УКРАЇНА

(19) UA (11) 54637 (13) U

(51) МПК
G06F 7/50 (2006.01)

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ДЕРЖАВНИЙ ДЕПАРТАМЕНТ ІНТЕЛЕКТУАЛЬНОЇ ВЛАСНОСТІ

ОПИС
ДО ПАТЕНТУ НА КОРИСНУ МОДЕЛЬ

видається під відповідальність власника патенту

(54) СУМАТОР ЗА МОДУЛЕМ ПРОСТОГО ЧИСЛА

(21) u201001074
(22) 02.02.2010
(24) 25.11.2010
(46) 25.11.2010, Бюл.№ 22, 2010 р.
(72) ДИЧКА ІВАН АНДРІЙОВИЧ, ОНАЙ МИКОЛА ВОЛОДИМИРОВИЧ
(73) НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ "КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ"

(57) Суматор за модулем простого числа, що містить шину (1) коду першого операнда, шину (2) коду другого операнда, шину (3) коду модуля, регістр (4) першого операнда та регістр (5) другого операнда, першу (7) та другу (8) групу елементів АБО, комбінаційний суматор (9), схему порівняння кодів (10), шину коду операції (14), групу елементів І (26) та вихід (27) пристрою, який **відрізняється** тим, що додатково містить регістр (6) модуля, регістр (11) проміжного результату, двовходовий логічний елемент АБО-НІ (12), блок керування (13), при цьому шина(1) коду першого операнда з'єднана з першими n входами регістра (4) першого операнда, шина (2) другого операнда з'єднана з першими n входами регістра (5) другого операнда, шина (3) коду модуля з'єднана з першими n входами регістра (6) модуля, вихід регістра (4) першого операнда з'єднаний з другим входом групи елементів АБО (7), прямий вихід регістра (5) другого операнда з'єднаний з першим входом другої групи елементів АБО (8), інверсний вихід регістра (5) другого операнда з'єднаний з другим входом другої групи елементів АБО (8), прямий вихід регістра (6) модуля з'єднаний з четвертим входом другої групи елементів АБО (8), а перші n-1 розрядів прямого виходу регістра (6) модуля з'єднані з другим входом схеми порівняння кодів (10), інверсний вихід регістра (6) модуля з'єднаний з третім входом другої групи елементів АБО (8), виходи першої (7) та другої (8) групи елементів АБО з'єднані з відповідними входами комбінаційного суматора (9), вихід комбінаційного суматора (9) з'єднаний з входом регістра (11) проміжного результату, вихід регістра (11) проміжного результату з'єднаний з першим входом першої групи елементів АБО (7) та з першим входом групи елементів І (26), перші n-1 розрядів виходу регістра (11) проміжного результату з'єднані з першим входом схеми порівняння кодів (10), (n+1)-й розряд (15) регістра (11) проміжного результату з'єднаний з другим входом двовходового логічного елемента АБО-НІ (12) та з другим входом блока керування (13), n-й розряд регістрегістра (11) проміжного результату з'єднаний з першим входом двовходового логічного елемента АБО-НІ (12), вихід (16) двовходового логічного елемента АБО-НІ (12) з'єднаний з третім входом блока керування (13), перший вхід блока керування (13) з'єднаний з шиною (14) коду операції, четвертий вхід блока керування (13) з'єднаний з виходом (17) схеми порівняння кодів (10), перший вихід (18) блока керування (13) з'єднаний з входом керування регістра (4) першого операнда, другий вихід (19) блока керування (13) з'єднаний з входом керування видачею коду регістра (5) другого операнда, третій вихід (20) блока керування (13) з'єднаний з входом керування видачею інверсного коду з регістра (5) другого операнда, четвертий вихід (21) блока керування (13) з'єднаний з входом керування видачею коду з регістра (6) модуля, п'ятий вихід (22) блока керування (13) з'єднаний з входом керування видачею інверсного коду з регістра (6) модуля, шостий вихід (23) блока керування (13) з'єднаний з керуючим входом прийому коду в регістр (11) проміжного результату, сьомий вихід (24) блока керування (13) з'єднаний з другим входом групи елементів І (26), восьмий вихід (25) блока керування (13) з'єднаний з входом вхідного переносу комбінаційного суматора (9), вихід (27) групи елементів І (26) є виходом пристрою.

(19) UA (11) 54637 (13) U

Корисна модель належить до галузі автоматики та обчислювальної техніки і може бути використана при реалізації додавання та віднімання за будь-яким модулем, а саме у спеціалізованих обчислювальних пристроях для побудови швидкодіючих пристроїв виконання операцій за модулем, системах криптографічних перетворень, системах цифрового підпису, системах обробки інформації

та системах кодування-декодування даних. Найбільш доцільним використанням даної корисної моделі є її застосування для виконання операцій додавання та віднімання за модулем простого числа.

Відомий пристрій для підсумовування в модулярній системі числення за модулем три [1], що містить шину першого операнда, шину другого операнда, регістр першого операнда та регістр другого операнда, елементи І та елементи АБО, а також шину результату. Даний пристрій дозволяє виконувати операцію додавання за модулем три. Недоліком його є обмежені функціональні можливості, оскільки цей винахід дає можливість виконувати тільки операцію додавання і тільки для фіксованого значення модуля, яке дорівнює трьом.

Відомий суматор за модулем п'ять [2], що містить, групу елементів І та групу елементів АБО, елементи І та АБО. Даний пристрій дозволяє виконувати операцію додавання за модулем п'ять. Недоліком його є обмежені функціональні можливості, оскільки суматор може виконувати тільки операцію додавання і тільки для фіксованого значення модуля, яке дорівнює п'яти.

Відомий суматор за модулем Р [3], що містить шину першого операнда, шину другого операнда, комбінаційний суматор та шину результату. Недоліком цього пристрою є обмежені функціональні можливості, оскільки він виконує тільки операцію додавання двох операндів, а операція віднімання не передбачена.

Найбільш близьким за технічною сутністю (прототипом) і результатом, що досягається, є суматор за модулем системи залишкових класів [4], що містить шини першого операнда, шину керування, шини другого операнда, першу групу елементів АБО, блок інвертування коду вхідного операнда, другу групу елементів АБО, регістр першого та другого операнда, комбінаційний суматор, схему порівняння двійкових чисел, шини коду модуля, елемент НЕ, першу та другу групи елементів І, шини доповняльного коду значення модуля, третю та четверту групи елементів І, елемент І-НЕ, регістр результату, виходи пристрою, при цьому шини першого операнда з'єднані з першими входами першої групи елементів АБО, шини другого операнда з'єднані з входами блока інвертування коду другого вхідного операнда, шина керування з'єднана з керуючим входом блока інвертування коду другого вхідного операнда, виходи блока інвертування коду другого вхідного операнда з'єднані з першими входами другої групи елементів АБО, виходи першої та другої груп елементів АБО з'єднані відповідно з входами регістра першого та другого операндів, виходи регістрів першого та другого операндів з'єднані з відповідними входами комбінаційного суматора, виходи комбінаційного суматора з'єднані з першими входами першої та другої групи елементів І та з першими входами схеми порівняння двійкових чисел, другі входи схеми порівняння двійкових чисел з'єднані з шинами коду модуля, вихід схеми порівняння двійкових чисел з'єднаний з входом елемента НЕ та другими входами другої та третьої груп елементів І, вихід елемента НЕ з'єднаний з другими входами першої групи елементів І, перші входи третьої групи елементів І з'єднані з шинами значення доповняльного коду модуля, виходи другої та третьої груп елементів І з'єднані з другими входами відповідно першої та другої груп елементів АБО, виходи першої групи елементів І, на яких присутній сигнал значення одиничних розрядів у записі модуля, з'єднані з входами елемента І-НЕ, вихід елемента І-НЕ з'єднаний з другими входами четвертої групи елементів І, виходи першої групи елементів І з'єднані з першими входами четвертої групи елементів І, виходи четвертої групи елементів І з'єднані з входами вихідного регістра, виходи вихідного регістра є виходами пристрою.

Недоліком цього пристрою є обмежені функціональні можливості, оскільки він виконує операцію віднімання тільки коли модулем є число двійковий код якого містить всі одиниці, наприклад, 7, 31 (такі числа називають числами Мерсена, узагальнена формула таких чисел має вигляд $P=2^n-1$, де n - будь-яке натуральне число).

