Методи відновлення десяткового числа за його залишками на основі операції додавання

УДК 519.6

Михайло Касянчук[1], Ігор Якименко[2], Степан Івасьєв[3], Наталя Стефурак[4]

Тернопільський національний економічний університет, [1]kasyanchuk@ukr.net, [2]iyakymenko@ukr.net,[3]stepan.ivasiev@gmail.com

Галицький коледж ім. В. Чорновола, [4]nat.stefurak@gmail.com

Відновлення десяткового числа по його залишках є важливим результатом для сучасної алгебри і теорії чисел. 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. Крім того, обчислення можна виконувати паралельно по кожному залишку. Дана система 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.

Відомо, що 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:

$$b_i = N \bmod p_i \quad . \tag{1}$$

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

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

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

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

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

де $0 \le n_i < p_{i+1}$, $n_i = \frac{b_{i+1} - \left(n_0 + n_1 p_1 + \ldots + n_{i-1} p_1 p_2 \ldots p_{i-1}\right)}{p_1 p_2 \cdots p_i} \bmod p_{i+1}$, i=0, 1, …, k-1.

Недоліками розглянутих вище методів є неможливість їх розпаралелення (або строго послідовна структура), виконання операцій над багаторозрядними числами (зокрема, обчислення залишку за модулем P), та необхідність

знаходження мультиплікативного оберненого елемента за модулем, методи пошуку якого характеризуються значною обчислювальною складністю.

Тому *метою даної роботи* є розробка методу відновлення десяткового числа за його залишками на основі додавання добутку модулів з можливістю уникнення процедури пошуку мультиплікативного оберненого елемента та залишку за модулем P.

Запишемо вираз (1) у вигляді системи:

$$\begin{cases} b_1 = N \bmod p_1 \\ b_2 = N \bmod p_2 \\ \ldots\ldots\ldots\ldots \\ b_k = N \bmod p_k . \end{cases} \quad (4)$$

Оскільки будь-яку конгруенцію $a \bmod p = b$ можна представити у вигляді $a = \gamma p + b$, де $\gamma = 0, 1, 2, \ldots$, то до залишку $b_1 = N_1$ потрібно додавати модуль p_1 стільки разів, поки не буде виконуватись рівність $N_2 \bmod p_2 = b_2$, де $N_2 = N_1 + \gamma_1 p_1$. Далі необхідно додавати добуток $p_1 p_2$, поки не буде виконуватись інша рівність $N_3 \bmod p_3 = b_3$, де $N_3 = N_2 + \gamma_2 p_1 p_2$. Даний процес продовжується до тих пір, поки не буде виконуватись останнє рівняння (4). Математично це записується так:

$$\begin{gathered} N_1 = b_1; \\ N_2 = N_1 + \gamma_1 p_1 = b_1 + \gamma_1 p_1;\ N_2 \bmod p_2 = b_2; \\ N_3 = N_2 + \gamma_2 p_1 p_2 = b_1 + \gamma_1 p_1 + \gamma_2 p_1 p_2;\ N_3 \bmod p_3 = b_3; \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ N_i = N_{i-1} + \gamma_{i-1} p_1 p_2 \ldots p_{i-1};\ N_i \bmod p_i = b_i; \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ N_k = N = N_{k-1} + \gamma_{k-1} p_1 p_2 \ldots p_{k-1};\ A_k \bmod p_k = r_k. \end{gathered} \quad (5)$$

Слід відмітити, що даний метод подібний до алгоритму Гарнера, однак у ньому уникається пошук оберненого елемента за модулем для отримання відповідних коефіцієнтів.

Для зменшення чисел, які використовуються у запропонованому методі, можна додавати не добуток модулів, а залишок цього добутку від ділення на відповідний модуль. Математичний запис даного методу виглядає таким чином:

$$\begin{gathered} N_1 = b_1;\ p_{11} = p_1 \bmod p_2; \\ (N_1 + \gamma_1 p_{11}) \bmod p_2 = b_2;\ N_2 = N_1 + \gamma_1 p_1;\ p_{12} = (p_1 p_2) \bmod p_3; \\ (N_2 + \gamma_2 p_{12}) \bmod p_3 = b_3,\ N_3 = N_2 + \gamma_2 p_1 p_2;\ p_{13} = (p_1 p_2 p_3) \bmod p_4; \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ (N_{i-1} + \gamma_{i-1} p_{1\,i-1}) \bmod p_i = b_i;\ N_i = N_{i-1} + \gamma_{i-1} p_1 p_2 p_3 \ldots p_{i-1};\ p_{1i} = (p_1 p_2 \ldots p_i) \bmod p_{i+1}; \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ (N_{k-1} + \gamma_{k-1} p_{1\,k-1}) \bmod p_k = r_k;\ N = N_k = N_{k-1} + \gamma_{k-1} p_1 p_2 p_3 \ldots p_{k-1}. \end{gathered} \quad (6)$$

Отже, розроблені методи дозволяють уникати виконання складних операцій, зокрема, ділення з остачею і пошуку мультиплікативного оберненого елемента, та проводити обчислення над числами значно меншої розрядності в порівнянні з класичною КТЗ та алгоритмом Гарнера. При цьому результати проміжних обчислень не виходять за межі встановленого діапазону, що усуває необхідність виконання операції знаходження залишку за модулем P.