УДК 681.1

МЕТОД ЗБЕРІГАННЯ ВЕЛИКИХ ПРОСТИХ ЧИСЕЛ У ДВІЙКОВІЙ СИСТЕМІ ЧИСЛЕННЯ

Івасьєв С.В.[1)], Неміш В.М.[2)], Шулак Р.В.[3)]
Тернопільський національний економічний університет
[1)] к.т.н., викладач, [2)]к.ф.-м.н., доцент, [3)] магістрант

I. Постановка задачі

Реалізація алгоритмів опрацювання великих простих чисел в задачах вибору системи взаємно простих модулів системи залишкових класів [1], пошуку найбільшого спільного дільника, виявлення квадратичного лишку, виконання арифметичних операцій модульної арифметики породжує необхідність зберігання та генерування значної кількості великих простих чисел [2]. Генерування та зберігання останніх, представлених повнорозрядними двійковими кодами, є неефективним у зв'язку з тим, що потребує великих об'ємів пам'яті.

II. Мета роботи

Мета роботи полягає в розробці методу зберігання великих простих чисел, який ґрунтується на записі розрядів числа та їх двійкового представлення, що дозволяє зменшити в кілька разів обсяг необхідної пам'яті.

III. Метод зберігання великихпростих чисел у двійковій системі числення

Для збереження цілого числа в двійковій системі числення потрібно використати всю послідовність байтів в його записі. Після проведених досліджень та аналізу простих чисел отримано такі результати: числа з однаковими молодшими бітами можна представити у вигляді трьох частин. Величини кожної з них залежать від розрядності простого числа та кількості бітів у закінченні. Обраний варіант розбиття ефективний для послідовності до 32 розрядів, для зберігання чисел розрядністю 512-1024 біт необхідно використати по два байти на число [3].

На рисунку 1 зображена схема порозрядного розбиття на групи послідовності великих простих чисел, яка є адаптивною і дозволяє вибрати довільне двійкове закінчення згенерованої двійкової послідовності великих простих чисел.

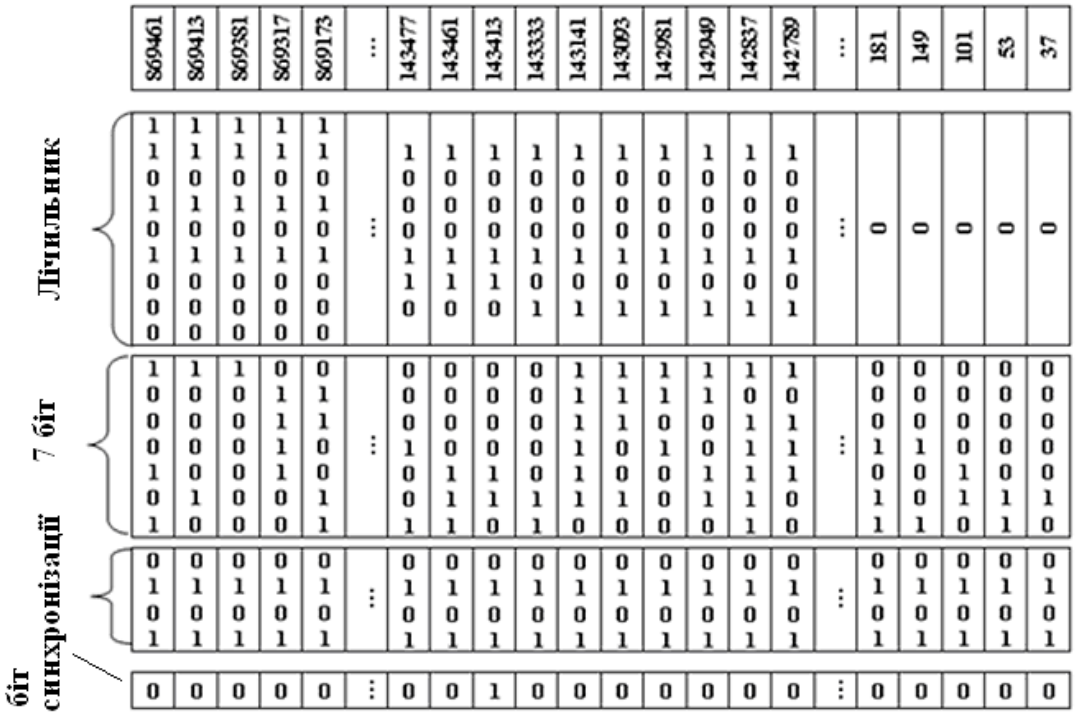


Рисунок 1 – Схема розбиття числа на групи розрядів

При обчисленні простих чисел створюється декілька потоків, що пришвидшує процес обчислення. У файл записується 7-бітний код та біт синхронізації, який фіксує збільшення значення