В основу корисної моделі покладена задача розширення функціональних можливостей суматора за модулем простого числа. Поставлена задача вирішується тим, що в суматорі за модулем простого числа, що містить шину 1 першого операнда, шину 2 другого операнда, шину 3 коду модуля, регістр 4 першого операнда та регістр 5 другого операнда, першу 7 та другу 8 групу елементів АБО, комбінаційний суматор 9, схему порівняння кодів 10, шину коду операції 14, групу елементів І 26 та вихід 27 пристрою, згідно корисної моделі новим є те, що додано регістр 6 модуля, регістр 11 проміжного результату, двовходовий логічний елемент АБО-НЕ 12, блок керування 13, при цьому шина 1 коду першого операнда з'єднана з першими n входами регістра 4 першого операнда, шина 2 другого операнда з'єднана з першими n входами регістра 5 другого операнда, шина 3 коду модуля з'єднана з першими n входами регістра 6 модуля, вихід регістра 4 першого операнда з'єднаний з другим входом групи елементів АБО 7, прямий вихід регістра 5 другого операнда з'єднаний з першим входом другої групи елементів АБО 8, інверсний вихід регістра 5 другого операнда з'єднаний з другим входом другої групи елементів АБО 8, прямий вихід регістра 6 модуля з'єднаний з четвертим входом другої групи елементів АБО 8, а перші n-1 розрядів прямого виходу регістра 6 модуля з'єднані з другим входом схеми порівняння кодів 10, інверсний вихід регістра 6 модуля з'єднаний з третім входом другої групи елементів АБО 8, виходи першої 7 та другої 8 групи елементів АБО з'єднані з відповідними входами комбінаційного суматора 9, вихід комбінаційного суматора 9 з'єднаний з входом регістра 11 проміжного результату, вихід регістра 11 проміжного результату з'єднаний з першим входом першої групи елементів АБО 7 та з першим входом групи елементів І 26, перші n-1 розрядів виходу регістра 11 проміжного результату з'єднані з першим входом схеми порівняння кодів 10, (n+1)-й розряд 15 регістра 11 проміжного результату з'єднаний з другим входом двовходового логічного елемента АБО-НЕ 12 та з другим входом блока керування 13, n-й розряд регістра 11

проміжного результату з'єднаний з першим входом двовходового логічного елемента АБО-НЕ 12, вихід 16 двовходового логічного елемента АБО-НЕ 12 з'єднаний з третім входом блока керування 13, перший вхід блока керування 13 з'єднаний з шиною 14 коду операції, четвертий вхід блока керування 13 з'єднаний з виходом 17 схеми порівняння кодів 10, перший вихід 18 блока керування 13 з'єднаний з входом керування регістра 4 першого операнда, другий вихід 19 блока керування 13 з'єднаний з входом керування видачею коду регістра 5 другого операнда, третій вихід 20 блока керування 13 з'єднаний з входом керування видачею інверсного коду з регістра 5 другого операнда, четвертий вихід 21 блока керування 13 з'єднаний з входом керування видачею коду з регістра 6 модуля, п'ятий вихід 22 блока керування 13 з'єднаний з входом керування видачею інверсного коду з регістра 6 модуля, шостий вихід 23 блока керування 13 з'єднаний з керуючим входом прийому коду в регістр 11 проміжного результату, сьомий вихід 24 блока керування 13 з'єднаний з другим входом групи елементів 126, восьмий вихід 25 блока керування 13 з'єднаний з входом вхідного переносу комбінаційного суматора 9, вихід 27 групи елементів І 26 є виходом пристрою.

Введення вказаних ознак дозволяє розширити функціональні можливості пристрою, а саме виконувати операції додавання та віднімання за будь-яким модулем.

Сутність винаходу пояснюється кресленнями.

На Фіг.1 наведена структурна схема суматора за модулем простого числа,

на Фіг.2 - функціональна схема блока керування 13,

на Фіг.3 - функціональна схема порівняння кодів 10 для (n-1)-розрядних двійкових чисел,

на Фіг.4 - змістова граф-схема алгоритму роботи суматора за модулем простого числа,

на Фіг.5 - закодована граф-схема алгоритму роботи суматора за модулем простого числа.

На Фіг.1 наведена структурна схема суматора за модулем простого числа, де: 1 - n-розрядна шина коду першого операнда, 2 - n-розрядна шина коду другого операнда, 3 - n-розрядна шина коду модуля, 4 - (n+1)-розрядний регістр першого операнда, він є регістром з асинхронним записом, синхронною видачею коду та виходами на три стани, 5 - (n+1)-розрядний регістр другого операнда, він є регістром з асинхронним записом, синхронною видачею коду та виходами на три стани, 6 - (n+1)-розрядний регістр коду модуля, він є регістром з асинхронним записом, синхронною видачею коду та виходами на три стани, 7 - перша група елементів АБО, 8 - друга група елементів АБО, 9 - комбінаційний суматор, 10 - схема порівняння кодів для (n-1)-розрядних двійкових чисел, 11 - регістр проміжного результату, він є регістром з синхронним записом, асинхронною видачею коду та виходами на три стани, 12 - двовходовий логічний елемент АБО-НЕ, 13- блок керування, 14 - шина коду операції (ОР), 15-вихід (n+1)-го розряду регістра 11 проміжного результату, 16 - вихід двовходового логічного елемента АБО-НЕ 12, 17 - вихід схеми порівняння кодів 10, 18 - перший вихід блока керування 13, 19 - другий вихід блока керування 13, 20 - третій вихід блока керування 13, 21 - четвертий вихід блока керування 13, 22 - п'ятий вихід блока керування 13, 23 - шостий вихід блока керування 13, 24 - сьомий вихід блока керування 13, 25 - восьмий вихід блока керування 13, 26 - група елементів І, 27 - n-розрядний вихід суматора за модулем простого числа.

Шина 1 кода першого операнда з'єднана з першими n входами регістра 4 першого операнда, шина 2 другого операнда з'єднана з першими n входами регістра 5 другого операнда, шина 3 кода модуля з'єднана з першими n входами регістра 6 модуля, вихід регістра 4 першого операнда з'єднаний з другим входом групи елементів АБО 7, прямий вихід регістра 5 другого операнда з'єднаний з першим входом другої групи елементів АБО 8, інверсний вихід регістра 5 другого операнда з'єднаний з другим входом другої групи елементів АБО 8, прямий вихід регістра 6 модуля з'єднаний з четвертим входом другої групи елементів АБО 8, а перші n - 1 розрядів прямого виходу регістра 6 модуля з'єднані з другим входом схеми порівняння кодів 10, інверсний вихід регістра 6 модуля з'єднаний з третім входом другої групи елементів АБО 8, виходи першої 7 та другої 8 групи елементів АБО з'єднані з відповідними входами комбінаційного суматора 9, вихід комбінаційного суматора 9 з'єднаний з входом регістра 11 проміжного результату, вихід регістра 11 проміжного результату з'єднаний з першим входом першої групи елементів АБО 7 та з першим входом групи елементів І 26, перші n-1 розрядів виходу регістра 11 проміжного результату з'єднані з першим входом схеми порівняння кодів 10, (n+1)-й розряд 15 регістра 11 проміжного результату з'єднаний з другим входом двовходового логічного елемента АБО-НЕ 12 та з другим входом блока керування 13, n-й розряд регістра 11 проміжного результату з'єднаний з першим входом двовходового логічного елемента АБО-НЕ 12, вихід 16 двовходового логічного елемента АБО-НЕ 12 з'єднаний з третім входом блока керування 13, перший вхід блока керування 13 з'єднаний з шиною 14 коду операції, четвертий вхід блока керування 13 з'єднаний з виходом 17 схеми порівняння кодів 10, перший вихід 18 блока керування 13 з'єднаний з входом керування регістра 4 першого операнда, другий вихід 19 блока керування 13 з'єднаний з входом керування видачею коду регістра 5 другого операнда, третій вихід 20 блока керування 13 з'єднаний з входом керування видачею інверсного коду з регістра 5 другого операнда, четвертий вихід 21 блока керування 13 з'єднаний з входом керування видачею коду з регістра 6 модуля, п'ятий вихід 22 блока керування 13 з'єднаний з входом керування видачею інверсного коду з регістра 6 модуля, шостий вихід 23 блока керування 13 з'єднаний з керуючим входом прийому коду в регістри проміжного результату, сьомий вихід 24 блока керування 13 з'єднаний з другим входом групи елементів І 26, восьмий вихід 25 блока керування 13 з'єднаний з входом вхідного переносу комбінаційного суматора 9, вихід 27 групи елементів І 26 є виходом пристрою.

На Фіг.2 наведена функціональна схема блока керування 13, де: 14 - однорозрядна шина коду операції, 15 - однорозрядна шина на яку подається результат виконання першої умови, а саме наявність одиниці в (n+1)-му розряді результату, 16 - однорозрядна шина на яку подається результат виконання другої умови, а саме наявність нулів в (n+1)-му та n-му розряді результату, 17 - однорозрядна шина на яку подається результат виконання третьої умови, а саме вихід схеми порівняння кодів 13, 26 - 28 - одновходові логічні елементи І-НЕ, 29 - трьохвходовий логічний елементні, 30-35 - двовходові логічні елементи І, 36 - трьохвходовий логічний елементи І, 37 - двовходовий логічний елементи І, 38 - шестивходовий логічний елемент АБО, 39 - п'ятивходовий логічний елемент АБО, 40-41 - чотирьохвходові логічні елементи АБО, 42 - 45 - D-тригери, інверсні S-входи D-тригерів є входами встановлення в одиницю значень D-тригерів, інверсні R-входи D-тригерів є входами встановлення в нуль значень D-тригерів, С - синхровхід D-тригерів, D - інформаційні входи D-тригерів, 46 - дешифратор на чотири входи, z_0-z_9 - перші десять виходів дешифратора, 47 - трьохвходовий логічний елементи АБО, 48-50 - двовходові логічні елементи АБО, 51 - однорозрядна шина на яку подається сигнал синхронізації роботи блока керування 13, 18 - однорозрядна шина, яка є першим виходом блока керування 13, 19 - однорозрядна шина, яке є другим виходом блока керування 13, 20 - однорозрядна шина, яка є третім виходом блока керування 13, 21 - однорозрядна шина, яка четвертим виходом блока керування 13, 22 - однорозрядна шина, яка є п'ятим виходом блока керування 13, 23 - однорозрядна шина, яка є шостим виходом блока керування 13, 24 - однорозрядна шина, яка є сьомим виходом блока керування 13, 25 - однорозрядна шина, яка є восьмим виходом блока керування 13.

