УДК 681.32

Н.Г. Гавришків[1], О.І. Карпюк[2]

[1]Галицький коледж ім. В. Чорновола

[2]Тернопільський національний економічний університет

ДОСЛІДЖЕННЯ МІЖБАЗИСНИХ ПЕРЕХОДІВ З СИСТЕМИ ЧИСЛЕННЯ ЗАЛИШКОВИХ КЛАСІВ В ДВІЙКОВУ

Вступ. Відновлення десяткового числа по його залишках є важливим результатом для сучасної алгебри і теорії чисел [1]. Така взаємно однозначна відповідність на практиці дозволяє працювати не з багаторозрядними числами, а з наборами залишків, які є менші від вибраних основ або модулів системи [2]. Крім того, обчислення можна виконувати паралельно по кожному залишку [3]. Дані властивості лежать в основі побудови системи числення залишкових класів, яка дозволяє підвищити швидкодію обчислювальних систем за рахунок розпаралелення процесу виконання арифметичних операцій [4], здійснювати контроль за помилками в задачах завадозахищеного кодування, визначати цілочисельні корені рівняння на основі принципу Хассе , виконувати швидке перетворення Фур'є на основі простих чисел тощо. Система залишкових класів має безліч застосувань в сучасних криптографічних алгоритмах, наприклад, в шифрах Віженера та Рабіна. В криптосистемі RSA шукаються залишки від ділення на велике число, яке є добутком двох простих чисел. Відповідно, обчислення можна здійснювати за модулем цих простих множників, які мають вдвічі меншу бітову довжину. Тому розробка методів та алгоритмів, які дозволяють зменшити часову складність при відновленні десяткового числа за його залишками є на даний час актуальною задачею.

Метою роботи є дослідження міжбазисних переходів з системи числення залишкових класів в двійкову.

Дослідження існуючих алгоритмів для між базисних перетворень

Теоретичною основою при відновленні десяткового числа за його залишками є алгебра і теорія чисел [4], зокрема китайська теорема про залишки (КТЗ). Будь-яке ціле невід'ємне десяткове число N можна представити у вигляді залишків b_i від ділення на натуральні попарно взаємно прості числа p_i, які називаються модулями:

$$b_i = N \bmod p_i. \qquad (1)$$

При виконанні умови $N < P = \prod_{i=1}^{k} p_i$, де k - кількість модулів, згідно КТЗ число N можна однозначно відновити за такою формулою:

$$N = \left(\sum_{i=1}^{k} m_i P_i b_i \right) \bmod P, \qquad (2)$$

де $P_i = \frac{P}{p_i}$, $m_i = P_i^{-1} \bmod p_i$.

На рисунку 1 приведено схему роботи для між базисного переходу запропоновану в [4].

