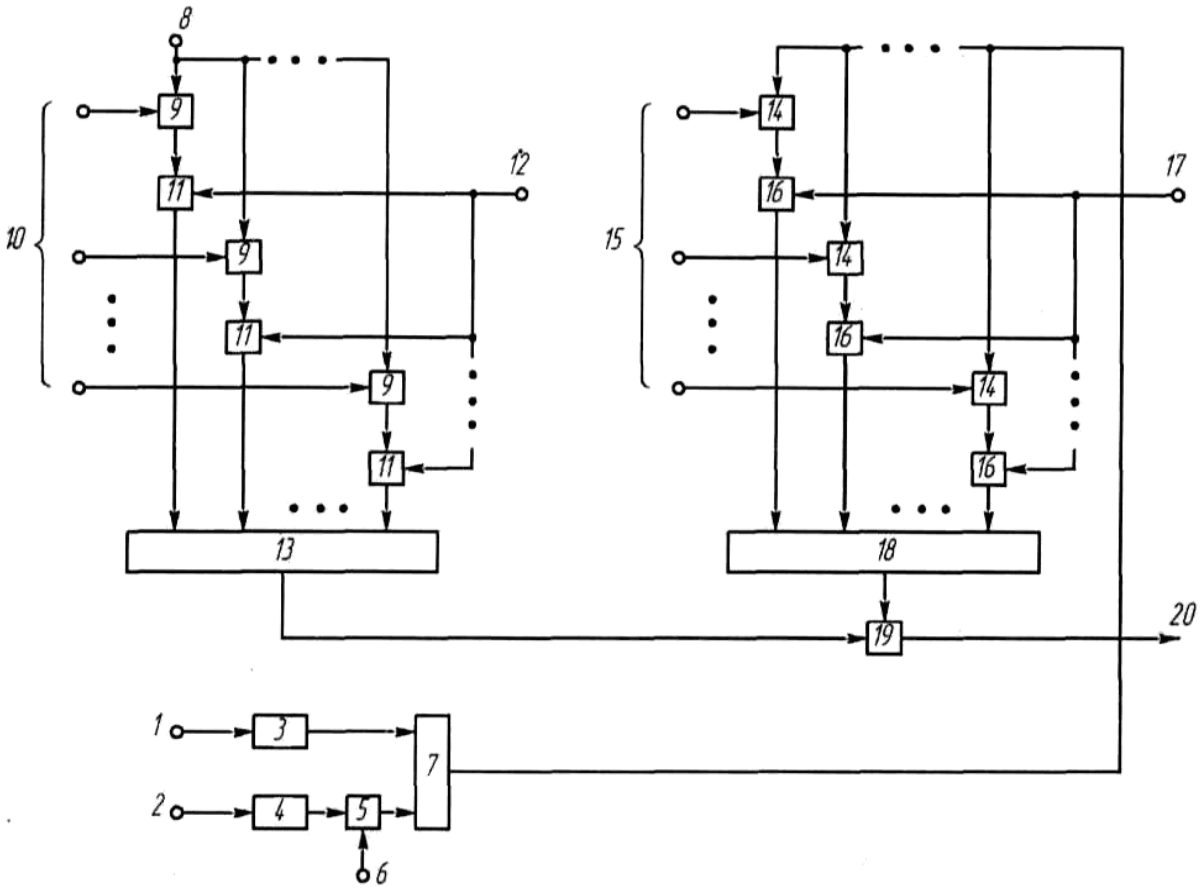
або $(-3)\equiv 2(\mathrm{mod}5)$. Так, у відповідності до (6) норма N модуля $\dot{m}$ дорівнює $N = p^2 + q^2 = 1^2 + 2^2 = 5$.

За першим 1 та другим 2 входами відповідно до першого 3 (дійсна a частина комплексного числа) і другого 4 (уявна b частина комплексного числа) регістрів надходить значення комплексного числа $\dot{A} = 3 + 4i$. На перші та другі входи суматора 7 відповідно надходять значення $a = 2$ і $b\cdot\rho = 8$ (див. співвідношення (4) та (6)). З виходу суматора 7 значення $Z = a + b\cdot\rho = 3 + 8 = 11$ (див. співвідношення (6)) надходить до перших входів суматорів 14, до других входів яких за шинами 15 надходять відповідні значення $0\cdot 5, 1\cdot 5, 2\cdot 5, \ldots$. Суматори 14 виконують операцію $Z - l\cdot N = 11 - l\cdot 5$, результати якої надходять до перших входів СП 16, до других входів яких за шиною 17 надходить значення $N = p^2 + q^2 = 5$. В цьому випадку з виходу однієї СП 16 значення $11 - 2\cdot 5 = 11 - 10 = 1$ лишку $h \equiv Z(\mathrm{mod}N)$ через елементи АБО 18 і 19 надходить до виходу 20 пристрою. Таким чином маємо значення дійсного лишку $h = 111 - 2\cdot 5 = 11 - 10 = 1$ (табл. 2).

Таким чином, запропонована корисна модель дозволяє підвищити швидкодію визначення дійсних лишків $\alpha \equiv A(\mathrm{mod}\ m_i)$ дійсних чисел за дійсним модулем та дійсних лишків $h \equiv \dot{A}(\mathrm{mod}\ \dot{m})$ комплексних чисел за комплексним модулем у СЗК. Це обумовлено тим, що процес визначення дійсних лишків здійснюється паралельно у часі. Дана обставина дозволяє підвищити ефективність використання непозиційних кодових структур у комп'ютерних системах та компонентах, що функціонують у СЗК.

ФОРМУЛА КОРИСНОЇ МОДЕЛІ

Пристрій для визначення дійсних лишків дійсних та комплексних чисел за модулями системи залишкових класів, що містить перший та другий регістри, блок множення двох чисел, шину подачі значення константи множення, суматор, при цьому перший і другий входи пристрою підключено до входів відповідно першого та другого вхідних регістрів, вихід другого вхідного регістра підключено до першого входу блока множення, до другого входу якого підключена шина подачі значення константи множення, виходи першого регістра та блока множення підключено до входів суматора, який **відрізняється** тим, що додатково введено першу та другу групи суматорів, першу та другу групи схем порівняння (СП), перший, другий та третій елементи АБО, при цьому, третій вхід пристрою підключено до перших входів суматорів першої групи, до других входів яких підключено відповідні шини подачі констант першої групи, виходи суматорів першої групи підключено до перших входів відповідних СП першої групи, до других входів яких підключено шину подачі модуля m_i, а виходи СП першої групи підключено до входів першого елемента АБО, вихід суматора підключено до перших входів суматорів другої групи, до других входів яких підключено відповідні шини подачі констант другої групи, виходи суматорів другої групи підключено до перших входів відповідних СП другої групи, до других входів яких підключено шину подачі модуля N, а виходи СП другої групи підключено до входів другого елемента АБО, виходи першого та другого елементів АБО підключено до входів третього елемента АБО, вихід якого є виходом пристрою.



Комп'ютерна верстка О. Рябко

Міністерство економічного розвитку і торгівлі України, вул. М. Грушевського, 12/2, м. Київ, 01008, Україна

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