КІБЕРНЕТИКА та КОМП'ЮТЕРНІ ТЕХНОЛОГІЇ

УДК 51.681.3 DOI:10.34229/2707-451X.20.4.2

С.Л. КРИВИЙ, Г.І. ГОГЕРЧАК

ЗАДАЧА ПРО МАТЕМАТИЧНИЙ СЕЙФ ТА ЇЇ РОЗВ'ЯЗАННЯ [1] (ЧАСТИНА 1)

Робота присвячена розв'язанню задачі про математичний сейф. Розглядається математична постановка задачі про математичний сейф, де показано що її розв'язання зводиться до розв'язання систем лінійних рівнянь у скінченних кільцях та полях. Також розглядаються методи та алгоритми розв'язання такого типу систем, де наводяться методи та алгоритми побудови базису множини розв'язків систем лінійних рівнянь для цих областей та приклади для ілюстрації їх роботи.

Ключові слова: *математичний сейф, скінченні кільця, скінченні поля, метод, алгоритм, розв'язок.*

1. Вступ. Задача про математичний сейф виникає у теорії комп'ютерних ігр та криптографічних застосуваннях і перше формулювання цієї задачі було дано в роботі [1].

Неформально під математичним сейфом розуміють таку систему $Z = (z_1, z_2, \ldots, z_n)$ взаємнопов'язаних між собою засувів, що коли виконується поворот ключа в одному із засувів, то такий же поворот виконується і у всіх засувах, які пов'язані з даним. Математичний сейф може задаватися двома способами:

- за допомогою прямокутної матриці елементи якої відповідають засувам, а значення її елементів – позиціям засувів, тобто у вигляді матриці $Z = \| z_{ij} \|$, $i = 1, \ldots, m, j = 1, \ldots, n$, і
- за допомогою графа $G(V, E)$, вершини якого відповідають засувам.

Далі ці способи будемо називати матричним сейфом і графовим сейфом відповідно. В матричному сейфі кожний засув z_{ij} пов'язаний з тими засувами, які розміщені в i-му рядку і в j-му стовпчику. А в графовому сейфі, пов'язаними з засувом у вершині u є ті, які відповідають засувам розміщеним у вершинах, суміжних з вершиною u. Кожний із засувів може знаходитися в одній із декількох позицій. Всіх можливих позицій скінченне число: $0, 1, \ldots, k-1$. Засув відкритий, якщо він знаходиться в позиції 0. В довільній іншій позиції засув вважається закритим. Початковий стан сейфа Z при першому способі задання визначається матрицею $B = \| b_{ij} \|$, а при другому позиціями засувів у вершинах. При цьому, якщо в якомусь засуві виконується поворот ключа, то всі засуви, які пов'язані з даним засувом, збільшують свої позиції на одиницю за модулем k.

Необхідно розв'язати таку задачу. Виходячи з початкового стану сейфа, знайти таку послідовність засувів і число поворотів ключа в них, щоб сейф перейшов у положення відкритого, тобто коли всі засуви знаходяться в позиції 0. Розглянемо строгу математичну постановку задачі про матричний математичний сейф.

[1] За фінансової підтримки НАН України (проект 0118U005227)

Математична постановка задачі. Нехай матриця $X = \| x_{ij} \|$ – шуканий розв'язок задачі, де x_{ij} дорівнює числу поворотів ключа в засуві z_{ij}. Тоді умовою того, що елемент b_{ij} перетвориться матрицею X в нуль, виражається співвідношенням

$$\sum_{s=1}^{n} x_{is} + \sum_{s=1, s \neq i}^{m} x_{sj} + b_{ij} \equiv 0 \,(mod\ k), \tag{1}$$

де $i = 1,\ldots,m,\ j = 1,\ldots,n$.

Позначимо $\bar{x} = (x_{11},\ldots,x_{1n},x_{21},\ldots,x_{2n},\ldots,x_{m1},\ldots,x_{mn})$ вектор-стовпчик, отриманий з матриці X послідовним записом її рядків. Аналогічно з матриці B початкових станів засувів отримаємо вектор-стовпчик $\bar{b}$. Крім того, нехай J_n – матриця розмірністю $n \times n$, яка складається із одиниць, E_n – одинична матриця тієї ж розмірності. Тоді розв'язок задачі про математичний сейф зводиться до перетворення (1) для всієї матриці B і записується у вигляді системи лінійних неоднорідних діофантових рівнянь (СЛНДР) за модулем k:

$$A\bar{x} + \bar{b} \equiv 0 \,(mod\ k), \tag{2}$$

де матриця A розмірністю $mn \times mn$ складається із m^2 клітинок:

$$A = \begin{bmatrix} J_n & E_n & E_n & \cdots & \cdots & E_n \\ E_n & J_n & E_n & \cdots & \cdots & E_n \\ E_n & E_n & J_n & \cdots & \cdots & E_n \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ E_n & E_n & E_n & \cdots & \cdots & J_n \end{bmatrix}. \tag{3}$$

Таким чином, розв'язання задачі про математичний сейф зводиться до пошуку розв'язків системи лінійних діофантових рівнянь у скінченних полях і кільцях лишків за модулем k.

Така постановка задачі про математичний сейф, як зазначалося вище, була дана в [1] і цю постановку будемо називати *первинною*. В другій частині роботи будуть розглянуті численні модифікації цієї постановки та методи розв'язання задачі про матетаичний сейф для цих модифікацій над такими областями як кільце лишків Z_m за модулем складеного числа m, поле лишків F_p за модулем простого числа p та розширення поля лишків F_{p^k} з p^k елементами, де p – просте.

2. Системи лінійних рівнянь у скінченних кільцях та полях

Кільце лишків за модулем $m \in N$ – це алгебра $Z_m = (A = \{0,1,\ldots,m-1\},\ \Omega = \{+,\cdot,-,^{-1},0,1\})$, де + і · – бінарні асоціативно-комутативні операції додавання і множення за модулем m, пов'язані законом дистрибутивності, унарні операції – і $^{-1}$ взяття протилежного і оберненого елемента відносно операцій + і · відповідно, 0 і 1 – нульарні операції – адитивний нуль і мультиплікативна одиниця [2]. Операція взяття оберненого елемента в кільці Z_m у загальному випадку є частковою, оскільки модуль m не є простим числом, то Z_m матиме дільники нуля, а для дільників нуля ця операція не визначена. На підставі законів для операцій у кільці Z_m справедлива така тотожність:

$$(\forall x \exists y \in Z_m)\ x + y = m = 0.$$

З цієї тотожності випливає, що в кільці Z_m $x = m - y$, а $-y = x - m$, що дає можливість замінити додатне число x на від'ємне число $-y = x - m$ і навпаки. Елементи x і y будемо називати протилежними (x протилежний до y і навпаки).

Кільце лишків Z_m називається **примарним**, якщо модуль m є степенем простого числа p, тобто $m = p^t$, де $t > 1$, $t \in N$. Оскільки m не обов'язково просте число, то порівняння $ax \equiv b\,(mod\ m)$ в кільці Z_m при $a \neq 0$ не завжди матиме розв'язок. Це порівняння матиме розв'язок, якщо НСД$(a, m) = 1$ або НСД$(a, m) = d$ і d – дільник числа b.

Кільце лишків Z_m стає полем лишків, якщо модуль m просте число.

Розглянемо СЛНДР над кільцем Z_m

$$S = \begin{cases} L_1(x) = a_{11}x_1 + \ldots + a_{1q}x_q = b_1, \\ L_2(x) = a_{21}x_1 + \ldots + a_{2q}x_q = b_2, \\ \ldots \quad \ldots \quad \ldots \quad \ldots \quad \ldots \quad \ldots \quad \ldots \quad \ldots \quad \ldots \\ L_s(x) = a_{s1}x_1 + \ldots + a_{sq}x_q = b_s, \end{cases} (mod\ m), \tag{4}$$

де $a_{ij}, b_i \in Z_m$, $i = 1,\ldots,s$, $j = 1,\ldots,q$.