До входу логічного елемента І-НЕ 26 під'єднана шина з сигналом першої умови 15, до входу логічного елемента І-НЕ 27 під'єднана шина третьої умови 17, до входу логічного елемента І-НЕ 28 під'єднана шина другої умови 16, вихід логічного елемента І-НЕ 26 з'єднаний з другим входом логічного елемента І 29, перший вхід логічного елемента І 29 з'єднано з другим виходом (z_2) дешифратора 46, до третього входу логічного елемента І 29 під'єднано шину другої умови 16, перший вхід логічного елемента І 30 з'єднано з третім виходом (z_3) дешифратора 46, другий вхід логічного елемента І 30 під'єднано до шини третьої умови 17, перший вхід логічного елемента І 31 з'єднано з виходом логічного елемента І-НЕ 26, другий вхід логічного елемента 131 з'єднано з шостим виходом (z_6) дешифратора 46, перший вхід логічного елемента 132 з'єднано з нульовим виходом (z_0) дешифратора 46, другий вхід логічного елемента І 32 під'єднано до шини 14 коду операції, перший вхід логічного елемента І 33 з'єднано з другим виходом (z_2) дешифратора 46, другий вхід логічного елемента 133 під'єднано до шини 15 першої умови, перший вхід логічного елемента І 34 з'єднано з третім виходом (z_3) дешифратора 46, другий вхід логічного елемента І 34 з'єднано з виходом логічного елемента І-НЕ 27, перший вхід логічного елемента І 35 з'єднано з шостим виходом (z_6) дешифратора 46, другий вхід логічного елемента І 35 під'єднано до шини 15 першої умови, перший вхід логічного елемента 136 з'єднано з другим виходом (z_2) дешифратора 46, другий вихід логічного елемента 136 з'єднано з виходом логічного елемента І-НЕ 26, третій вхід логічного елемента І 36 з'єднано з виходом логічного елемента І-НЕ 28, перший вхід логічного елемента І 37 з'єднано з шостим виходом (z_6) дешифратора 46, другий вхід логічного елемента 37 під'єднано до шини 15 першої логічної умови, перший вхід логічного елемента АБО 38 з'єднано з сьомим виходом (z_7) дешифратора 46, другий вхід логічного елемента АБО 38 з'єднано з четвертим виходом (24) дешифратора 46, третій вхід логічного елемента АБО 38 з'єднано з виходом логічного елемента І 29, четвертий вхід логічного елемента АБО 38 з'єднано з виходом логічного елемента І 30, п'ятий вхід логічного елемента АБО 38 з'єднано з виходом логічного елемента І 31, шостий вхід логічного елемента АБО 38 з'єднано з восьмим виходом (z_8) дешифратора 46, перший вхід логічного елемента АБО 39 з'єднано з п'ятим виходом (z_5) дешифратора 46, другий вхід логічного елемента АБО 39 з'єднано з виходом логічного елемента І 32, третій вхід логічного елемента АБО 39 з'єднано з виходом логічного елемента І 33, четвертий вхід логічного елемента АБО 39 з'єднано з виходом логічного елемента І 34, п'ятий вхід логічного елемента АБО 39 з'єднано з виходом логічного елемента І 35, перший вхід логічного елемента АБО 40 з'єднано з першим виходом (z_1) дешифратора 46, другий вхід логічного елемента АБО 40 з'єднано з п'ятим виходом (z_5) дешифратора 46, третій вхід логічного елемента АБО 40 з'єднано з виходом логічного елемента І 36, четвертий вхід логічного елемента АБО 40 з'єднано з виходом логічного елемента І 37, перший вхід логічного елемента АБО 41 з'єднано з нульовим виходом (z_0) дешифратора 46, другий вхід логічного елемента АБО 41 з'єднано з восьмим виходом (z_8) дешифратора 46, третій вхід логічного елемента АБО 41 з'єднано з виходом логічного елемента І 36, четвертий вхід логічного елемента АБО 41 з'єднано з виходом логічного елемента І 37, вихід логічного елемента АБО 38 з'єднано з D-входом третього D-тригера 45, вихід логічного елемента АБО 39 з'єднано з D-входом другого D-тригера 44, вихід логічного елемента АБО 40 з'єднано з D-входом першого D-тригера 43, вихід логічного елемента АБО 41 з'єднано з D-входом нульового D-тригера 42, прямі виходи D-тригерів (Q_0, Q_1, Q_2, Q_3) під'єднані до відповідних входів дешифратора 46, перший вхід логічного елемента АБО 47 з'єднано з восьмим виходом (z_8) дешифратора 46, другий вхід логічного елемента АБО 47 з'єднано з другим виходом (z_2) дешифратора 46, третій вхід логічного елемента АБО 47 з'єднано з шостим виходом (z_6) дешифратора 46, вихід 23 логічного елемента АБО 47 є шостим виходом (y_6) блока керування 13, перший вхід логічного елемента АБО 48 з'єднано з першим виходом (z_1) дешифратора 46, другий вхід логічного елемента АБО 48 з'єднано з п'ятим виходом (z_5) дешиф-

ратора 46, вихід 18 логічного елемента АБО 48 є першим виходом (y_1) блока керування 13, перший вхід логічного елемента АБО 49 з'єднано з третім виходом (z_3) дешифратора 46, другий вхід логічного елемента АБО 49 з'єднано з сьомим виходом (z_7) дешифратора 46, вихід 21 логічного елемента АБО 49 є четвертим виходом (y_4) блока керування 13, перший вхід логічного елемента АБО 50 з'єднано з четвертим виходом (z_4) дешифратора 46, другий вхід логічного елемента АБО 50 з'єднано з п'ятим виходом (z_5) дешифратора 46, вихід 25 логічного елемента АБО 50 є восьмим виходом (y_8) блока керування 13, перший вихід (z_1) дешифратора 46 є другим виходом 19 (y_2) блока керування 13, четвертий вихід (z_4) дешифратора 46 є п'ятим виходом 22 (y_5) блока керування 13, п'ятий вихід (z_5) дешифратора 46 є третім виходом 20 (y_3) блока керування 13, дев'ятий вихід (z_9) дешифратора 46 є сьомим виходом 24 (y_7) блока керування 13.

На Фіг.3 наведена функціональна схема порівняння кодів 10 призначена для порівняння (n-1)-розрядних чисел. Схема порівняння кодів 10 складається з n-1 логічного двовходового елемента І-НЕ (56.1-56.n-2, 57.n-1), одного логічного трьохвходового елемента І-НЕ (57.n-2), одного чотирьохвходового логічного елемента І-НЕ (57.n-3), ..., двох (n-1)-входових логічних елементів І-НЕ (57.2, 58) і одного n-входового логічного елемента І-НЕ (57.1). Вхід 53 є входом прямого коду проміжного результату, 53.і означає і-ий розряд коду з регістра 11 проміжного результату, вхід 52 є інверсним значенням коду модуля, 52.і означає і-ий розряд інверсного значення коду модуля, вхід 54 є входом прямого коду модуля, 54.і означає і-ий розряд значення коду модуля, вхід 55 є інверсним значенням коду з регістра 11 проміжного результату, 55.і означає і-ий розряд інверсного значення проміжного результату. Вихід 17 є виходом схеми порівняння кодів.

На Фіг.4 наведена змістова граф-схема алгоритма роботи суматора, яка містить вершини Початок і Кінець, операторні вершини (прямокутники) та умовні вершини (ромби). Розглянемо скорочені позначення, які використані на цій граф-схемі алгоритма: ОР - код операції, ADD - операція додавання, SUB - операція віднімання, $ВК_A$ - видача коду з регістра 4 першого операнда, $ВК_B$ - видача коду з регістра 5 другого операнда, $ВІК_B$ - видача інверсного коду з регістра 5 другого операнда, $ПК_C$ - прийом коду в регістр 11 проміжного результату, α - перша умова, β - друга умова, $ВК_P$ - видача коду з регістра 6, γ - третя умова, $ВІК_P$ - видача інверсного коду з регістра 6, "+1"- сигнал вхідного переносу комбінаційного суматора 9, $ВК_{Рез}$ - видача результату на вихід суматора за модулем простого числа.

На Фіг.5 наведена закодована граф-схема алгоритма роботи суматора, де сигнал $ВК_A$ позначено як y_1, $ВК_B$-y_2, $ВІК_B$-y_3, $ВК_P$-y_4, $ВІК_P$-y_5, $ПК_C$-y_6, $ВК_{Рез}$-y_7, "+1"-y_8, а операторні вершини позначено від z_0 до z_9 відповідно.

Суматор за модулем простого числа (Фіг.1) забезпечує виконання двох операцій:

- додавання (C=(A+B) mod P),
- віднімання (C=(A-B) mod P),

де A - перший операнд, B - другий операнд, C - результат операції, а P - модуль за яким працює суматор.

Розрядність регістрів та більшості шин дорівнює n+1, де n=]$\log_2$ P[, символ] [- округлення до найближчого більшого цілого числа.

A, B, C є елементами поля GF (P), тобто A, B, C $\in$ {0,1,2,..., P-1}.

