УДК 5.681.3

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

АЛГОРИТМИ РОЗВ'ЯЗАННЯ ЛІНІЙНИХ ОБМЕЖЕНЬ У КІЛЬЦІ ЛИШКІВ

Анотація. Запропоновано алгоритми перевірки виконáнності обмежень типу лінійних рівностей у кільцях лишків Z_m. Показано, що ці алгоритми належать класу поліноміальної часової складності.

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

Розглянуто алгоритми розв'язання лінійних обмежень типу рівностей у кільці лишків Z_m. У роботах [1, 2] запропоновано алгоритми поліноміальної часової складності розв'язання цих обмежень за умови відомого розкладу модуля m на прості множники. Задача розкладу числа на прості множники (задача факторизації) є складною (в обчислювальному сенсі) задачею теорії чисел. Найкращим сучасним алгоритмом факторизації вважають алгоритм решета числового поля (NFS-алгоритм) з оцінкою складності $O(2^{(1.526+O(1))(\ln n)^{1/3}(\ln\ln n)^{2/3}})$ [3, 4].

Алгоритми, запропоновані у цій роботі, будують базис множини всіх розв'язків лінійних обмежень без потреби розкладу модуля на прості множники. Це дає змогу стверджувати, що проблема перевірки виконáнності лінійних обмежень типу рівностей у кільці лишків Z_m належить класу поліноміальної складності.

ЛІНІЙНІ ОБМЕЖЕННЯ У КІЛЬЦІ Z_m

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

Операція взяття оберненого елемента у кільці $\mathcal{Z}_m$ у загальному випадку є частковою. Коли модуль m не є простим числом, то $\mathcal{Z}_m$ матиме крім дільників одиниці ще й дільники нуля (ненульові елементи $a, b \in Z_m$ 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 у кільці $\mathcal{Z}_m$

$$x = m - y \text{ або } -y = x - m,$$

що дає можливість замінити додатне число x на від'ємне число $-y = x - m$ і навпаки. Тоді елементи x і $-y$ будемо називати протилежними (x протилежний $-y$ і навпаки).

Кільце лишків $\mathcal{Z}_m$ називають примарним, якщо модуль m є степенем простого числа p, тобто $m = p^t$, де $t > 1$, $t \in \mathcal{N}$ [5]. Оскільки m не обов'язково про-