Нехай модуль має розклад на прості множники $m = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$, де $p_1 < p_2 < \ldots < p_r$. Тоді системі S відповідає еквівалентна їй система із $r \cdot s$ рівнянь вигляду [3]

$$S' = \begin{cases} \begin{cases} L_1(x) = a_{11}x_1 + \ldots + a_{1q}x_q = b_1, \\ L_2(x) = a_{21}x_1 + \ldots + a_{2q}x_q = b_2, \\ \ldots \quad \ldots \quad \ldots \quad \ldots \quad \ldots \quad \ldots \quad \ldots \quad \ldots \quad \ldots \\ L_s(x) = a_{s1}x_1 + \ldots + a_{sq}x_q = b_s, \end{cases} (mod\ p_1^{k_1}) \\ \begin{cases} L_1(x) = a_{11}x_1 + \ldots + a_{1q}x_q = b_1, \\ L_2(x) = a_{21}x_1 + \ldots + a_{2q}x_q = b_2, \\ \ldots \quad \ldots \quad \ldots \quad \ldots \quad \ldots \quad \ldots \quad \ldots \quad \ldots \quad \ldots \\ L_s(x) = a_{s1}x_1 + \ldots + a_{sq}x_q = b_s, \end{cases} (mod\ p_2^{k_2}) \\ \vdots \\ \begin{cases} L_1(x) = a_{11}x_1 + \ldots + a_{1q}x_q = b_1, \\ L_2(x) = a_{21}x_1 + \ldots + a_{2q}x_q = b_2, \\ \ldots \quad \ldots \quad \ldots \quad \ldots \quad \ldots \quad \ldots \quad \ldots \quad \ldots \quad \ldots \\ L_s(x) = a_{s1}x_1 + \ldots + a_{sq}x_q = b_s. \end{cases} (mod\ p_r^{k_r}) \end{cases} \tag{5}$$

Дійсно, еквівалентність систем випливає з того, що коли x – розв'язок системи S, то він буде розв'язком і кожної із підсистем за модулем $p_i^{k_i}$, оскільки модуль m ділиться на кожне з чисел $p_i^{k_i}$, $i = 1, 2\ldots, r$. Якщо ж x – розв'язок системи S', то він буде розв'язком кожної із її підсистем за модулем $p_i^{k_i}$, а тому і розв'язком системи S за модулем m, оскільки числа $p_i^{k_i}$ взаємно прості та їх добуток дорівнює m.

Перейдемо від системи S' до системи однорідних рівнянь

$$S'' = \begin{cases} \begin{cases} L_1(x) = a_{11}x_1 + \ldots + a_{1q}x_q - b_1x_0 = 0, \\ L_2(x) = a_{21}x_1 + \ldots + a_{2q}x_q - b_2x_0 = 0, \\ \ldots \quad \ldots \quad \ldots \quad \ldots \quad \ldots \quad \ldots \quad \ldots \quad \ldots \quad \ldots \quad \ldots \\ L_s(x) = a_{s1}x_1 + \ldots + a_{sq}x_q - b_sx_0 = 0, \end{cases} (mod\ p_1^{k_1}) \\ \begin{cases} L_1(x) = a_{11}x_1 + \ldots + a_{1q}x_q - b_1x_0 = 0, \\ L_2(x) = a_{21}x_1 + \ldots + a_{2q}x_q - b_2x_0 = 0, \\ \ldots \quad \ldots \quad \ldots \quad \ldots \quad \ldots \quad \ldots \quad \ldots \quad \ldots \quad \ldots \quad \ldots \\ L_s(x) = a_{s1}x_1 + \ldots + a_{sq}x_q - b_sx_0 = 0, \end{cases} (mod\ p_2^{k_2}) \\ \vdots \\ \begin{cases} L_1(x) = a_{11}x_1 + \ldots + a_{1q}x_q - b_1x_0 = 0, \\ L_2(x) = a_{21}x_1 + \ldots + a_{2q}x_q - b_2x_0 = 0, \\ \ldots \quad \ldots \quad \ldots \quad \ldots \quad \ldots \quad \ldots \quad \ldots \quad \ldots \quad \ldots \quad \ldots \\ L_s(x) = a_{s1}x_1 + \ldots + a_{sq}x_q - b_sx_0 = 0. \end{cases} (mod\ p_r^{k_r}) \end{cases} \tag{6}$$

Нехай x – розв’язок підсистеми вигляду

$$S_1 = \begin{cases} L_1(x) = a_{11}x_1 + \ldots + a_{1q}x_q - b_1x_0 = 0, \\ L_2(x) = a_{21}x_1 + \ldots + a_{2q}x_q - b_2x_0 = 0, \\ \ldots \quad \ldots \quad \ldots \quad \ldots \quad \ldots \quad \ldots \quad \ldots \quad \ldots \quad \ldots \quad \ldots \\ L_s(x) = a_{s1}x_1 + \ldots + a_{sq}x_q - b_sx_0 = 0. \end{cases} (mod\ p_1^{k_1})$$

Тоді вектор m_1x, де $m_1 = \dfrac{m}{p_1^{k_1}}$ є розв'язком системи S''. Дійсно, для другої системи S_2, аналогічної попередній за модулем $p_2^{k_2}$, дістаємо для довільного її рівняння L_i

$$L_i(m_1x) = m_1L_i(x) = m_1d_i \equiv 0\ (mod\ p_2^{k_2}),$$

$i = 1,2\ldots,s$, оскільки m_1 кратне $p_2^{k_2}$, а d_i кратне $p_1^{k_1}$.

Аналогічно, якщо y – розв'язок S_2, то m_2y, де $m_2 = \dfrac{m}{p_2^{k_2}}$, буде розв'язком системи S'' і так далі для довільної із систем $S_3,\ldots,S_r$. Тоді загальний розв'язок системи S'' набуває вигляду

$$x = m_1x_1 + m_2x_2 + \ldots + m_rx_r,$$

де x_i – розв'язок системи S_i.

Позначимо $e_i = m_ix_i$, де x_i – розв'язок системи $S_i, i = 1,2,\ldots,r$. Покажемо, що ці вектори лінійно незалежні над кільцем Z_m. Для цього подамо вектори e_i в координатній формі

$$e_1 = (c_{11},\ldots,c_{1q}), e_2 = (c_{21},\ldots,c_{2q}),\ldots,e_k = (c_{k1},\ldots,c_{kq})$$

і припустимо, що існують числа $a_1, a_2, \ldots, a_k$, де $a_i < p_i^{k_i}$, такі, що

$$a_1e_1 + a_2e_2 + \ldots + a_ke_k \equiv 0\,(mod\ m)$$

або, що те саме $a_2e_2 + \ldots + a_ke_k \equiv b_1e_1\,(mod\ m)$, де b_1 протилежний до a_1 в кільці Z_m і $a_1e_1 \not\equiv 0(mod\ m)$. Приймаючи до уваги координатну форму векторів $e_i, i = 1,2,\ldots k$, дістаємо систему

$$S_1^{'} = \begin{cases} a_2m_2c_{21}' + \ldots + a_km_kc_{k1} \equiv b_1m_1c_{11}', \\ a_2m_2c_{22}' + \ldots + a_km_kc_{k2} \equiv b_1m_1c_{12}', \\ \ldots \quad \ldots \quad \ldots \quad \ldots \quad \ldots \quad \ldots \\ a_2m_2c_{2q}' + \ldots + a_km_kc_{kq} \equiv b_1m_1c_{1q}', \end{cases} (mod\ p_1^{k_1}),$$

де c_{ij}' – координати векторів $x_i, i = 1,2,\ldots,r$.

З порівнянь системи $S_1^{'}$ випливає, що ліва частина кожного з порівнянь кратна $p_1^{k_1}$, як і сам модуль m. Але тоді система $S_1^{'}$ буде мати розв'язок тільки у випадку кратності числа b_1m_1 (і тим самим кратності a_1c_{1i}) числу $p_1^{k_1}$. Але якщо всі числа a_1c_{1i} кратні $p_1^{k_1}$, то отримуємо $a_1e_1 \equiv 0\,(mod\ m)$, що суперечить припущенню $a_1e_1 \not\equiv 0\ \ (mod\ m)$. Отримана суперечність показує несумісність системи $S_1^{'}$, а це означає лінійну незалежність сукупності векторів $e_1, e_2, \ldots, e_k$.

Таким чином, достатньо вміти розв'язувати систему S'. А розв'язання такої системи зводиться до розв'язання систем або в полі лишків F_p, або в примарному кільці за модулем степеня простого числа.

2.1. Системи лінійних рівнянь в полі F_p

Оскільки p – просте число, то в полі F_p при $a \not\equiv 0$ завжди існує розв'язок порівняння $ax \equiv b\,(mod\ p)$, причому цей розв'язок єдиний.

Нехай дано СЛНДР в полі F_p

$$S = \begin{cases} L_1(x) = a_{11}x_1 + \ldots + a_{1n}x_n = b_1, \\ L_2(x) = a_{21}x_1 + \ldots + a_{2n}x_n = b_2, \\ \ldots \quad \ldots \quad \ldots \quad \ldots \quad \ldots \quad \ldots \quad \ldots \quad \ldots \quad \ldots \\ L_q(x) = a_{q1}x_1 + \ldots + a_{qn}x_n = b_q, \end{cases} (mod\ p) \qquad (7)$$

де $a_{ij}, b_i, x_i \in F_p, i = 1,\ldots,n,\ j = 1,\ldots,q$.

Розглянемо TSS-метод побудови базиса множини розв'язків систем лінійних однорідних діофантових рівнянь (СЛОДР) в полі F_p. Цей метод детально описаний в [4, 5], а в цьому розділі наведемо його модифікацію орієнтовану на розв'язання задачі побудови базиса множини всіх розв'язків СЛНДР в полі лишків F_p.