Операцію віднімання C=(A-B) mod P реалізуємо як

C=(A+$B_{пр}$) mod P,

де $B_{пр}$ - елемент поля GF (P), протилежний до елемента B, $B_{пр}$=P-B. Зрозуміло, що B+$B_{пр}$=P.

Вираз $B_{пр}$=P-B реалізуємо як $B_{пр}$=P+$B_{доп}$, $B_{доп}$ - доповнення величини B до 2^n (доповняльний код величини B), тобто

$B_{пр} = P - B = P + \left(2^n - B\right) = P + \overline{B} + 1$, де $\overline{B}$ - інверсний код величини B.

$$\text{Тоді } C = (A - B) \bmod P = (A + P + \overline{B} + 1) \bmod P = (A + \overline{B} + 1) \bmod P.$$

Отже, величина C на виході суматора за модулем простого числа дорівнює

$$C = \begin{cases} (A + B) \bmod P, & \text{якщо } OP = 0; \\ (A + \overline{B} + 1) \bmod P, & \text{якщо } OP = 1. \end{cases}$$

Розглянемо докладніше призначення деяких функціональних вузлів суматора за модулем простого числа.

Регістр 4 першого операнда, регістр 5 другого операнда, регістр 6 коду модуля та регістр 11 проміжного результату призначені для зберігання відповідно вхідних операндів, значення модуля та проміжного і остаточного результату. Регістр 4 першого операнда, регістр 5 другого операнда та вхідний регістр 6 коду модуля є (n+1)-розрядними регістрами з асинхронним записом, синхронною видачею коду та виходами на три стани. Регістр проміжного результату 11 є (n+1)-розрядним регістром з синхронним записом, асинхронною видачею коду та виходами на три стани. Комбінаційний суматор 9 призначений для підсумовування двох двійкових операндів, які поступають відповідно з виходів першої 7 та другої 8 групи елементів АБО з урахуванням вхідного переносу 25. Розрядність вхідних та вихідних шин комбінаційного суматора 9 дорівнює n+1. Вихідні шини комбінаційного суматора 9 з'єднані з входами регістра 11 проміжного результату. Вихідні шини регістра 11 проміжного результату з першої до n+1 з'єднані з відповідними першими входами групи 7 елементів АБО, з першої до n-ої з'єднані з відповідними першими входами групи елементів І 26, а з першої до (n-1)-ої з'єднані з першими входами схеми порівняння кодів 10 (Фіг.3).

Схема порівняння кодів 10 (Фіг.3) призначена для порівняння n-1 молодших розрядів результату суми операндів C=A+B (яка з виходу регістра 11 проміжного результату поступає на перші входи

схеми порівняння кодів 10) з n-1 молодшими розрядами модуля, за яким працює суматор. На виході схеми порівняння кодів 10 (Фіг.3) з'являється сигнал, якщо n-1 молодших розрядів результату суми операндів менше за n-1 молодших розрядів модуля.

Відзначимо той факт, що, порівняно з прототипом [4], кількість входів схеми порівняння кодів 10 (Фіг.3) зменшена з n+1 до n-1, що дає змогу зменшити апаратні витрати на: два двовходових елемента І-НЕ, один (n+2)-входовий елемент І-НЕ і один (n+1)-входовий елемент І-НЕ, а також зменшити кількість входів одного елемента І-НЕ з n+1 до n-1. Це стає зрозумілим, якщо детальніше розглянути схему порівняння кодів 10.

У загальному випадку схема порівняння кодів реалізує такий вираз:

$$H_M(C,P) = \bar{c}_n p_n \bigvee_{i=n-1}^{1} \bar{c}_i p_i \,\&\, \bigwedge_{j=n}^{i+1} (\bar{c}_j \vee p_j).$$

Представимо цю формулу у вигляді придатному для схемотехнічної реалізації на елементах І-НЕ:

$$H_M(C,P) = \overline{\overline{\bar{c}_n p_n \bigvee_{i=n-1}^{1} \bar{c}_i p_i \,\&\, \bigwedge_{j=n}^{i+1} (\bar{c}_j \vee p_j)}} = \overline{\overline{\bar{c}_n p_n} \,\&\, \bigwedge_{i=n-1}^{1} \overline{\bar{c}_i p_i \,\&\, \bigwedge_{j=n}^{i+1} c_j \bar{p}_j}}.$$

Якщо взяти схему порівняння кодів для (n-1)-розрядних чисел (Фіг.3), то формула набуває вигляду:

$$H_M(C,P) = \overline{\overline{\bar{c}_{n-1} p_{n-1}} \,\&\, \bigwedge_{i=n-2}^{1} \overline{\bar{c}_i p_i \,\&\, \bigwedge_{j=n-1}^{i+1} c_j \bar{p}_j}}.$$

На Фіг.3 наведена схема порівняння кодів 10, призначена для порівняння двох двійкових (n-1)-розрядних чисел.

Блок керування 13 (Фіг.2) побудований, як автомат Мура. Процес синтезу блока керування 13 (Фіг.2) починається з побудови змістової (Фіг.4) та закодованої (Фіг.5) граф-схеми алгоритма роботи суматора за модулем простого числа.

По закодованій граф-схемі алгоритма (Фіг.5) будується структурна таблиця переходів автомата Мура (Таблиця).

Таблиця

Вихідний стан	Код вихідного стану				Керуючі сигнали	Стан переходу	Код стану переходу				Логічні умови				Функції збудження			
	$Q_3(t)$	$Q_2(t)$	$Q_1(t)$	$Q_0(t)$			$Q_3(t+1)$	$Q_2(t+1)$	$Q_1(t+1)$	$Q_0(t+1)$	OP	α	β	γ	D_3	D_2	D_1	D_0
z_0	0	0	0	0		z_1	0	0	0	1	0	*	*	*	0	0	0	1
						z_5	0	1	0	1	1	*	*	*	0	1	0	1
z_1	0	0	0	1	y_1, y_2	z_2	0	0	1	0	*	*	*	*	0	0	1	0
z_2	0	0	1	0	y_6	z_3	0	0	1	1	*	0	0	*	0	0	1	1
						z_4	0	1	0	0	*	1	*	*	0	1	0	0
						z_8	1	0	0	0	*	0	1	*	1	0	0	0
z_3	0	0	1	1	y_4	z_4	0	1	0	0	*	*	*	0	0	1	0	0
						z_8	1	0	0	0	*	*	*	1	1	0	0	0
z_4	0	1	0	0	y_5, y_8	z_8	1	0	0	0	*	*	*	*	1	0	0	0
z_5	0	1	0	1	y_1, y_3, y_8	z_6	0	1	1	0	*	*	*	*	0	1	1	0
z_6	0	1	1	0	y_6	z_7	0	1	1	1	*	1	*	*	0	1	1	1
						z_8	1	0	0	0	*	0	*	*	1	0	0	0
z_7	0	1	1	1	y_4	z_8	1	0	0	0	*	*	*	*	1	0	0	0
z_8	1	0	0	0	y_6	z_9	1	0	0	1	*	*	*	*	1	0	0	1
z_9	1	0	0	1	y_7	z_0	0	0	0	0	*	*	*	*	0	0	0	0

За побудованою структурною таблицею переходів автомата Мура визначаємо функції збудження D-тригерів:

$D_3 = z_2\bar{\alpha}\beta \vee z_3\gamma \vee z_6\bar{\alpha} \vee z_4 \vee z_7 \vee z_8;$

$D_2 = z_0 OP \vee z_2\alpha \vee z_3\bar{\gamma} \vee z_6\alpha \vee z_5;$

$D_1 = z_2\bar{\alpha}\bar{\beta} \vee z_6\alpha \vee z_1 \vee z_5;$

$D_0 = z_2\bar{\alpha}\bar{\beta} \vee z_6\alpha \vee z_0 \vee z_8.$

В залежності від станів автомата Мура функції виходів блока керування 13 набувають такого вигляду: $y_1=z_1\vee z_5$; $y_2=z_1$; $y_3=z_5$; $y_4=z_3\vee z_7$; $y_5=z_4$; $y_6=z_2\vee z_6\vee z_8$; $y_7=z_9$; $y_8=z_4\vee z_5$.

За наведеними функціями збудження D-тригерів та функціями виходів блока керування 13 легко будуємо функціональну схему блока керування 13. Вона наведена на Фіг.2.

Розглянемо як функціонує блок керування 13 (Фіг.2). Блок керування 13 спочатку знаходиться в стані z_0 (початковий стан), далі, в залежності від вхідних сигналів, за граф-схемою алгоритма (Фіг.4 та Фіг.5) він переходить з одного стану в інший і формує на своїх виходах відповідні сигнали керування. В кінці алгоритма блок керування 13 повертається в початковий стан z_0.

Розглянемо, як працює суматор за модулем простого числа. Логіка роботи суматора за модулем простого числа представлена змістовою (Фіг.4) та закодованою (Фіг.5) граф-схемою алгоритма роботи. Значення вхідних операндів та зна-

чення модуля надходять відповідно на шину 1 коду першого операнда, шину 2 коду другого операнда та шину 3 коду модуля. Регістр 4 першого операнда, регістр 5 другого операнда та регістр 6 модуля є регістрами з асинхронним записом, тому після надходження значень на шини вони будуть відразу записані у відповідні регістри. На вхід 14 блока керування 13 надходить значення коду операції (ОР).

Далі блок керування 13 аналізує код операції:

1. Якщо ОР=0, то треба виконувати операцію додавання двох операндів. Блок керування 13 формує сигнали 18 та 19 видачі прямого коду з регістра першого та другого операнда. Перший операнд через першу 7 групу елементів АБО надходить на перший вхід комбінаційного суматора 9, другий операнд через другу 8 групу елементів АБО надходить на другий вхід комбінаційного суматора 9. На комбінаційному суматорі 9 виконується підсумовування двійкових кодів, які присутні на першому та другому входах. З виходу комбінаційного суматора 9 результат потрапляє на вхід регістра 11 проміжного результату. Блок керування 13 формує сигнал 23 прийому коду в регістр 11 проміжного результату. Далі блок керування аналізує дві умови (α та β), де α дорівнює одиниці коли старший (n+1)-ий розряд регістра 11 проміжного результату дорівнює 1, а β дорівнює одиниці коли два старших, (n+1)-ий та n-й, розряди регістра 11 проміжного результату дорівнюють 0. Потім в залежності від значення умов α та β блок керування 13 формує певні сигнали, а саме:

- Якщо умова α дорівнює 0, а умова β дорівнює 1, то отримано результат, який не вимагає корекції, оскільки він менше за значення модуля. В цьому випадку блок керування 13 формує сигнал 24 відкривання групи елементів І 26, на другому вході яких знаходиться значення суми двох операндів. Через групу елементів І 26 результат потрапляє на вихід 27 суматора за модулем простого числа.

- Якщо умова α дорівнює 0 і умова β дорівнює 0, то без залучення схеми порівняння кодів 10 не можна визначити чи є отриманий результат меншим від значення модуля, тому блок керування 13 формує сигнал 21 видачі прямого коду з регістра 6 модуля. Перші n-1 розрядів значення модуля надходять на другий вхід схеми порівняння кодів 10, а на першому вході вже присутні перші n-1 розрядів отриманого результату. Далі схема порівняння кодів 10 формує на виході 17 значення третьої умови γ:

- Якщо γ=1, то це означає, що отриманий результат не вимагає корекції, оскільки він менше за значення модуля, тоді блок керування 13 формує сигнал 24 відкривання групи елементів І 26, на другому вході яких знаходиться значення суми двох операндів. Через групу елементів І 26 результат потрапляє на вихід 27 суматора за модулем простого числа.

- Якщо γ=0, то це означає, що отриманий результат вимагає корекції, оскільки він дорівнює або більше за значення модуля, тоді блок керування 13 формує сигнал 22 видачі інверсного коду з регістра 6 модуля і сигнал 25 вхідного переносу комбінаційного суматора 9. Проміжний результат з виходів регістра 11 проміжного результат через першу 7 групу елементів АБО надходить на перший вхід комбінаційного суматора 9, інверсний код модуля через другу 8 групу елементів АБО надходить на другий вхід комбінаційного суматора 9. На комбінаційному суматорі 9 виконується підсумовування двійкових кодів, які присутні на першому та другому входах з урахуванням вхідного переносу. З виходу комбінаційного суматора 9 результат потрапляє на вхід регістра 11 проміжного результату. Блок керування 13 формує сигнал 23 прийому коду в регістр 11 проміжного результату. Далі блок керування 13 формує сигнал 24 відкривання групи елементів І 26, на другому вході яких знаходиться значення суми двох операндів. З виходів групи елементів І 26 результат потрапляє на вихід 27 суматора за модулем простого числа.

- Якщо умова α дорівнює 1, то отримано результат, який вимагає корекції, оскільки він дорівнює або більше за значення модуля, тоді блок керування 13 формує сигнал 22 видачі інверсного коду з регістра 6 модуля і сигнал 25 вхідного переносу комбінаційного суматора 9. Проміжний результат з виходів регістра 11 проміжного результат через першу 7 групу елементів АБО надходить на перший вхід комбінаційного суматора 9, інверсний код модуля через другу 8 групу елементів АБО надходить на другий вхід комбінаційного суматора 9. На комбінаційному суматорі 9 виконується підсумовування двійкових кодів, які присутні на першому та другому входах з урахуванням вхідного переносу. З виходу комбінаційного суматора 9 результат потрапляє на вхід регістра 11 проміжного результату. Блок керування 13 формує сигнал 23 прийому коду в регістр 11 проміжного результату. Далі блок керування 13 формує сигнал 24 відкривання групи елементів І 26, на другому вході яких знаходиться значення суми двох операндів. З виходів групи елементів І 26 результат потрапляє на вихід 27 суматора за модулем простого числа.

2. Якщо ОР=1, то треба виконувати операцію віднімання двох операндів. Блок керування 13 формує сигнали 18 видачі прямого коду з регістра 4 першого операнда та сигнал 20 видачі інверсного коду з регістра 5 другого операнда, а також сигнал 25 вхідного переносу комбінаційного суматора 9. Перший операнд через першу 7 групу елементів АБО надходить на перший вхід комбінаційного суматора 9, другий операнд через другу 8 групу елементів АБО надходить на другий вхід комбінаційного суматора 9. На комбінаційному суматорі 9 виконується підсумовування двійкових кодів, які присутні на першому та другому входах з урахуванням вхідного переносу. З виходу комбінаційного суматора 9 результат потрапляє на вхід регістра 11 проміжного результату. Блок керування 13 формує сигнал 23 прийому кода в регістр 11 проміжного результату. Далі блок керування 13 аналізує значення умови α, де α дорівнює одиниці коли старший (n+1)-ий розряд регістра 11 проміжного результату дорівнює 1:

- Якщо умова α дорівнює 0, то отримано результат, який не вимагає корекції, оскільки він менше за значення модуля. Блок керування 13 фор-

мує сигнал 24 відкривання групи елементів І 26, на другому вході яких знаходиться значення суми двох операндів. Через групу елементів І 26 результат потрапляє на вихід 27 суматора за модулем простого числа.

- Якщо умова α дорівнює 1, то отримано результат, який вимагає корекції, оскільки значення першого операнда було менше за значення другого ми отримали "від'ємний" результат. Для корекції результату необхідно до нього додати значення модуля. Блок керування 13 формує сигнал 21 видачі прямого коду з регістра 6 модуля. Проміжний результат з виходів регістра 11 проміжного результату через першу 7 групу елементів АБО надходить на перший вхід комбінаційного суматора 9, прямий код модуля через другу 8 групу елементів АБО надходить на другий вхід комбінаційного суматора 9. На комбінаційному суматорі 9 виконується підсумовування двійкових кодів, які присутні на першому та другому входах. З виходу комбінаційного суматора 9 результат потрапляє на вхід регістра 11 проміжного результату. Блок керування 13 формує сигнал 23 прийому коду в регістр 11 проміжного результату. Далі блок керування 13 формує сигнал 24 відкривання групи елементів І 26, на другому вході яких знаходиться значення суми двох операндів. З виходів групи елементів І 26 результат потрапляє на вихід 27 суматора за модулем простого числа.

Наведемо приклади роботи суматора за модулем простого числа при виконанні операцій додавання та віднімання для модуля $P=19_{10}=10011_2$.

Приклад 1

Операція додавання. Сума операндів менша за Р та менша за 2^n.

Нехай $A=6_{10}=000110_2$, $B=7_{10}=000111_2$ (жирним позначено (n+1)-ий розряд регістрів першого та другого операндів, які беруть участь у визначенні знаку проміжного результату, чи є проміжний результат додатним чи від'ємним).

Вхідні операнди А=000110, В=000111 та значення модуля Р=010011 поступають відповідно через шину 1 коду першого операнда, шину 2 коду другого операнда та шину 3 коду модуля на регістр 4 першого операнда (регістр А), на регістр 5 другого операнда (регістр В) та на регістр 6 коду модуля (регістр Р). Код операції додавання ОР=0 поступає на відповідний вхід 14 блока керування 13. У відповідності до отриманого коду операції блок керування 13 формує сигнали 18 (y_1, $ВК_A$) та 19 (y_2, $ВК_B$) видачі прямого коду з регістра А та регістра В. Операнд А через першу 7 групу елементів АБО потрапляє на перший вхід комбінаційного суматора 9. Операнд В через другу 8 групу елементів АБО потрапляє на другий вхід комбінаційного суматора 9. На комбінаційному суматорі 9 виконується підсумовування операндів А=000110 та В=000111. З виходу комбінаційного суматора 9 результат суми С=001101 потрапляє на вхід регістра 11. Блок керування 13 видає сигнал 23 (y_6, $ПК_C$) прийому коду в регістр 11 проміжного результату і результат з виходів комбінаційного суматора 9 записується в регістр 11 проміжного результату. Далі значення п'ятого розряду (умова $\alpha=c_5=0$) регістра 11 проміжного результату поступає на відповідний вхід блока керування 13, а також на перший вхід логічного елемента АБО-НЕ 12, на другий вхід логічного елемента АБО-НЕ 12 поступає четвертий розряд ($c_4=0$) регістра 11 проміжного результату, на виході логічного елемента АБО-НЕ 12 отримуємо значення умови $\beta=\overline{0\vee 0}=1$, яке надходить на відповідний вхід блока керування 13. Аналізуючи умови α та β блок керування 13 формує сигнал 24 (y_7, $ВК_{Рез}$) відкривання "защіпки" 26 (групи елементів І) на другому вході якої знаходиться значення результату суми двох операндів. З виходів групи елементів І 26 результат потрапляє на вихід 27 суматора за модулем простого числа.