лічильника на 1. Таким чином, метод дозволяє уникнути зберігання надлишкового двійкового коду, зберігаючи лише 1 байт інформації для кожного числа. При декодуванні підраховується кількість бітів синхронізації і їх сума утворює верхню частину числа. Конкатенація отриманої суми, семи бітів та обраних нижніх розрядів для вибірки з послідовності простих чисел утворює код простого числа.

Алгоритм зберігання великих простих чисел наведено у блок-схемі на рисунку 2.

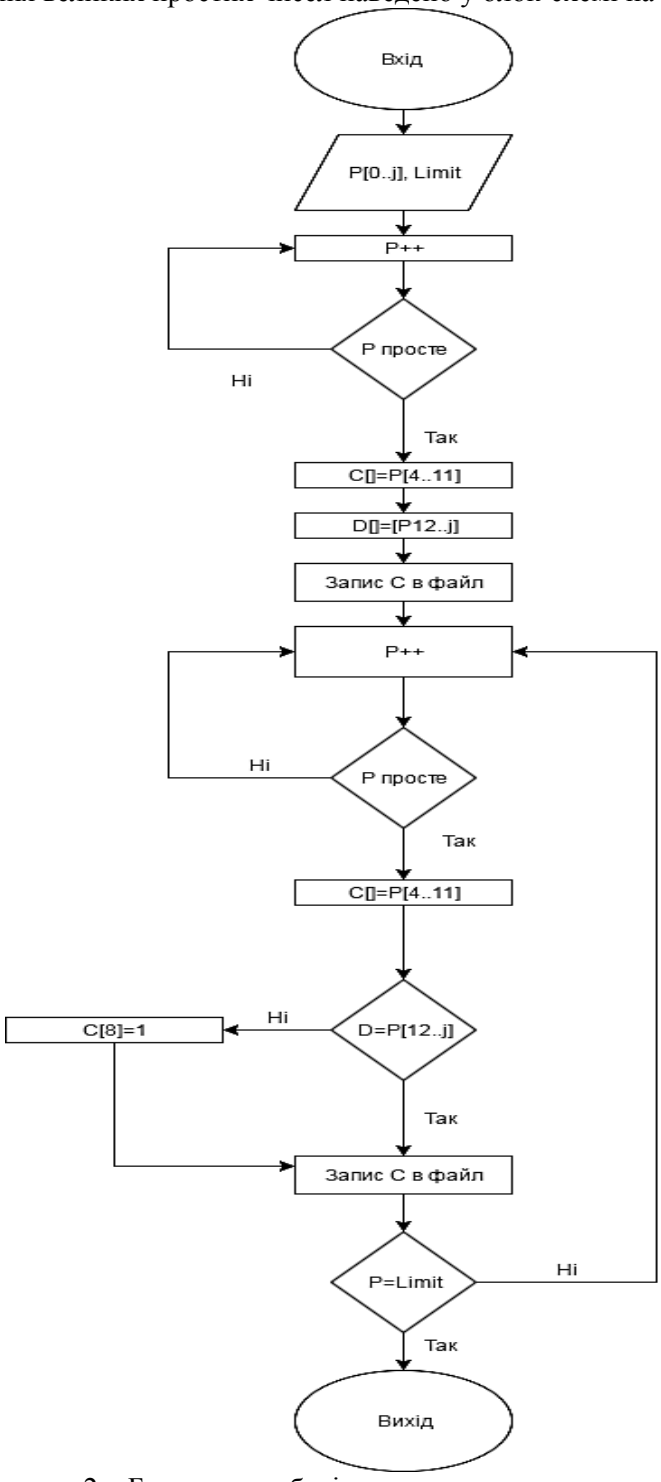


Рисунок 2 – Блок-схема зберігання великих простих чисел

Попередній аналіз методу кодування великих простих чисел показує, що, у порівнянні з відомими алгоритмами у двійковій системі числення, він характеризуються лінійно-логарифмічною обчислювальною складністю [3]. Дослідження показали, що ефективність методу зберігання великих простих чисел зростає у відповідності із збільшенням розрядності чисел.