Випадок лінійного однорідного діофантового рівняння (ЛОДР). Нехай дано ЛОДР

$$L(x) = a_1x_1 + \ldots + a_ix_i + \ldots + a_nx_n = 0, \qquad (8)$$

де $a_i, x_i \in F_p, i = 1,\ldots,n$. Припустимо, що $a_i \not\equiv 0$, тоді має місце таке просте твердження.

Лема 1. Якщо $c=(c_1,\ldots,c_n)$ – розв'язок ЛОДР (8) в F_p, то він буде розв'язком ЛОДР $a_1x_1+\ldots-b_ix_i+\ldots+a_nx_n=0$, де $-b_i$ – протилежний до коефіцієнта a_i.

Доведення. За умовою леми маємо $a_1c_1+\ldots+a_ic_i+\ldots+a_nc_n=0$, але тоді

$$a_1c_1+\ldots-b_ic_i+\ldots+a_nc_n=-pc_i+a_1c_1+\ldots+a_ic_i+\ldots+a_nc_n=0.$$

Зауважимо, що коли $c=k\cdot c'$, де $k=\text{НСД}(c_1,c_2,\ldots,c_n)$, то $c'=(c_{1'},c_{2'},\ldots,c_{n'})$ теж буде розв'язком (8). Дійсно, якщо c – розв'язок, то

$$a_1c_1+a_2c_2+\ldots+a_nc_n=k(a_1c_{1'}+a_2c_{2'}+\ldots+a_nc_{n'})=0$$

і оскільки $k\neq 0$, то $a_1c_{1'}+a_2c_{2'}+\ldots+a_nc_{n'}=0$. ■

Розглянемо множину векторів канонічного базису $M_0=\{e_1,\ e_2,\ldots,e_n\}$ і функцію $L(x)=a_1x_1+a_2x_2+\ldots+a_nx_n$ ЛОДР (8). Замінимо в функції $L(x)$ перший ненульовий коефіцієнт a_k його протилежним $-b_k$ і побудуємо множину векторів:

$$B=\{(0,\ldots,a_j,0,\ldots,0,b_k,0,\ldots,0)\}\cup M_0,$$

де $M_0=\{e_r: L_1(e_r)=0\}$, $a_j\neq 0$, а b_k є j-ю координатою у векторах із B. Причому, якщо для деякого a_i НСД$(a_i,b_k)\neq 1$, то скоротимо координати такого вектора на цей спільний дільник (це можна зробити на підставі леми 1). Таким чином, можна вважати, що всі вектори в множині B такі, що a_i і b_k взаємно прості, а множина B будується шляхом комбінування протилежного елемента до першого ненульового коефіцієнта, взятого з від'ємним знаком, з рештою ненульових коефіцієнтів і поповненого векторами канонічного базису, які відповідають нульовим коефіцієнтам ЛОДР (8). Побудована таким чином множина буде називатися *TSS*-множиною. Очевидно, що вектори із множини B є розв'язками ЛОДР (8).

Лема 2. Якщо $d=(0,\ldots,0,d_i,0,\ldots,0,d_j,0,\ldots,0)$ – розв'язок ЛОДР (8), то він або є елементом B, або представляється у вигляді невід'ємної лінійної комбінації векторів із B.

Доведення. Якщо $d\in B$, то доводити немає чого. Якщо $d=(0,\ldots,0,d_i,0,\ldots,0,d_j,0,\ldots,0)\notin B$, то можливі два випадки.

Випадок 1. У множині B існують вектори $s_1=(0,\ldots,0,a_{i'},\ 0,\ldots,0,a_{k'},0,\ldots,0)$ і $s_2=(0,\ldots,0,a_{j'},0,\ldots,0,a_{k'},\ 0,\ldots,0)$, в яких $a_{i'}$ і $a_{j'}$ є k-ми координатами, а $a_{k'}$ в s_1 і s_2 є відповідно i-ю і j-ю координатами. Розглянемо вектор

$$s=us_1+vs_2=(0,\ldots,0,a_{i'}u+a_{j'}v,0,\ldots,0,d_i,0,\ldots,0,d_j,0,\ldots,0),$$

де u,v – розв'язки порівнянь $a_{k'}x\equiv d_i\ (mod\ p)$ і $a_{k'}y\equiv d_j\ (mod\ p)$, відповідно. В полі F_p розв'язки u і v єдині. Покажемо, що $a_{i'}u+a_{j'}v=0$. Для цього підставимо вектор s в ЛОДР (8):

$$L(s)=a_k(a_{i'}u+a_{j'}v)+a_id_i+a_jd_j=a_k(a_{i'}u+a_{j'}v)+0=a_k(a_{i'}u+a_{j'}v)=0$$

і оскільки $a_k\neq 0$, то $a_{i'}u+a_{j'}v=0$, а це і вимагалося показати.

Випадок 2. У B існує вектор $s_1=(0,\ldots,0,b_i,0,\ldots,0,b_j,0,\ldots,0)$. Розглянемо вектор

$$s=ys_1=(0,\ldots,0,c_i,0,\ldots,0,yb_j,0,\ldots,0),$$

де y – єдиний розв'язок порівняння $b_i y \equiv c_i \pmod{p}$. Оскільки x і s – розв'язки ЛОДР (8), то $x - s$ теж буде розв'язком цього ЛОДР, тобто $x - s = (0,\ldots,0,d_j - b_j y,0,\ldots,0)$ і

$$L(x-s) = a_j(d_j - yb_j) = 0 .$$

Оскільки $a_j \not\asymp 0$, то $d_j = yb_j$. ■

Теорема 1. *TSS* ЛОДР (8) В, побудована комбінуванням протилежного до першого ненульового коефіцієнта, взятого з від'ємним знаком, з рештою ненульових коефіцієнтів і поповнена векторами канонічного базису, які відповідають нульовим коефіцієнтам ЛОДР (8), є базисом множини всіх розв'язків цього ЛОДР.

Часова складність алгоритму пропорціональна величині l^3, де $l = \max(m,n)$, m – кількість розрядів у двійковому зображенні модуля p, а n – кількість невідомих в ЛОДР.

Доведення проводиться індукцією за числом k ненульових координат у розв'язку ЛОДР. Нехай $x = (x_1, x_2, \ldots, x_n)$ – довільний розв'язок ЛОДР (8).

Базис індукції. Якщо $k = 1$, то x має збігатися з одним із векторів канонічного базиса (який за побудовою є елементом B) і доводити немає чого. При $k = 2$ справедливість теореми випливає з леми 2.

Крок індукції. Припустимо, що теорема справедлива для всіх $2 \le k < m$ і x має m ненульових координат. Розглянемо ненульові координати x_i, x_j вектора x. Можливі три випадки.

Випадок 1. У B існує вектор канонічного базису s з i-ю координатою, яка дорівнює 1. Тоді вектор $y = x - x_i s$ буде мати $m-1$ ненульових координат. За припущенням індукції для цього вектора існує подання

$$x - x_i s = d_1 e_1 + \ldots + d_r e_r ,$$

де $e_i \in B, i = 1,\ldots,r$. Але тоді

$$x = x_i s + d_1 e_1 + \ldots + d_r e_r .$$

Випадок 2. У B існує вектор $s = (0,\ldots,0,b_i,0,\ldots,0,b_j,\ 0,\ldots,0)$ з ненульовими координатами b_i і b_j. Розглянемо вектор

$$x - us = (x_1,\ldots,x_{i-1},0,x_{i+1},\ldots,x_j - ub_j,\ldots,x_n),$$

де u – розв'язок порівняння $b_i u \equiv x_i \pmod{p}$. Побудований вектор має $m-1$ ненульових координат і за припущенням індукції отримуємо, що

$$x - us = d_1 e_1 + \ldots + d_r e_r \text{ або } x = us + d_1 e_1 + \ldots + d_r e_r .$$

Випадок 3. У B існують вектори $s_1 = (0,\ldots,0,b_i,0,\ldots,0,b_k,\ 0,\ldots,0)$ і $s_2 = (0,\ldots,0,b_j,0,\ldots,0,\ b_k,0,\ldots,0)$ з ненульовими координатами b_i, b_j і b_k. Побудуємо вектор

$$s = b_j s_1 - b_i s_2 = (0,\ldots,0,b_k b_j,0,\ldots,0,-b_k b_i,0,\ldots,0),$$

у якого після заміни $-b_k b_i$ його додатним протилежним ненульовими координатами будуть координати з номерами i і j. Очевидно, що вектор s є розв'язком ЛОДР (8) і тоді на підставі леми 2 він виражається через вектори із множини B. Нехай

$$s' = (0,\ldots,0,b_j,0,\ldots,0,b_i,0,\ldots,0) = d_1 e_1 + \ldots + d_r e_r$$

це подання. Після цього доведення зводиться до випадку 2, який був вище розглянутий.

При отриманні оцінки часової складності елементарними вважаються операції додавання і віднімання. При побудові TSS для ЛОДР обчислюються $n-1$ векторів і не більше, ніж $n-1$ разів НСД двох чисел у полі F_p. Побудова векторів вимагає, очевидно, не більше ніж $n(n-1)$ кроків, а складність обчислення НСД за допомогою алгоритма Евкліда пропорціональна m^2, де m – розрядність чисел, для яких обчислюється НСД [6, 7]. Додаючи всі ці величини, отримуємо оцінку $O(l^3)$, де $l = \max(m,n)$. ■

Приклад 1. Побудувати базис множини всіх розв'язків ЛОДР $2x_1 + x_2 + 0x_3 + x_4 + 2x_5 = 0$ в полі лишків F_3.

Розв'язання. Перший ненульовий коефіцієнт в даному ЛОДР є $a_1 = 2$, а його протилежний дорівнює 2 – 3 = –1. Отримуємо ЛОДР $-x_1 + x_2 + 0x_3 + x_4 + 2x_5 = 0$. Застосовуючи TSS-метод, отримуємо такі базисні розв'язки: $e_1 = (1,1,0,0,0)$, $e_2 = (1,0,0,1,0)$, $e_3 = (2,0,0,0,1)$, $e_4 = (0,0,1,0,0)$.

Наприклад, очевидними розв'язками даного ЛОДР є вектори $c_1 = (1,1,1,1,1)$ і $c_2 = (0,2,0,1,0)$.

Подання цих векторів через базисні вектори виглядає так:

$$c_1 = e_1 + e_2 + e_3 + e_4 = (4\ (mod\ 3),1,1,1,1) = (1,1,1,1,1),\ c_2 = 2e_1 + e_2 = (0,2,0,1,0).$$

Примітка: ♠ – кінець приклада.

Випадок СЛОДР. Нехай дана СЛОДР S (7). Розглянемо множину векторів канонічного базису $M_0^{'} = \{s_1, s_2, ..., s_n\}$ і перше рівняння $L_1(x) = a_{11}x_1 + a_{12}x_2 + \ldots + a_{1q}x_n = 0$ системи S. Побудуємо базис $B_1 = \{e_1, \ldots, e_m\}$ множини всіх розв'язків цього ЛОДР вище описаним способом. Візьмемо функцію $L_2(x) = a_{21}x_1 + a_{22}x_2 + \ldots + a_{2n}x_n$ і розглянемо ЛОДР

$$L_2(e_1)y_1 + L_2(e_2)y_2 + \ldots + L_2(e_m)y_m = 0. \qquad (9)$$

Зазначимо, що коли всі $L_2(e_i) = 0$, то рівняння $L_2(x)$ лінійно виражається через $L_1(x)$ і його можна вилучити із СЛОДР S. Через це будемо вважати, що всі рівняння в S лінійно незалежні.

Знайдемо TSS-методом базис $B' = \{r_1, r_2, \ldots, r_{m-1}\}$ множини розв'язків ЛОДР (9) і побудуємо за векторами із B' відповідні лінійні комбінації векторів із B_1. Позначимо цю множину $M = \{s_1,\ s_2, \ldots, s_{m-1}\}$.

Лема 3. Множина M – базис множини всіх розв'язків СЛОДР

$$S = \begin{cases} L_1(x) = a_{11}x_1 + \ldots + a_{1n}x_n = 0, \\ L_2(x) = a_{21}x_1 + \ldots + a_{2n}x_n = 0. \end{cases} \qquad (10)$$

Доведення. Очевидно, що всі елементи із M – розв'язки СЛОДР S. Нехай $x = (x_1, \ldots, x_n)$ – довільний розв'язок СЛОДР S, тоді $x = d_1e_1 + \ldots + d_me_m$, де $e_i \in B_1, i = 1, \ldots, m$. Підставляючи x в $L_2(x)$, дістаємо ЛОДР

$$d_1L_2(e_1) + \ldots + d_mL_2(e_m) = c_1d_1 + \ldots + c_md_m = 0,$$

тобто вектор $(d_1, d_2, \ldots, d_m)$ є розв'язком ЛОДР (9) і, отже, він представляється у вигляді невід'ємної лінійної комбінації векторів із B':

$$(d_1, \ldots, d_m) = f_1r_1 + \ldots + f_{m-1}r_{m-1}.$$

Але тоді отримуємо $x = d_1e_1 + \ldots + d_me_m = f_1s_1 + \ldots + f_{m-1}s_{m-1}$, а це означає, що x представляється у вигляді невід'ємної лінійної комбінації векторів із M. На підставі довільності вектора x отримуємо справедливість леми. ■

Теорема 2. Нехай M – TSS-множина, побудована вищеописаним способом для СЛОДР S, тоді M є базисом множини всіх розв'язків цієї СЛОДР.

Складність побудови базиса пропорціональна величині ql^3, де q – число рівнянь СЛОДР, $l = \max(m,n)$, m – кількість розрядів у двійковому зображенні модуля p, а n – кількість невідомих СЛОДР.

Доведення виконується індукцією за числом k рівнянь в СЛОДР S.

Базис індукції при $k = 2$ має місце на підставі леми 3.

Крок індукції. Припустимо, що теорема справедлива для всіх $k < q$. Тоді TSS-множина розв'язків СЛОДР S', що складається з перших $q-1$ рівнянь, за припущенням індукції є базисом множини розв'язків S'.

Повторюючи викладки, аналогічні тим, які використовувалися при доведенні леми 3, отримуємо справедливість теореми.

Оцінка часової складності, що наведена у формулюванні теореми, очевидним чином випливає з теореми 1. ■

Приклад 2. Знайти в полі F_3 базис множини розв'язків СЛОДР

$$S = \begin{cases} 2x_1 + x_2 + 0x_3 + x_4 + 2x_5 = 0, \\ x_1 + 2x_2 + 1x_3 + 0x_4 + x_5 = 0, \\ x_1 + x_2 + 2x_3 + 2x_4 + 0x_5 = 0. \end{cases}$$

Розв'язання. В прикладі 1 знайдено базис множини розв'язків першого ЛОДР цієї системи:

$$e_1 = (1,1,0,0,0), e_2 = (1,0,0,1,0), e_3 = (2,0,0,0,1), e_4 = (0,0,1,0,0).$$

Знаходимо $L_2(e_1) = 0, L_2(e_2) = 1, L_2(e_3) = 0, L_2(e_4) = 1$ і будуємо ЛОДР $0y_1 + y_2 + 0y_3 + y_4 = 0y_1 - 2y_2 + 0y_3 + y_4 = 0.$

Базис множини розв'язків складається із векторів

$$r_1 = (1,0,0,0), r_2 = (0,1,0,2), r_3 = (0,0,1,0).$$

Базисні вектори множини розв'язків для перших двох рівнянь із S, що відповідають векторам r_1, r_2, r_3, є такими:

$$e_1^{'} = 1e_1 = (1,1,0,0,0), \; e_2^{'} = e_2 + 2e_4 = (1,0,2,1,0), \; e_3^{'} = 1e_3 = (2,0,0,0,1).$$

Знаходимо значення $L_3(e_1^{'}) = 2, L_3(e_2^{'}) = 1, L_3(e_3^{'}) = 2$, будуємо ЛОДР

$$2y_1 + y_2 + 2y_3 = -y_1 + y_2 + 2y_3 = 0$$

і знаходимо його розв'язки: $r_1 = (1,1,0), r_2 = (2,0,1)$. Відповідні їм вектори базису множини розв'язків СЛОДР S мають вигляд: $s_1 = e_1^{'} + e_2^{'} = (2,1,2,1,0), \; s_2 = 2e_1^{'} + e_3^{'} = (1,2,0,0,1)$. ♠

2.2. *TSS*-метод розв'язання СЛНДР

Випадок ЛНДР. Нехай дано ЛНДР в полі F_p

$$a_1x_1 + a_2x_2 + \ldots + a_nx_n = b. \tag{11}$$

Розглянемо рівняння $a_1x_1 + a_2x_2 + \ldots + a_nx_n - bx_0 = 0$, розв'язки якого при $x_0 = 1$ будуть розв'язками (11). Застосовуючи TSS-метод до цього ЛОДР, знаходимо

$$s_1 = (b,0,\ldots,a_1),\ldots,s_n = (0,\ldots,0,b,a_n).$$

Серед цих розв'язків необхідно знайти ті, у яких $x_0 = 1$. Але $x_0 \in \{a_1, a_2, \ldots, a_n\}$ і тоді шуканими розв'язками будуть ті розв'язки x, які є розв'язками порівняння $a_i x \equiv 1 (mod\ p)$.

На підставі простоти p це порівняння має єдиний розв'язок, причому це має місце для довільного $a_i \neq 0, i = 1,2,\ldots,n$. Отже, можна вибрати довільне $a_i \neq 0$ і для нього розв'язувати порівняння. Оскільки порівняння $a_i x \equiv 1 (mod\ p)$ має розв'язок, то і порівняння (11) теж буде мати розв'язок.