Приклад 2

Операція додавання. Сума операндів менша за Р, але більша за 2^n-1.

Нехай $A=8_{10}=001000_2$, $B=10_{10}=001010_2$.

Вхідні операнди А=001000, В=001010 та значення модуля Р=010011 поступають відповідно через шину 1 коду першого операнда, шину 2 коду другого операнда та шину 3 коду модуля на регістр 4 першого операнда (регістр А), на регістр 5 другого операнда (регістр В) та на регістр 6 коду модуля (регістр Р). Код операції додавання ОР=0 поступає на відповідний вхід блока керування 13. У відповідності до отриманого коду операції блок керування 13 формує сигнали 18 (y_1, $ВК_A$) та 19 (y_2, $ВК_B$) видачі прямого коду з регістра А та регістра В. Перший операнд через першу 7 групу елементів АБО потрапляє на перший вхід комбінаційного суматора 9. Другий операнд через другу 8 групу елементів АБО потрапляє на другий вхід комбінаційного суматора 9. На комбінаційному суматорі 9 виконується підсумовування операндів А=001000 та В=001010. З виходу комбінаційного суматора 9 результат суми С=010010 потрапляє на вхід регістра 11 проміжного результату. Блок керування 13 видає сигнал 23 (y_6, $ПК_C$) прийому коду в регістр 11 проміжного результату і результат з виходів комбінаційного суматора записується в регістр 11 проміжного результату. Далі значення п'ятого розряду (умова $\alpha=c_5=0$) регістра 11 проміжного результату поступає на відповідний вхід блока керування 13, а також на перший вхід логічного елемента АБО-НЕ 12, на другий вхід логічного елемента АБО-НЕ 12 поступає значення четвертого розряду ($c_4=1$) регістра 11 проміжного результату, на виході логічного елемента АБО-НЕ 12 отримуємо значення умови $\beta=\overline{0\vee 1}=0$, яке надходить на відповідний вхід блока керування 13. Аналізуючи умови α та β блок керування 13 формує сигнал 21 (y_4, $ВК_P$) видачі прямого коду з регістра Р. На схемі порівняння кодів 10 виконується порівняння чотирьох молодших розрядів результату суми операндів та модуля Р. Схема порівняння кодів 10 формує значення третьої умови у, яке дорівнює 1, тобто перший операнд (значення суми) менше другого операнда (значення модуля Р). Значення третьої умови у надходить відповідно на четвертий вхід блока керування 13. Отримавши на четвертий вхід одиничне значення третьої умови блок керування 13 формує сигнал 24 (y_7, $ВК_{Рез}$) відкривання "защіпки" 26 (групи елементів І) на другому

вході якої знаходиться значення результату суми двох операндів. З виходів групи елементів І 26 результат потрапляє на вихід 27 суматора за модулем простого числа.

Приклад 3

Операція додавання. Сума операндів більша за Р, але менша за 2^{n+1}.

Нехай $A=15_{10}=001111_2$, $B=9_{10}=001001_2$.

Вхідні операнди А=001111, В=001001 та значення модуля Р=010011 поступають відповідно через шину 1 коду першого операнда, шину 2 коду другого операнда та шину 3 коду модуля на регістр 4 першого операнда (регістр А), на регістр 5 другого операнда (регістр В) та на регістр 6 коду модуля (регістр Р). Код операції додавання ОР=0 поступає на вхід 14 блока керування 13. У відповідності до отриманого коду операції блок керування 13 формує сигнали 18 (y_1, $ВК_A$) та 19 (y_2, $ВК_B$) видачі прямого коду з регістра А та регістра В. Операнд А через першу 7 групу елементів АБО потрапляє на перший вхід комбінаційного суматора 9. Операнд В через другу 8 групу елементів АБО потрапляє на другий вхід комбінаційного суматора 9. На комбінаційному суматорі 9 виконується підсумовування операндів А=001111 та В=001001. З виходу комбінаційного суматора 9 результат суми С=011000 потрапляє на вхід регістра 11 проміжного результату. Блок керування 13 видає сигнал 23 (y_6, $ПК_C$) прийому кода в регістр 11 проміжного результату і результат з виходів комбінаційного суматора 9 записується в регістр 11 проміжного результату. Далі значення п'ятого розряду (умова $\alpha=c_5=0$) регістра 11 проміжного результату поступає відповідний на вхід блока керування 13, а також на перший вхід логічного елемента АБО-НЕ 12, на другий вхід логічного елемента АБО-НЕ 12 поступає значення четвертого розряду ($c_4=1$) регістра 11 проміжного результату, на виході логічного елемента АБО-НЕ 12 отримуємо значення умови $\beta=\overline{0\vee 1}=0$, яке надходить на відповідний вхід блока керування 13. Аналізуючи умови α та β блок керування 13 формує сигнал 21 (y_4, $ВК_Р$) видачі прямого коду з регістра Р. На схемі порівняння кодів 10 виконується порівняння чотирьох молодших розрядів результату суми операндів та модуля. Схема порівняння кодів 10 формує значення третьої умовну, яке дорівнює 0, тобто перший операнд (значення суми) більше або дорівнює другому операнду (значення модуля). Отримавши на четвертий вхід нульове значення третьої умови у блок керування 13 формує сигнал 22 (y_5, $ВІК_Р$) видачі інверсного коду з регістра 6 модуля та сигнал 25 (y_8, +1), який є вхідним переносом для комбінаційного суматора 9. Далі виконується підсумовування першого операнда (отримане значення суми С=011000) та другого операнда (проінвертоване значення модуля $\overline{P}=101100$) з урахуванням одиничного вхідного переносу. На виході комбінаційного суматора 9 отримуємо результат С=000101. Далі блок керування 13 видає сигнал 23 (y_6, $ПК_C$) прийому коду в регістр 11 проміжного результату і результат з виходів комбінаційного суматор 9 записується в регістр 11 проміжного результату. В наступному такті формується сигнал 24 (y_7, $ВК_{Рез}$) відкривання "защіпки" 26 (групи елементів І) на другому вході якої знаходиться значення результату суми двох операндів. З виходів групи елементів І 26 результат потрапляє на вихід 27 суматора за модулем простого числа.

Аналогічно буде виконуватись операція, коли сума двох вхідних операндів буде дорівнювати значенню модуля.

Приклад 4

Операція додавання. Сума операндів більша за Р і більша за 2^{n+1}-1.

Нехай $A=17_{10}=010001_2$, $B=18_{10}=010010_2$.

Вхідні операнди А=010001, В=010010 та значення модуля Р=010011 поступають відповідно через шину 1 коду першого операнда, шину 2 коду другого операнда та шину 3 коду модуля на регістр 4 першого операнда (регістр А), на регістр 5 другого операнда (регістр В) та на регістр 6 коду модуля (регістр Р). Код операції додавання ОР=0 поступає на вхід 14 блока керування 13. У відповідності до отриманого коду операції блок керування 13 формує сигнали 18 (y_1, $ВК_A$) та 19 (y_2, $ВК_B$) видачі прямого коду з регістра А та регістра В. Операнд А через першу 7 групу елементів АБО потрапляє на перший вхід комбінаційного суматора 9. Операнд В через другу 8 групу елементів АБО потрапляє на другий вхід комбінаційного суматора 9. На комбінаційному суматорі 9 виконується підсумовування операндів А=010001 та В=010010. З виходу комбінаційного суматора 9 результат суми С=100011 потрапляє на вхід регістра 11 проміжного результату. Блок керування 13 видає сигнал 23 (y_6, $ПК_C$) прийому коду в регістр 11 проміжного результату і результат з виходів комбінаційного суматора 9 записується в регістр 11 проміжного результату. Далі значення п'ятого розряду (умова $\alpha=c_5=1$) регістра 11 проміжного результату поступає на відповідний вхід блока керування 13. Отримавши одиничне значення умови а блок керування 13 формує сигнал 22 (y_5, $ВІК_Р$) для видачі інверсного коду з регістра Р та сигнал 25 (y_8, +1), який є вхідним переносом для комбінаційного суматора 9. Далі виконується підсумовування першого операнда (отримане значення суми С=100011) та другого операнда (проінвертоване значення модуля $\overline{P}=101100$) з урахуванням вхідного переносу. На виході комбінаційного суматора 9 отримуємо наступний результат С=010000. Далі блок керування 13 видає сигнал 23 (y_6, $ПК_C$) прийому кода в регістр 11 проміжного результату і результат з виходів комбінаційного суматор 9 записується в регістр 11 проміжного результату. В наступному такті формується сигнал 24 (y_7, $ВК_{Рез}$) відкривання "защіпки" 26 (групи елементів І) на другому вході якої знаходиться значення результату суми двох операндів. З виходів групи елементів І 26 результат потрапляє на вихід 27 суматора за модулем простого числа.

Приклад 5

Операція віднімання. Перший операнд більше за другий.

Нехай $A=10_{10}=001010_2$, $B=8_{10}=001000_2$.