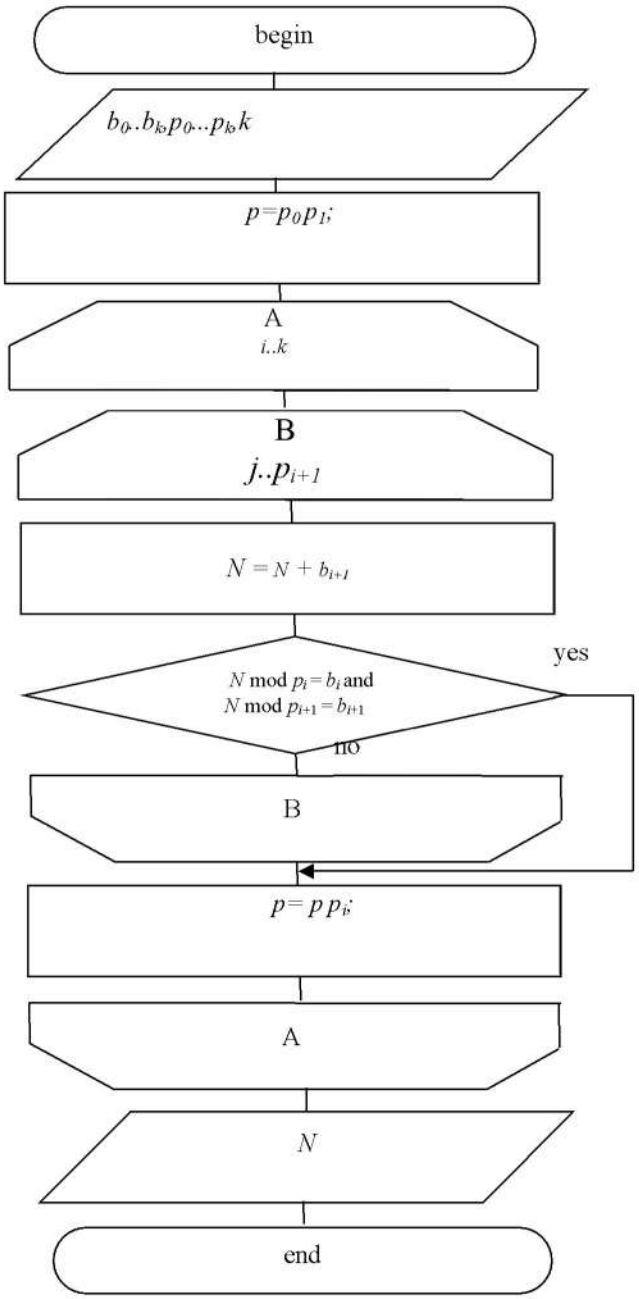

Рисунок 1 - Схема роботи алгоритму переходу з СЗК в позиційну систему числення

Ще одним способом відновлення десяткового числа по його залишках є алгоритм Гарнера, згідно якого

$$N = n_0 + n_1 p_1 + n_2 p_1 p_2 + \ldots + n_{n-1} p_1 p_2 \ldots p_{i-1}, \quad (3)$$

де $0 \le n_i < p_{i+1}$, $i=0, 1, \ldots, k-1$,

$$n_i = \frac{b_{i+1} - \left(n_0 + n_1 p_1 + \ldots + n_{i-1} p_1 p_2 \ldots p_{i-1}\right)}{p_1 p_2 \ldots p_i} \bmod p_{i+1}. \quad (4)$$

Таким чином, коефіцієнти n_i можуть бути один за одним послідовно обчислені на основі рекурентної формули (4). Крім того, алгоритм Гарнера придатний для аналогічних операцій з поліномами.

Недоліками розглянутих вище методів відновлення десяткового числа по його залишках є неможливість їх розпаралелення (або строго послідовна структура), виконання операцій над багаторозрядними числами (зокрема, обчислення залишку за модулем P), та необхідність пошуку мультиплікативного оберненого елемента за модулем.

Для знаходження останнього найбільш поширеними є методи перебору всіх можливих варіантів, за допомогою розширеного алгоритму Евкліда, на основі функції Ейлера. Всі вони характеризуються значною обчислювальною складністю. Подібним чином можна обчислювати і коефіцієнти n_i в алгоритмі Гарнера.

Висновки.

В роботі розроблено алгоритм відновлення десяткового числа за його залишками на основі додавання добутку модулів з можливістю розпаралелення обчислень та уникнення процедури пошуку мультиплікативного оберненого елемента. При цьому результати проміжних обчислень не будуть виходити за межі встановленого діапазону, що усуває необхідність виконання операції знаходження залишку за модулем P.

Перелік джерел.

1. S. Lang, Algebra. 3rd ed. New York: Springer-Verlag; 2002.

2. A. Omondi, B. Premkumar, "Residue Number System: Theory and Implementation". Imperial College Press, 2007, 296 p.

3. P.V. Ananda Mohan, "Residue number systems: algorithms and architectures", Springer Science+Business Media, NewYork, LLC, 2002, 378 p.

4. М. Касянчук, І. Якименко, С. Івасьєв, Н. Стефурак, Методи відновлення десяткового числа за його залишками на основі операції додавання, ITSec: Безпека інформаційних технологій: IX міжнародна науково-технічна конференція, 22-27 березня 2019 р. – К.: НАУ, 2019. – С.38-40