Нехай $x^1 = (c_1, c_2, \ldots, c_n)$ – деякий окремий розв'язок (11), знайдений вищеописаним способом, а $B = \{e_1, e_2, \ldots, e_m\}$ базис множини розв'язків ЛОДР

$$a_1 x_1 + a_2 x_2 + \ldots + a_n x_n = 0. \tag{12}$$

Лема 4. Довільний розв'язок **u** ЛНДР (11) записується у вигляді $u = x^1 + \sum_{i=1}^{m} b_i e_i$, де x^1 – окремий розв'язок ЛНДР (11), а $e_1, \ldots, e_m$ – базисні вектори множини розв'язків ЛОДР (12), яке відповідає ЛНДР (11).

Доведення. Нехай $u = (u_1, u_2, \ldots, u_n, 1)$ – довільний розв'язок ЛНДР (11), а $B = \{e_1, e_2, \ldots, e_m\}$ – базис множини розв'язків ЛОДР, яке відповідає (11). Розглянемо вектор

$$y = u - x^1 = (d_1, d_2, \ldots, d_n).$$

Якщо деякі з координат вектора y стали від'ємними, то замінимо їх додатними протилежними. Вектор y є розв'язком ЛОДР і, отже, представляється у вигляді невід'ємної лінійної комбінації векторів із B, тобто $y = \sum_{i=1}^{m} b_i e_i$, $e_i \in B, i = 1,2,\ldots,m$. Але тоді $u = x^1 + \sum_{i=1}^{m} b_i e_i$. ■

Приклад 3. Знайти в полі F_{13} загальний розв'язок ЛНДР $2x + 3y + 5z + 6u + 4v = 7$.

Розв'язання. Виберемо перший ненульовий коефіцієнт $a_1 = 2$ і побудуємо вектор $(7,0,0,0,0,2)$. Розв'язуємо порівняння $2s \equiv 1 (mod\ 13)$. Розв'язком цього порівняння буде, очевидно, $s = 7$. Тоді вектор $x^1 = 7(7,0,0,0,0) = (10,0,0,0,0)$ буде шуканим окремим розв'язком ЛНДР.

Знайдемо базис множини розв'язків ЛОДР $2x + 3y + 5z + 6u + 4v = 0$. Замінивши, наприклад, коефіцієнт 3 його протилежним –10 і побудуємо базис множини розв'язків ЛОДР $2x - 10y + 5z + 6u + 4v = 0$. Цими розв'язками будуть вектори:

$$e_1 = (5,1,0,0,0), e_2 = (0,1,2,0,0), \quad e_3 = (0,3,0,5,0), e_4 = (0,2,0,0,5).$$

Отже, загальний розв'язок даного ЛНДР матиме вигляд: $x = x^1 + b_1 e_1 + b_2 e_2 + b_3 e_3 + b_4 e_4$.

Наприклад, при $b_1 = b_2 = b_3 = b_4 = 1$ отримуємо $u = (2,7,2,5,5)$. ♠

Випадок СЛНДР. Нехай дана СЛНДР

$$S = \begin{cases} L_1(x) = a_{11}x_1 + \ldots + a_{1n}x_n = b_1, \\ L_2(x) = a_{21}x_1 + \ldots + a_{2n}x_n = b_2, \\ \ldots \quad \ldots \quad \ldots \quad \ldots \quad \ldots \quad \ldots \quad \ldots \quad \ldots \quad \ldots \\ L_q(x) = a_{q1}x_1 + \ldots + a_{qn}x_n = b_q, \end{cases} \tag{13}$$

де $a_{ij}, b_i, x_i \in F_p, i = 1,\ldots,n,\ j = 1,\ldots,q, q < n$. Оскільки рівняння можна додавати і віднімати, то перетворимо S до вигляду (вважаючи, що $b_q \neq 0$)

$$S' = \begin{cases} L_1'(x) = a_{11}'x_1 + \ldots + a_{1n}'x_n = 0, \\ L_2'(x) = a_{21}'x_1 + \ldots + a_{2n}'x_n = 0, \\ \ldots \quad \ldots \quad \ldots \quad \ldots \quad \ldots \quad \ldots \quad \ldots \quad \ldots \quad \ldots \\ L_{q-1}'(x) = a_{q-11}'x_1 + \ldots + a_{q-1n}'x_n = 0, \\ L_q(x) = a_{q1}x_1 + \ldots + a_{qn}x_n = b_q. \end{cases} \quad (14)$$

Нехай $B' = \{e_1', e_2', \ldots, e_m'\}$ – базис множини розв'язків СЛОДР, яка складається із перших $q-1$ рівнянь системи S', а $B = \{e_1, e_2, \ldots, e_k\}$ – базис множини розв'язків СЛОДР, яка відповідає S'. Побудуємо рівняння

$$L_q(e_1')y_1 + \ldots + L_q(e_m')y_m = b_q.$$

Якщо всі $L_q(e_i') = 0$, то дане рівняння не має розв'язків, а разом з ним не має розв'язків і початкова СЛНДР (в цьому випадку $L_q(x)$ лінійно залежить від $L_1'(x), \ldots, L_{q-1}'(x)$). Якщо хоча б одне $L_q(e_i') \neq 0$, то розв'язок завжди існує і нехай $y = (d_1, \ldots, d_m)$ – розв'язок цього ЛОДР. Тоді вектор $x^1 = d_1e_1' + \ldots + d_me_m'$ є окремим розв'язком рівняння $L_q(x) = b_q$. Отже, загальний розв'язок СЛОДР S', а разом з ним і розв'язок системи S, подається у вигляді

$$u = x^1 + \sum_{i=1}^{k} b_i e_i,$$

де $e_i \in B, i = 1, 2, \ldots, k$.

Підсумовує сказане таке твердження.

Теорема 3. СЛНДР S, всі рівняння якої лінійно незалежні і розмірність якої $q \times n$, при $q < n$ завжди сумісна над полем F_p і її загальний розв'язок має вигляд $u = x^1 + \sum_{i=1}^{k} b_i e_i$, де x^1 – деякий окремий розв'язок S, а e_i – базисні вектори множини розв'язків СЛОДР, яка відповідає даній СЛНДР S.

Часова складність побудови загального розв'язку СЛНДР пропорціональна величині ql^3, де q – кількість рівнянь у системі, $l = \max(m, n)$, m – кількість разрядів у двійковому зображенні модуля p, а n – число невідомих в СЛНДР.

Приклад 4. Знайти в полі F_3 базис множини розв'язків СЛНДР

$$S = \begin{cases} 2x_1 + x_2 + 0x_3 + x_4 + 2x_5 = 2, \\ x_1 + 2x_2 + 1x_3 + 0x_4 + x_5 = 1, \\ x_1 + x_2 + 2x_3 + 2x_4 + 0x_5 = 2. \end{cases}$$

Розв'язання. СЛОДР S' для цієї системи отримуємо шляхом почленного віднімання третього рівняння (хоча краще було б почленно додавати друге рівняння до першого і третього) з відповідним коефіцієнтом від першого і другого рівнянь, тобто

$$S' = \begin{cases} x_1 + 0x_2 + 1x_3 + 2x_4 + 2x_5 = 0, \\ x_1 + 0x_2 + 0x_3 + 1x_4 + 2x_5 = 0, \\ x_1 + x_2 + 2x_3 + 2x_4 + 0x_5 = 2. \end{cases}$$

Базис B' підсистеми, що складається з перших двох рівнянь, включає такі вектори:

$$e_1' = (1,0,0,0,1),\ e_2' = (0,1,0,0,0),\ e_3' = (0,0,1,2,2).$$

Будуємо ЛОДР $L_3(e_1')y_1 + L_3(e_2')y_2 + L_3(e_3')y_3 = 2$, тобто $y_1 + y_2 + 0y_3 = 2$.

Знаходимо його корені шляхом розв'язання порівняння $1x \equiv 2\,(mod\ 3)$: $x_1' = (2,0,0)$, $x_2' = (0,2,0)$.

Вибираємо один із отриманих векторів, наприклад, другий. Цьому вектору відповідає окремий розв'язок $x^1 = (0,2,0,0,0)$.

В прикладі 2.5.2 знайдений базис множини розв'язків СЛОДР, що відповідає даній СЛНДР S: $s_1 = (2,1,2,1,0),\ s_2 = (1,2,0,0,1)$. Отже, загальний розв'язок СЛНДР приймає вигляд: $u = x^1 + b_1 s_1 + b_2 s_2$.

Наприклад, коли $b_1 = b_2 = 1$, то отримуємо $u_1 = (0,2,2,1,1)$. ♠

На закінчення підрозділу наведемо висновок загального характеру. Оскільки поле F_p є простим (тобто, полем, яке не має власних підполів), а кожне просте скінченне поле ізоморфне відповідному полю F_p [2], то наведені алгоритми застосовні в кожному скінченному простому полі.

2.3. Системи лінійних рівнянь в примарному кільці Z_{p^y}

Нехай дано ЛОДР в кільці Z_{p^y}

$$L(x) = a_1x_1 + \ldots + a_ix_i + \ldots + a_nx_n = 0, \qquad (15)$$

де $a_i, x_i \in Z_{p^y}$, $y > 1$, p – просте число, $i = 1,\ldots,n$, які задовольняють таку умову.

Умова 1. Серед коефіцієнтів ЛОДР існує коефіцієнт, який взаємно простий з модулем $m = p^y$.

Зауважимо, що для такого типу ЛОДР справедлива лемма 1. Припустимо, що в даному ЛОДР коефіцієнтом, який задовольняє умові 1, є перший ненульовий коефіцієнт a_k, $k \in [1,n]$. Розглянемо функцію $L(x) = a_1x_1 + a_2x_2 + \ldots + a_nx_n$ ЛОДР (15). Замінимо в ній перший ненульовий коефіцієнт a_k, який взаємно простий з модулем, його протилежним $-b_k$ і побудуємо множину векторів

$$B = \{(0,\ldots,a_j,0,\ldots,0,b_k,0,\ldots,0)\} \cup M_0,$$

де $M_0 = \{e_r : L(e_r) = 0\}$, $a_j \not\asymp 0$, а b_k є j-ю координатою у векторах із B. Причому, якщо для деякого a_j НСД$(a_j, b_k) \not\asymp 1$, то скоротимо координати такого вектора на цей спільний дільник. Отже, можна вважати, що всі вектори в множині B такі, що a_j і b_k взаємно прості. Побудована

таким чином множина також будемо називати TSS. Очевидно, що вектори із множини B є розв'язками ЛОДР (15).

Лема 5. Якщо $d = (0,\ldots,0,d_i,0,\ldots,0,d_j,0,\ldots,0)$ – розв'язок ЛОДР (15), то він або є елементом B, або представляється у вигляді невід'ємної лінійної комбінації векторів із B.

Доведення. Якщо $d \in B$, то доводити нічого. Якщо $d = (0,\ldots\ \ldots,0,d_i,0,\ldots\ \ldots,0,d_j,0,\ldots,0) \notin B$, то можливі два випадки.

Випадок 1. В множині B існують вектори $s_1 = (0,\ldots,0,a_{i'},\ 0,\ldots,0,a_{k'},0,\ldots,0)$ і $s_2 = (0,\ldots,0,\ a_{j'},0,\ldots,0,a_{k'},0,\ldots,0)$, в яких $a_{i'}$ і $a_{j'}$ є k-ми координатами, а $a_{k'}$ в s_1 і s_2 є відповідно i-ю і j-ю координатами. Оскільки s_1 і s_2 – розв'язки ЛОДР (15), то $s = us_1 + vs_2 = (0,\ldots,0,a_iu + a_jv,0,\ldots,0,d_i,0,\ldots,0,d_j,0,\ldots,0)$ теж є розв'язком цього ЛОДР, де u,v – розв'язок порівнянь $a_{k'}x \equiv d_i \ (mod\ m)$ і $a_{k'}y \equiv d_j \ (mod\ m)$ відповідно. В кільці Z_m розв'язки u і v єдині на підставі взаємної простоти $a_{k'}$ і $m = p^y$. Покажемо, що $a_iu + a_jv = 0$. Для цього підставимо вектор s в ЛОДР (15):

$$L(s) = a_{k'}(a_iu + a_jv) + a_id_i + a_jd_j = a_{k'}(a_iu + a_jv) + 0 = a_{k'}(a_iu + a_jv) = 0.$$

Оскільки $a_{k'} \neq 0$ і не є дільником нуля, то $a_iu + a_jv = 0$, що і потрібно було показати.

Випадок 2. В множині B існує вектор $s_1 = (0,\ldots,0,a_{i'},\ 0,\ldots,0,a_{k'},0,\ldots,0)$. Розглянемо вектор $s = ys_1 = (0,\ldots,0,ya_{i'},0,\ldots,0,d_j,0,\ldots,0)$, де y – єдиний розв'язок порівняння $a_{k'}y \equiv d_j \ (mod m)$. Оскільки x і s – розв'язки ЛОДР (15), то $d - s$ теж буде розв'язком цього ЛОДР, тобто $d - s = (0,\ldots,0,d_i - a_{i'}y,0,\ldots,0)$ і $L(d - s) = a_{k'}(d_i - a_{i'}y) = 0$. Оскільки $a_{k'} \neq 0$ і не є дільником нуля, то $d_i = a_{i'}y$. ■

Теорема 4. Множина В розв'язків ЛОДР (15), побудована комбінуванням протилежного до першого ненульового коефіцієнта, що задовольняє умові 1, з рештою ненульових коефіцієнтів і поповнена векторами канонічного базиса, які відповідають нульовим коефіцієнтам ЛОДР (15), є базисом множини всіх розв'язків цього ЛОДР.

Складність алгоритма побудови базиса пропорціональна величині l^3, де $l = \max(t,n)$, $t = \log m$ – кількість двійкових розрядів числа m, а n – кількість невідомих в ЛОДР.

Доведення проводиться індукцією за числом k ненульових координат у розв'язку ЛОДР. Нехай $x = (x_1,x_2,\ldots,x_n)$ – довільний розв'язок ЛОДР (15).

Базис індукції. Якщо $k = 1$, то x має збігатися з одним із векторів канонічного базису (який за побудовою є елементом B) або збігатися з одним із векторів, у якого ненульова координата є дільником нуля в кільці Z_m. Перший випадок очевидний. У другому випадку вектор має вигляд $(0,\ldots,0,c_j,0,\ldots,0)$. Виберемо розв'язок з B, в якого j-а координата $a_{k'}$ не дорівнює нулю (такий розв'язок має існувати за побудовою множини B). Нехай це буде вектор $s_1 = (0,\ldots,0,a_{i'},0,\ldots,0,a_{k'},0,\ldots,0)$. Розглянемо вектор $z = ys_1$, де y – розв'язок порівняння $a_{k'}y \equiv c_j \ (mod\ m)$ (такий розв'язок існує і єдиний на підставі взаємної простоти $a_{k'}$ і $m = p^y$).

Але тоді вектор $z-x$ буде мати єдину ненульову координату $ya_{i'}$ і при підстановці його в $L(x)$ дістаємо $ya_{i'}a_k n \equiv 0\,(mod m)$, тобто число $c_j a_{i'} = 0\,(mod\ m)$. Отже, $x = z$.

При $k = 2$ справедливість теореми випливає з леми 5.

Крок індукції. Припустимо, що теорема справедлива для всіх $1 \le k < n$ і вектор-розв'язок x має n ненульових координат. Розглянемо ненульові координати x_i, x_j вектора x. Можливі такі випадки.

Випадок 1. У B є вектор канонічного базиса s з i-ю координатою рівною одиниці. Тоді вектор $y = x - x_i s$ буде мати $n-1$ ненульових координат. За припущенням індукції для цього вектора існує зображення $x - x_i s = d_1 e_1 + \ldots + d_p e_p$, де $e_i \in B, i = 1,\ldots, p$. Але тоді $x = x_i s + d_1 e_1 + \ldots + d_p e_p$.

Випадок 2. У B є вектор канонічного базиса s з єдиною ненульовою j-ю координатою равною a, тобто a – дільник нуля в Z_m. Виберемо розв'язок із B, в якому j-а координата $a_{k'}$ не дорівнює нулю (такий розв'язок має існувати за побудовою множини B). Нехай це буде вектор $s_1 = (0,\ldots,0,a_{i'},0,\ldots,0,a_{k'},0,\ldots,0)$. Розглянемо вектор $z = ds_1$, де d – розв'язок порівняння $a_{k'} y \equiv c_j\ (mod\ m)$ (такий розв'язок існує і єдиний на підставі взаємної простоти $a_{k'}$ і m). Але тоді вектор $x - z$ буде мати на одну ненульову координату менше, ніж x. За припущенням індукції вектор $x - z$ має зображення (від'ємні координати заміняються своїми додатними протилежними)

$$x - z = d_1 e_1 + \ldots + d_p e_p \text{ або } x = ds_1 + d_1 e_1 + \ldots + d_p e_p .$$

Випадок 3. У B є вектор $s = (0,\ldots,0,a_{j'},0,\ldots,0,a_{k'},0,\ldots,0)$ з k-ю і j-ю ненульовими координатами. Розглянемо вектор

$$x - us = (x_1,\ldots,x_{k-1},x_k - ua_{j'},x_{k+1},\ldots,0,\ldots,x_n),$$

де u – розв'язок порівняння $a_{k'}u \equiv x_j\ (mod\ m)$. Побудований вектор має $n-1$ ненульових координат і за припущенням індукції отримуємо, що

$$x - us = d_1 e_1 + \ldots + d_p e_p \text{ або } x = us + d_1 e_1 + \ldots + d_p e_p .$$

Випадок 4. У B є вектори $s_1 = (0,\ldots,0,a_{i'},0,\ldots,0,a_{k'},0,\ldots,0)$ і $s_2 = (0,\ldots,0,a_{j'},0,\ldots,0,a_{k'},0,\ldots,0)$ з i-ю, j-ю і k-ю ненульовими координатами. Побудуємо вектор

$$s = a_{j'}s_1 - a_{i'}s_2 = (0,\ldots,0,a_{k'}a_{j'},0,\ldots,0,-a_{k'}a_{i'},0,\ldots,0),$$

у якого після заміни $-a_{k'}a_{i'}$ його додатними протилежними ненульовими координатами будуть координати з номерами i і j. Очевидно, що вектор s є розв'язком ЛОДР (15), і тоді на підставі леми 5 він виражається через вектори із множини B. Нехай $s' = (0,\ldots,0,b_j,0,\ldots,0,b_i,0,\ldots,0)$ і $s' = d_1 e_1 + \ldots + d_r e_r$ ці вирази. Далі доведення зводиться до вищерозглянутого випадку 3.

При отриманні оцінки складності елементарними вважаються операції додавання і віднімання (арифметична складність виконання яких пропорціональна t). При побудові множини *TSS* для ЛОДР обчислюється $n-1$ вектор і не більше, ніж $n-1$ разів обчислюється НСД двох чисел в кільці Z_m. Побудова векторів потребує, очевидно, не більше ніж $n \cdot (n-1)$ операцій, а складність обчислення НСД за допомогою алгоритма Евкліда пропорціональна t^2, де t – розрядність чисел

в двійковому зображенні, для яких обчислюється НСД [6, 7]. Додаючи всі ці величини, дістаємо l^3, де $l = \max(t,n)$. ■

Наслідок 1. Якщо модуль m є простим числом, то множина В розв'язків ЛОДР (15) є базисом множини всіх розв'язків цього ЛОДР.

Складність алгоритма побудови цього базиса пропорціональна величині l^3, де $l = \max(t,n)$, $t = \log m$ – число двійкових розрядів простого числа m, а n – кількість невідомих в ЛОДР.

Дійсно, якщо модуль m – просте число, то умова 1 виконується автоматично.

Приклад 5. Побудувати базис множини всіх розв'язків ЛОДР $2x_1 + 5x_2 + 7x_3 + 3x_4 + 6x_5 = 0$ в кільці Z_{12}.

Розв'язання. Вибираємо ненульовий коефіцієнт 7, який взаємно простий з модулем 12, замінюємо його протилежним –5 і отримуємо ЛОДР $2x_1 + 5x_2 - 5x_3 + 3x_4 + 6x_5 = 0$. Застосовуючи *TSS*-метод, знаходимо такі базисні розв'язки: $e_1 = (5,0,2,0,0)$, $e_2 = (0,1,1,0,0)$, $e_3 = (0,0,3,5,0)$, $e_4 = (0,0,6,0,5)$. ♠

Випадок ЛНДР. Нехай дано ЛНДР

$$a_1x_1 + \ldots + a_kx_k + \ldots + a_nx_n = b, \tag{16}$$

в якому коефіцієнт a_k взаємно простий з модулем m. Знайдемо розв'язок порівняння $a_k y \equiv b \,(mod\ m)$, який за даних умов буде єдиним. Нехай цим числом буде c, тобто вектор $x^1 = (0,\ldots\ \ldots,0,c,0,\ldots,0)$ буде розв'язком (16). Застосовуючи *TSS*-метод до ЛОДР, яке відповідає (16), знаходимо базис B множини його розв'язків.

Нехай $x^1 = (c_1, c_2, \ldots, c_n)$ – деякий окремий розв'язок (16), знайдений описаним вище способом, а $B = \{e_1, e_2, \ldots, e_m\}$ – базис множини розв'язків ЛОДР

$$a_1x_1 + a_2x_2 + \ldots + a_nx_n = 0. \tag{17}$$

Теорема 5. Довільний розв'язок ЛНДР (16) має вигляд $u = x^1 + \sum_{i=1}^{m} b_i e_i$, де x^1 – окремий розв'язок ЛНДР (16), а $e_1, \ldots, e_m$ – базисні вектори множини розв'язків ЛОДР (17), яке відповідає ЛНДР (16).

Доведення. Нехай $u = (u_1, u_2, \ldots, u_n)$ – довільний розв'язок ЛНДР (16), а $B = \{e_1, e_2, \ldots, e_m\}$ – базис множини розв'язків ЛОДР, яке відповідає (16). Розглянемо вектор $y = u - x^1 = (d_1, d_2, \ldots, d_n)$. Якщо деякі координати у векторі y стали від'ємними, то замінимо їх додатними протилежними. Вектор y є розв'язком ЛОДР і тому представляється у вигляді невід'ємної лінійної комбінації векторів із B, тобто $y = \sum_{i=1}^{m} b_i e_i$, $e_i \in B, i = 1,2,\ldots,m$. Але тоді $u = x^1 + \sum_{i=1}^{m} b_i e_i$. ■

Приклад 6. Знайти в кільці F_{12} загальний розв'язок ЛНДР $2x + 3y + 5z + 6u + 4v = 7$.

Розв'язання. Вибираємо ненульовий коефіцієнт $a_3 = 5$, який взаємно простий з 12. Розв'язуємо порівняння $5s \equiv 7(mod\ 12)$. Розв'язком цього порівняння є $s = 11$. Тоді вектор $x^1 = (0,0,11,0,0)$ є шуканим окремим розв'язком ЛНДР.

Знайдемо базис множини розв'язків ЛОДР $2x+3y+5z+6u+4v=0$. Для цього замінимо коефіцієнт 5 його протилежним –7 і побудуємо базис множини розв'язків ЛОДР $2x+3y-7z+6u+4v=0$. Цими розв'язками будуть вектори

$$e_1=(7,0,2,0,0),\ e_2=(0,7,3,0,0),\ e_3=(0,0,6,7,0),\ e_4=(0,0,4,0,7).$$

Отже, загальний розв'язок даного ЛНДР матиме вигляд $x=x^1+b_1e_1+b_2e_2+b_3e_3+b_4e_4$.

Наприклад, при $b_1=2, b_2=7, b_3=b_4=0$ дістаємо $u=(2,1,0,0,0)$. ♠

Розглянемо ЛОДР загального вигляду над примарним кільцем Z_m

$$L(x)=a_1x_1+\ldots+a_ix_i+\ldots+a_nx_n=0, \tag{18}$$

де $a_i, x_i\in Z_m, m=p^y, y>1, y\in N, i=1,\ldots,n$. Нехай НСД$(a_1,a_2,\ldots,a_n,m)=p^u$, тоді, скорочуючи (18) на p^u, дістаємо ЛОДР

$$b_1x_1+b_2x_2+\ldots+b_nx_n=0 \tag{19}$$

над примарним кільцем $Z_{m'}$, де $m'=p^v, v=y-u$.

Отримане рівняння має ту властивість, що довільний розв'язок ЛОДР (18) буде розв'язком ЛОДР (19). Обернене твердження не має місця. Дійсно, нехай b_1 в (19) взаємно простий з модулем m'. Тоді будуємо TSS цього ЛОДР, яке на підставі теореми 4 буде базисом його множини розв'язків:

$$s_1=(b_2,c,0,0,0,\ldots,0), s_2=(b_3,0,c,0,,0\ldots,0),$$

$$s_3=(b_4,0,0,c,0,\ldots,0),\ldots,s_{n-1}=(b_n,0,0,0,\ldots,0,c),$$

де $c=b_1-p^v$ – протилежний до коефіцієнта b_1. Оскільки кільце Z_m з дільниками нуля, то очевидним розв'язком (18) буде вектор $s_n=(p^v,0,0,\ldots,0)$, який не виражається невід'ємною лінійною комбінацією векторів із TSS, так як $c\cdot x\equiv 0(mod\ p^v)$ тоді і тільки тоді, коли $x=p^v$ на підставі взаємної простоти c і p^v.

Справедлива

Теорема 6. *TSS* рівняння (19), серед коефіцієнтів якого є коефіцієнти, які задовольняють умові 1, доповнена вектором $s_n=(p^v,0,0,\ldots,0)$, складає базис множини розв'язків ЛОДР (18).

Доведення. Нехай $x=(d_1,d_2,\ldots,d_n)$ – довільний розв'язок рівняння (18). Побудуємо вектор $y=c_1s_1+\ldots+c_{n-1}s_{n-1}=(c_1b_2+\ldots+c_{n-1}b_n,d_2,\ldots,d_n)$, тобто $d_i\equiv c_i\cdot c(mod\ m'), i=2,\ldots,n$, $c=b_1-p^v$, і розглянемо вектор

$$y-x-c_ns_n=(c_1b_2+\ldots+c_{n-1}b_n-d_{1'},0,\ldots,0)=(c_1b_2+\ldots,c_{n-1}b_n+d_{1''},0,\ldots,0),$$

де $d_{1''}$ – протилежний до $d_{1'}c_n\equiv d_{1''}\ (mod\ m')$. Отриманий вектор є розв'язком (18), а отже, є розв'язком (19). Подамо $d_{1''}$ у вигляді b_1d, де $b_1d\equiv d_{1''}\ (mod\ p^v)$ (таке подання єдине на підставі взаємної простоти b_1 і p^v). Тоді $y-x-c_ns_n=(c_1b_2+\ldots+c_{n-1}b_n+b_1d'',0,\ldots,0)$, і після підстановки $y-x$ в ЛОДР (19) дістаємо

$$b_1(b_1d''+b_2c_1+\ldots,b_nc_{n-1})\equiv 0\ (mod\ p^v).$$

Отже, можливі два випадки:

а) $b_1d'' + b_2c_1 + \ldots, b_nc_{n-1} = gp^l \equiv 0(mod\ p^y)$;

б) $b_1d'' + b_2c_1 + \ldots, b_nc_{n-1} = gp^l \not\equiv 0(mod\ p^y)$.