Вхідні операнди А=001010, В=001000 та значення модуля Р=010011 поступають відповідно через шину 1 коду першого операнда, шину 2 коду

другого операнда та шину 3 коду модуля на регістр 4 першого операнда (регістр А), на регістр 5 другого операнда (регістр В) та на регістр 6 коду модуля (регістр Р). Код операції віднімання ОР=1 поступає на відповідний вхід блока керування 13. У відповідності до отриманого коду операції блок керування 13 формує сигнали 18 (y_1, $ВК_A$) та 20 (y_3, $ВІК_B$) видачі прямого кода з регістра А та інверсного з регістра В і формує сигнал 25 (y_8, +1), який є вхідним переносом для комбінаційного суматора 9. Операнд А через першу 7 групу елементів АБО потрапляє на перший вхід комбінаційного суматора 9. Проінвертований операнд В через другу 8 групу елементів АБО потрапляє на другий вхід комбінаційного суматора 9. На комбінаційному суматорі 9 виконується підсумовування операндів А=001010 та $\overline{B}=110111$ з урахуванням вхідного переносу. З виходу комбінаційного суматора 9 результат суми С=000010 потрапляє на вхід регістра 11 проміжного результату. Блок керування 13 видає сигнал 23 (y_6, $ПК_C$) прийому коду в регістр 11 проміжного результату і результат з виходів комбінаційного суматора 9 записується в регістр 11 проміжного результату. Далі значення п'ятого розряду (умова $\alpha=c_5=0$) регістра 11 проміжного результату поступає на вхід блока керування 13. Аналізуючи умову α блок керування 13 формує сигнал 24 (y_7, $ВК_{Рез}$) відкривання "защіпки" 26 (групи елементів І) на другому вході якої знаходиться значення результату суми двох операндів. З виходів групи елементів І 26 результат потрапляє на вихід 27 суматора за модулем простого числа.

Приклад 6

Операція віднімання. Перший операнд менший за другий.

Нехай $A=12_{10}=001100_2$, $B=15_{10}=001111_2$.

Вхідні операнди А=001100, В=001111 та значення модуля Р=010011 поступають відповідно через шину 1 коду першого операнда, шину 2 коду другого операнда та шину 3 коду модуля на регістр 4 першого операнда (регістр А), на регістр 5 другого операнда (регістр В) та на регістр 6 коду модуля (регістр Р). Код операції віднімання ОР=1 поступає на вхід 14 блока керування 13. У відповідності до отриманого коду операції блок керування 13 формує сигнали 18 (y_1, $ВК_A$) та 20 (y_3, $ВІК_B$) видачі прямого коду з регістра А та інверсного з регістра В і формує сигнал 25 (y_8, +1), який є вхідним переносом для комбінаційного суматора 9. Операнд А через першу 7 групу елементів АБО потрапляє на перший вхід комбінаційного суматора 9. Проінвертований операнд В через другу 8 групу елементів АБО потрапляє на другий вхід комбінаційного суматора 9. На комбінаційному суматорі 9 виконується підсумовування операндів А=001100 та В=110000 з урахуванням вхідного переносу. З виходу комбінаційного суматора 9 результат суми С=111101 потрапляє на вхід регістра 11 проміжного результату. Блок керування 13 видає сигнал 23 (y_6, $ПК_C$) прийому коду в регістр 11 проміжного результату і результат з виходів комбінаційного суматора 9 записується в регістр 11 проміжного результату. Далі значення п'ятого розряду (умова $\alpha=c_5=1$) регістра 11 проміжного результату поступає на відповідний вхід блока керування 13. Аналізуючи умову а блок керування 13 формує сигнал 21 (y_4, $ВК_P$) видачі прямого коду з регістра Р. На комбінаційному суматорі 9 відбувається підсумовування першого операнда (отриманий результат С=111101) та значення модуля, яке дорівнює 010011. На виході комбінаційного суматора 9 отримуємо результат С=010000. Далі блок керування 13 видає сигнал 23 (y_6, $ПК_C$) прийому коду в регістр 11 проміжного результату і результат з виходів комбінаційного суматора 9 записується в регістр 11 проміжного результату. В наступному такті формується сигнал 24 (y_7, $ВК_{Рез}$) відкривання "защіпки" 26 (групи елементів І) на другому вході якої знаходиться значення результату суми двох операндів. З виходів групи елементів І 26 результат потрапляє на вихід 27 суматора за модулем простого числа.

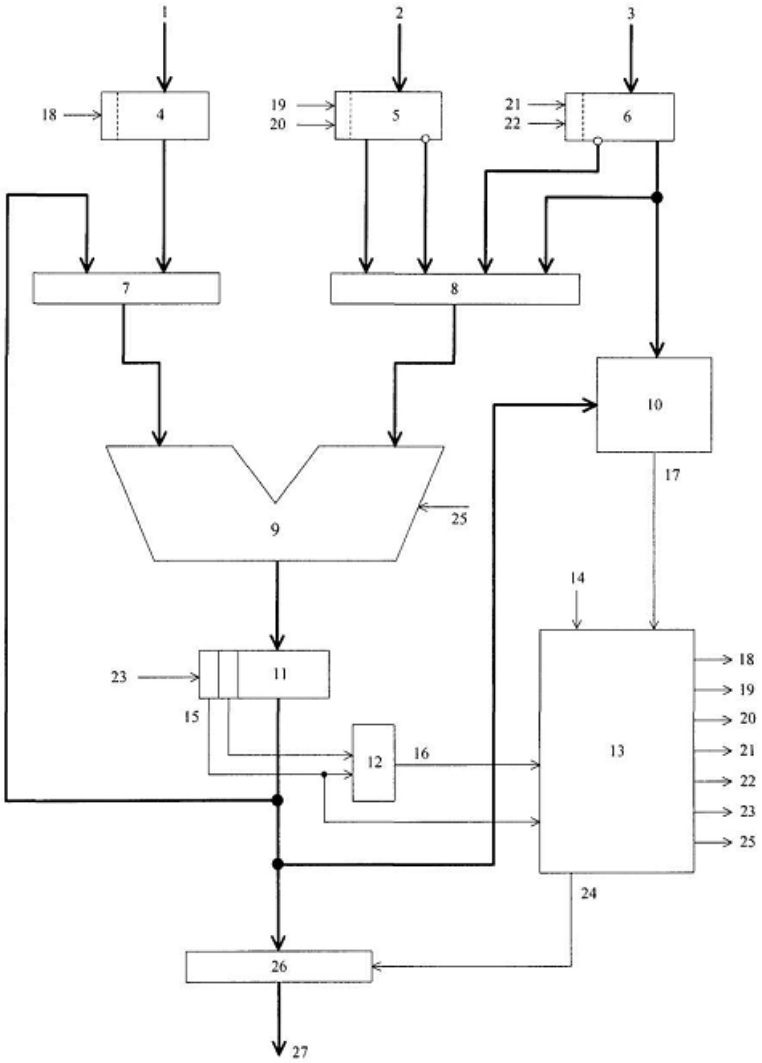
Джерела інформації:

1. Україна, Патент № 42437, МПК G06F7/50; Заявники Кошман Сергій Олександрович; Барсов Валерій Ігорович; Сіора Олександр Андрійович; Краснобаев Віктор Анатолійович; № u200814704, Дата подачі 22.12.2008; Дата публ. 10.07.2009, бюл. № 13, 2009р.; Пристрій для підсумовування в модулярній системі числення за модулем три.

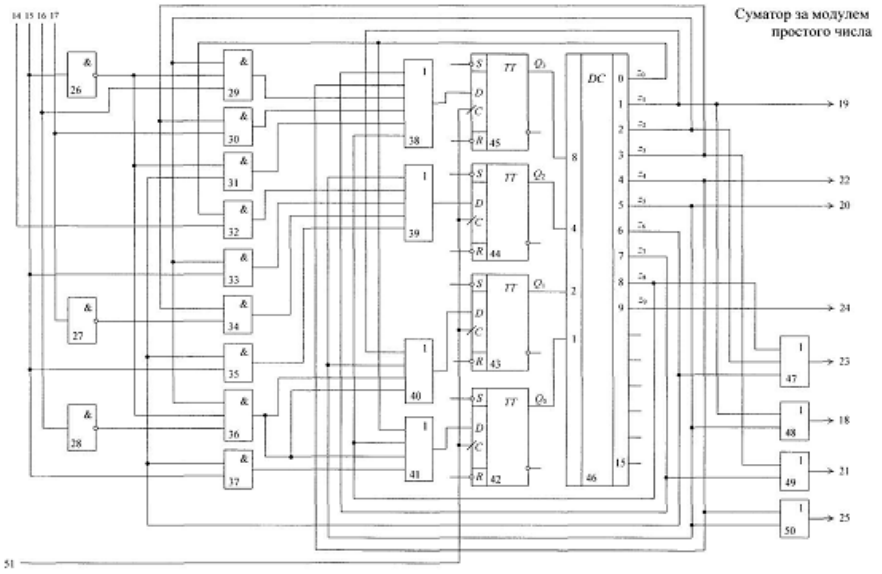
2. СССР, Авторское свидетельство № 1566342, МПК G06F 7/49; Изобретатель О.Н. Музыченко; №4487196/24-24, Дата подачи 28.09.1988; Дата публ. 23.05.1990, Бюл. № 19; Сумматор по модулю пять.

3. Россия, Патент № 2032934, МПКG06F7/49; Заявители Петренко Вячеслав Иванович, Чипига Александр Федорович; № 5040687/24, Дата подачи 30.04.1992; Дата публ. 10.04.1995; Сумматор по модулю Р.