Висновок

Проаналізувавши метод зберігання великих простих чисел у двійковій системі числення, виявлено, що у порівнянні з відомими алгоритмами він вимагає менше обчислювальних ресурсів, а

також дозволяє в декілька разів зменшити число пам'яті для зберігання великого простого числа, оскільки для запису, наприклад, 16-бітного числа використовується лише його семибітне закінчення та біт синхронізації.

Список використаних джерел

1. M. Kasianchuk. Theoretical Foundations of the Modified Perfect form of Residue Number System / M. Kasianchuk, Ya. M. Nykolaychuk, , I. Z. Yakymenko // Cybernetics and Systems Analysis. – March, 2016. -Volume 52, Issue 2. – pp.219-223.
2. Karpinski M. Advanced method of factorization of multi-bit numbers based on Fermat's theorem in the system of residual classes / M. Karpiński, S. Ivasiev, I. Yakymenko, M. Kasianchuk ,T. Gancarczyk// Proc. of 16th International Conference on Control, Automation and Systems (ICCAS–2016) – Gyeongju, Korea. – V.1. – October, 2016. – P.1484–1486.
3. Николайчук Я.М. Метод збереження простих великорозрядних чисел у базисі Радемахера / Я.М. Николайчук, І.З. Якименко, М.М. Касянчук, С.В. Івасьєв // Праці міжнародної молодіжної математичної школи "Питання оптимізації обчислень (ПОО-XXXVII)". Київ: Інститут кібернетики імені В.М. Глушкова НАН України. - 2015. –С. 159-161.

УДК 681.3

МЕТОДИ ВИКОНАННЯ АРИФМЕТИЧНИХ ОПЕРЦІЙ СИСТЕМИ ЗАЛИШКОВИХ КЛАСІВ

Івасьєв С.В.[1)], Паздрій І.Р.[2)], Петелько В.В. [3)]

Тернопільський національний економічний університет

[1)] к.т.н.; [2)] к.т.н., доцент; [3)] магістрант

I. Постановка проблеми

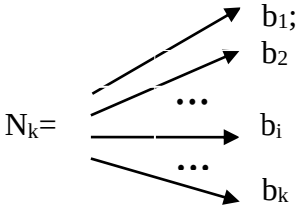
З огляду на сучасний рівень розвитку обчислювальних засобів використання непозиційних систем числення дозволяє збільшити надійність та швидкість цифрової обробки даних. Сучасні обчислювальні потужності дозволяють розв'язувати задачі оптимального вибору модулів системи та розрахунку відповідних вагових коефіцієнтів та базисних чисел, що відкриває нові можливості застосування непозиційних систем числення, в яких можлива реалізація розпаралелення процесу виконання арифметичних операцій. Однією з них є система залишкових класів (СЗК) [1-3].

II. Мета роботи

Метою роботи є дослідження методів виконання арифметичних операцій в СЗК. До недоліків існуючих рішень відносять труднощі під час виконання немодульних операцій, зокрема, порівняння чисел, ділення, визначення знаку числа, оцінка виходу результату за допустимий діапазон тощо.

III. Арифметичні операції в системі залишкових класів

В основу цілочисельного перетворення СЗК покладена Китайська теорема про залишки, згідно якої будь-яке ціле число можна однозначно перетворити набором найменших невід'ємних залишків в системі взаємно простих модулів за схемою, представленою на рисунку, та відповідною її формулою:



$$b_i = res\ N_k (mod\ p_i), \quad (1)$$

що відповідає рішенню діофантового рівняння:

$$N_k = b_i (\mathrm{mod}\ p_i) \quad (2)$$

або цілочисельному рішенню лінійного рівняння:

$$N_k = a_i p_i + b_i, \quad (3)$$

де a_i – ранг; b_i – найменший невід'ємний залишок.

При цьому діапазон кодування чисел N_k: