УДК 61.681.3

С.Л. КРИВИЙ
Київський національний університет імені Тараса Шевченка, Київ, Україна,
e-mail: *sl.krivoi@gmail.com*.

О.В. ЧУГАЄНКО
ТОВ «Самсунг РнД Інститут Україна», Київ, Україна, email: *firestreami13@yahoo.com*.

ПРО АЛГОРИТМИ РОЗВ'ЯЗАННЯ ЛІНІЙНИХ РІВНЯНЬ У КІЛЬЦЯХ ЛИШКІВ

Анотація. Проаналізовано два алгоритми розв'язання систем лінійних конгруенцій у кільцях лишків. Перший алгоритм ґрунтується на факторизації модуля з подальшим розв'язанням підсистем, на які розпадається початкова система, у примарних кільцях і полях. В основу другого алгоритму покладено введення певної надлишковості під час обчислень. Обидва алгоритми знаходять твірні вектори множини всіх розв'язків початкової системи лінійних конгруенцій. Наведено отримані у результаті експериментів залежності обох алгоритмів від величини модуля, кількості конгруенцій та кількості змінних у системах.

Ключові слова: лінійні рівняння, кільце лишків, алгоритми, складність.

У роботі проаналізовано два алгоритми, які будують твірні вектори множини всіх розв'язків системи лінійних однорідних конгруенцій (СЛОК) у кільці лишків за модулем m. Перший алгоритм потребує розкладу модуля m на прості множники. Проблема розкладу числа на прості множники (проблема факторизації) є складною (в обчислювальному сенсі) проблемою теорії чисел. Нині найуживанішим алгоритмом факторизації є алгоритм решета числового поля (NFS-алгоритм) з оцінкою складності $O(2^{(1.526+O(1))\sqrt[3]{\ln n}\sqrt[3]{\ln^2 n}})$ [1, 2].

Другий алгоритм не потребує факторизації модуля кільця, але під час побудови твірних векторів множини всіх розв'язків СЛОК потребує введення певної надлишковості. Ця надлишковість пов'язана з обчисленням лінійної комбінації найбільшого спільного дільника взаємно простих коефіцієнтів системи. Цей алгоритм має поліноміальну оцінку часової складності.

1. НЕОБХІДНІ ОЗНАЧЕННЯ ТА ПОНЯТТЯ

Кільцем лишків за модулем числа m називають скінченну алгебру $\mathcal{Z}_m = (A = \{0, 1, \ldots, m-1\}, \Omega = \{+, \cdot, -, {}^{-1}, 0, 1\})$, де + і $\cdot$ — бінарні операції додавання і множення за модулем m, які задовольняють закони асоціативності й комутативності та пов'язані законом дистрибутивності; операції $-$ і ${}^{-1}$ — унарні операції взяття протилежного та оберненого елемента відносно операцій + і $\cdot$ відповідно; 0 і 1 — нульарні операції, тобто адитивний нуль і мультиплікативна одиниця.

Операція взяття оберненого елемента у кільці $\mathcal{Z}_m$ у загальному випадку є частковою, оскільки коли модуль m не є простим числом, то $\mathcal{Z}_m$ матиме, крім дільників одиниці, і дільники нуля (ненульові елементи $a, b \in \mathcal{Z}_m$ називають дільниками нуля, якщо $ab = 0$; елемент a називають дільником 1, якщо для нього існує обернений елемент b такий, що $ab = 1$). Для дільників нуля операція взяття оберненого елемента невизначена.

На підставі законів для операцій у кільці $\mathcal{Z}_m$ справедлива тотожність

$$(\forall x, y \in \mathcal{Z}_m)\ x + y = m = 0 \pmod m.$$

З цієї тотожності випливає, що $x = m - y$ або $-y = x - m$. Це дає можливість замінити додатне число x на від'ємне число $-y = x - m$ і навпаки. Тоді елементи x і $-y$ називають протилежними (x протилежний до $-y$ і навпаки).