УДК 511 УДК 519.6

М.В. СЕМОТЮК
Інститут кібернетики ім. В.М. Глушкова НАН України, Київ, Україна,
e-mail: *semo@i.ua.*

ТЕОРЕТИКО-ЧИСЛОВІ МЕТОДИ ФАКТОРИЗАЦІЇ СКЛАДЕНИХ ЧИСЕЛ ТА ОБЧИСЛЕННЯ ДИСКРЕТНОГО ЛОГАРИФМА

Анотація. Стаття присвячена новому застосуванню теоретико-числових перетворень. Подання систем числення цими перетвореннями дає змогу створити принципово нові і ефективні алгоритми факторизації чисел, обчислення періоду показникової функції та дискретного логарифма. Алгоритм факторизації дозволяє за один прохід розкласти будь-який скінченний добуток на множники, він є точним тестом простоти чисел. Цей алгоритм ґрунтується на поданні систем числення теоретико-числовим перетворенням і не має аналогів, оскільки використовує тільки прості арифметичні дії. Властивості простоти чисел або інші властивості чисел не застосовуються. Отже, факторизація чисел, обчислення періоду показникової функції та дискретного логарифма є арифметичними операціями, що виконуються за скінченний час і належать до P-класу складності.

Ключові слова: множина, грані множини, алгебра, кільце лишків, модуль, аксіоматика цілих чисел, теоретико-числове перетворення, система числення, основа системи числення, факторизація, арифметична операція, період показникової функції, дискретний логарифм.

ВСТУП

Існує багато задач, для яких не знайдено поліноміального алгоритму, але не доведено, що його не існує, тому невідомо, чи належать такі задачі до класу складності P. Однією з таких задач є розкладання складеного числа на множники, яке коротко називають факторизацією. Факторизація великих чисел — надзвичайно трудомістке завдання навіть для сучасних комп'ютерів [1]. У роботі [2] показано, що існує метод факторизації складених чисел, який ґрунтується на дуалізмі (подвійності) операцій у кільці лишків за модулем і породжує систему рівнянь. Хоча метод дає змогу звести факторизацію великих чисел до факторизації малих чисел, він не дозволяє стверджувати, що факторизація чисел належить до класу P-складності, оскільки вимагає інших підходів до вирішення цієї задачі.

АКСІОМАТИКА ЦІЛОГО (АНТЬЄ)

Зафіксуємо число m і розглянемо множину

$$\mathbf{Z}_m = \{0, 1, 2, \ldots, m-1\} \tag{1}$$

всіх залишків від ділення елементів числової множини $\mathbf{Z}$ на m, які входять до множини $\mathbf{Z}_m$ лише один раз. Тоді стосовно множини (1) можна констатувати, що верхньою межею або супремумом цієї множини є вираз

$$\sup \mathbf{Z}_m = \min_{i=0}^{\infty} \left(m * \operatorname{int} \frac{z_i}{m} \right) = \min_{i=0}^{m-1} (m * \operatorname{int}_m (z_i)) \;\; \forall z_i \in \mathbf{Z} | z_i \neq 0, \tag{2}$$

де $\operatorname{int}_m()$ — ціла частина відносно модуля m (коротке позначення), а максимальний елемент цієї множини має вигляд

$$\max\{z_i\} = \max_{i=0}^{m-1} ((z_i) \bmod m). \tag{3}$$