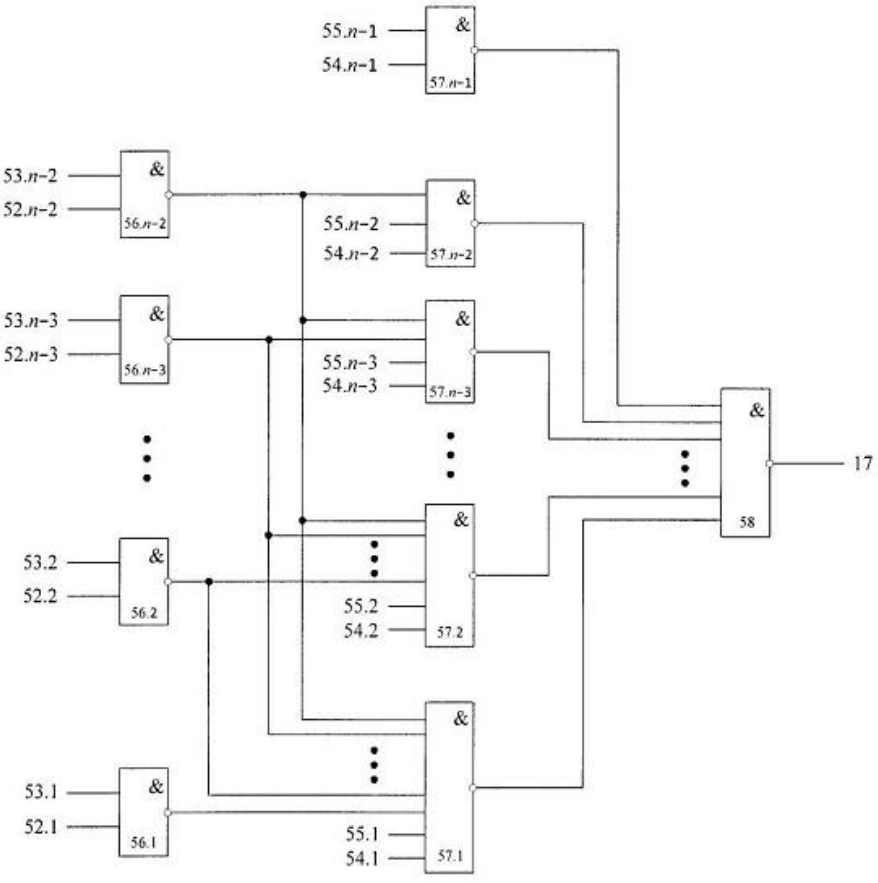
4. Україна, Патент № 86637, МПК G06F7/50; Заявники Фурман Ілля Олександрович; Кошман Сергій Олександрович; Деренько Микола Семенович; Краснобаев Віктор Анатолійович; № a200701744, Дата подачі 19.02.2007; Дата публ. 12.05.2009, бюл. № 9; Суматор по модулю m системи залишкових класів.


1
2
3
18
4
19
20
5
21
22
6
7
8
10
17
9
25
14
23
11
15
12
16
13
18
19
20
21
22
23
25
24
26
27

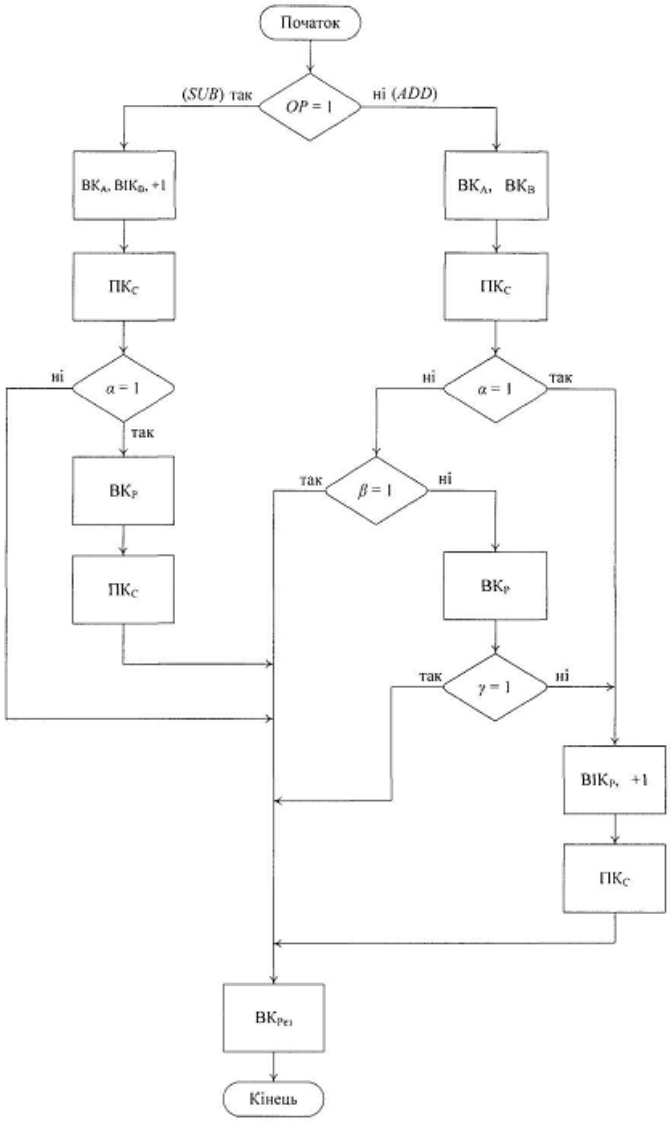
Фіг. 1


Суматор за модулем
простого числа
14 15 16 17
51
19
22
20
24
23
18
21
25

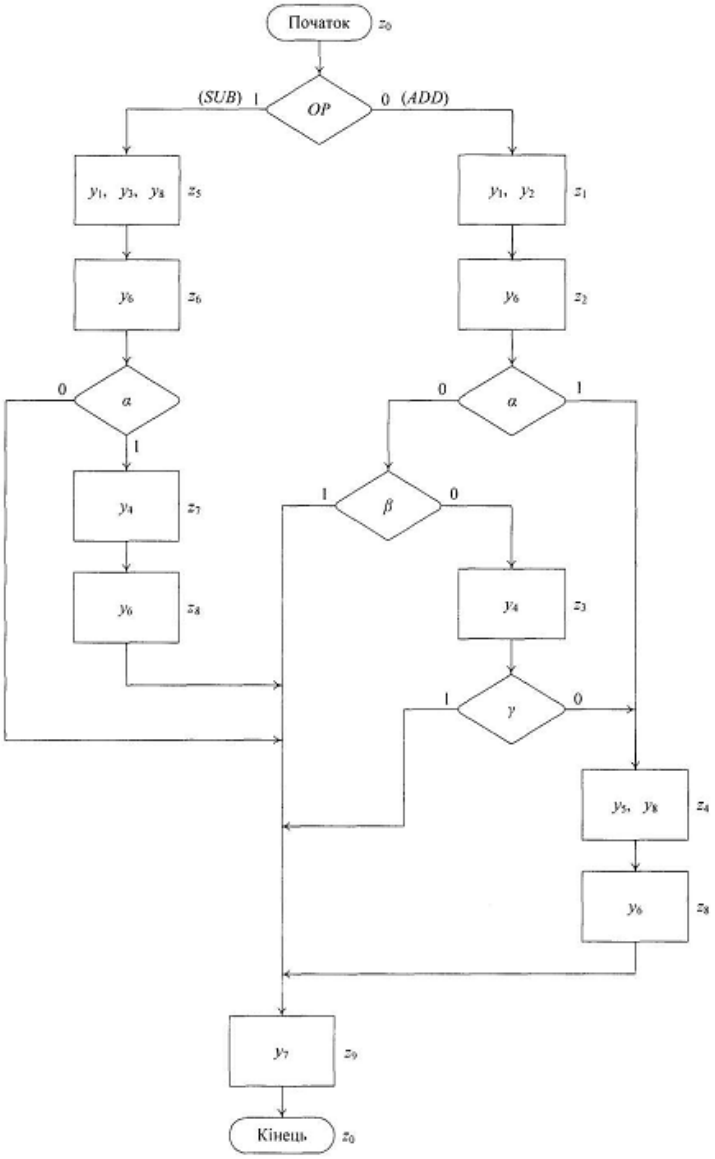
Фіг. 2


55.n−1
54.n−1
57.n−1
53.n−2
52.n−2
56.n−2
55.n−2
54.n−2
57.n−2
53.n−3
52.n−3
56.n−3
55.n−3
54.n−3
57.n−3
53.2
52.2
56.2
55.2
54.2
57.2
53.1
52.1
56.1
55.1
54.1
57.1
58
17

Фіг. 3


Початок
(SUB) так
OP = 1
ні (ADD)
ВКА, ВІКВ, +1
ВКА, ВКВ
ПКС
ПКС
ні
α = 1
так
ні
α = 1
так
ВКР
так
β = 1
ні
ПКС
ВКР
так
γ = 1
ні
ВІКР, +1
ПКС
ВКРез
Кінець

Фіг. 4



Фіг. 5

Комп'ютерна верстка Л. Ціхановська Підписне Тираж 26 прим.

Міністерство освіти і науки України

Державний департамент інтелектуальної власності, вул. Урицького, 45, м. Київ, МСП, 03680, Україна

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