У випадку а) доводити нічого. У випадку б) для остаточного подання вектора x необхідно від вектора $x - y$ відняти вектор gs_n: $x - y - (c_n + g)s_n = 0$ і $x = y + (c_n + g)s_n$. ■

Якщо для ЛОДР не виконується умова 1, то цього завжди можна досягти. Це випливає з такого простого твердження.

Лема 6. ЛОДР (19) задовольняє умові 1, тобто в цьому рівнянні існує принаймні один коефіцієнт, який взаємно простий з модулем $m = p^y$.

Доведення. Розглянемо довільний ненульовий коефіцієнт a_i ЛОДР (18). Якщо a_i і m взаємно прості, то доведення не потрібне. Якщо таких коефіцієнтів немає, тобто НСД$(a_1, a_2, \ldots, a_n, m) = p^u, u < y$, то скорочуючи на p^u коефіцієнти і модуль, дістаємо рівняння, яке еквівалентне початковому і для якого виконується умова 1. ■

Звідси випливає, що ЛОДР (19) задовольняє умові 1. Тоді базис множини розв'язків перетвореного ЛОДР будується *TSS* -алгоритмом.

2.4. *TSS*-метод розв'язання СЛОДР

З вищенаведених теорем випливає така процедура побудови базиса множини розв'язків СЛОДР над примарним кільцем Z_m, де $m = p^y$. Вона зводиться до розв'язання ЛОДР в примарному кільці Z_m за допомогою *TSS* -метода. Проілюструємо це на прикладах.

Приклад 7, а) побудувати базис множини всіх розв'язків в кільці Z_8 для СЛОДР

$$S = \begin{cases} 2x + 3y + 8z + 6u + 4v = 0, \\ 4x + 6y + 2z + 3u + 2v = 0, \\ 2x + 3y + 2z + 2u + 8v = 0. \end{cases}$$

Розв'язання. В результаті приведення коефіцієнтів системи отримуємо СЛОДР:

$$S_1 = \begin{cases} L_1 = 2x + 3y + 0z + 6u + 4v = 0, \\ L_2 = 4x + 6y + 2z + 3u + 2v = 0, \\ L_3 = 2x + 3y + 2z + 2u + 0v = 0. \end{cases}$$

Будуємо базис B СЛОДР S_1, вибираючи коефіцієнт $a_{12} = 3$ і його протилежний $b = -5$:

$$B_1 = \{e_1 = (5,2,0,0,0), e_2 = (0,0,1,0,0), e_3 = (0,6,0,5,0), e_4 = (0,4,0,0,5)\}.$$

Значення L_2 на векторах із B_1: 0, 2, 3, 2. Дістаємо порівняння $0d_1 + 2d_2 + 3d_3 + 2d_2 = 0\ (mod\ 8)$, яке має базисні розв'язки (1,0,0), (0,5,2,0), (0,0,2,5). Цим розв'язкам відповідають базисні вектори

$$B_2 = \{s_1 = 1 \cdot e_1 = (5,2,0,0,0), s_2 = 5e_2 + 2e_3 = (0,4,5,2,0),$$
$$s_3 = 2e_3 + 5e_4 = (0,0,0,2,1)\}.$$

Значення L_2 на векторах із B_2: 0, 2, 4. Дістаємо порівняння $0d_1 + 2d_2 + 4d_3 = 0\ (mod\ 8)$, яке має розв'язки (1,0,0), (0,2,3) і (0,4,0) (скільки НСД(2,4) = 2). Цим розв'язкам відповідають базисні вектори початкової системи S

$$B = \{v_1 = 1 \cdot s_1 = (5,2,0,0,0), v_2 = 4s_2 = (0,0,4,0,0), v_3 = 2s_2 + 3s_3 = (0,0,2,2,3)\}.$$

б) побудувати базис множини всіх розв'язків в кільці Z_{24} для СЛОДР

$$S = \begin{cases} 2x + 3y + 8z + 6u + 4v = 0, \\ 4x + 6y + 2z + 3u + 2v = 0, \\ 2x + 3y + 2z + 2u + 8v = 0. \end{cases}$$

Розв'язання. В результаті розкладу модуля $m = 24 = 3 \cdot 8$ дістаємо дві СЛОДР:

$$S_1 = \begin{cases} L_{11} = 2x + 0y + 0z + 0u + 1v = 0, \\ L_{12} = 1x + 0y + 2z + 0u + 2v = 0, \\ L_{13} = 2x + 0y + 2z + 2u + 2v = 0, \end{cases}$$

$$S_2 = \begin{cases} L_{21} = 2x + 3y + 0z + 6u + 4v = 0, \\ L_{22} = 4x + 6y + 2z + 3u + 2v = 0, \\ L_{23} = 2x + 3y + 2z + 2u + 0v = 0. \end{cases}$$

Розв'язки СЛОДР S_1 знаходимо в полі F_3, а СЛОДР S_2 – в примарному кільці Z_8.

Будуємо базис B_1 СЛОДР S_1: $B_{11} = \{(2,0,1,0,0),(0,1,0,0,0),(0,0,0,1,0),(1,0,0,0,1)\}$.

Значення L_{12} на векторах із B_{11}: 1,0,0,0. Тоді $B_{12} = \{(0,1,0,0,0),(0,0,0,1,0),(1,0,0,0,1)\}$.

Значення L_{13} на векторах із B_{12}: 0,2,1. Тоді $B_1 = B_{13} = \{(0,1,0,0,0),(1,0,0,1,1)\}$.

Базис B_2 СЛОДР S_2 вищепобудований у п. а):

$$B_2 = \{(5,2,0,0,0),(0,0,2,2,3)\} \cup \{(0,0,4,0,0)\}.$$

Таким чином, остаточно отримуємо базис множини розв'язків початкової СЛОДР

$$B = 8 \cdot B_1 \cup 3 \cdot B_2 = \{(0,8,0,0,0),(8,0,0,8,8),(15,6,0,0,0),(0,0,6,6,9),(0,0,12,0,0)\}. \spadesuit$$

В загальному випадку, якщо модуль m має розклад, який включає більше двох множників, тобто $m = p_1^{y_1} p_2^{y_2} \dots p_r^{y_r}$, то отримуємо r підсистем. Приймаючи до уваги те, що арифметична складність виконання операцій додавання і віднімання в кільці Z_m пропорціональна s (s – максимальна розрядність чисел), операцій множення і ділення, як і обчислення НСД двох чисел, менших від m – s^2, то арифметична складність побудови базиса множини розв'язків СЛОДР має такі складові:

- l^3 – розв'язок одного ЛОДР і розв'язок одного проміжного ЛОДР;
- $n^2 l^3$ – обчислення значень і скорочення на НСД $L(x)$;
- $n^2 l^3$ – побудова комбінацій векторів, які складають базис множини розв'язків ЛОДР ($l = \max(n, s)$).

Отже, арифметична складність переходу від попереднього до наступного ЛОДР в одній підсистемі пропорціональна величині l^5, де $l = \max(n, s, r), s = \log m$. Така процедура повторюється r разів і в результаті маємо $O(l^6)$, де $l = \max(n, s, r)$. Іншими словами, має місце наступна

Теорема 7. Множина B, побудована *TSS* -методом, є базисом множини розв'язків СЛОДР (4). Арифметична складність побудови B пропорціональна величині $O(l^6)$, де $l = \max(n, s, r)$.

2.5. *TSS*-метод розв'язання СЛНДР

Побудова базиса множини розв'язків СЛНДР зводиться до пошуку окремого розв'язку СЛНДР і базиса множини розв'язків відповідної СЛОДР. Ця побудова виконується шляхом переходу до розширенної СЛОДР, у якої до початкової СЛОДР додається стовпчик з вільних членів з додатковим невідомим. Побудувавши базис множини розв'язків такої СЛОДР, виділяємо базисні розв'язки, у яких остання координата (вона відповідає додатковій невідомій) відмінна від нуля. Якщо таких координат немає, то початкова СЛНДР несумісна. В протилежному випадку складаємо порівняння

$$c_1 z_1 + \ldots + c_r z_r = 1 (mod\ m), \tag{20}$$

де $c_1, \ldots, c_r$ – значення останніх ненульових координат виділенних векторів. Якщо це порівняння не має розв'язків, то початкова СЛНДР несумісна, в протилежному випадку за одним із його розв'язків будуємо окремий розв'язок СЛНДР, який разом з базисними розв'язками СЛОДР, що відповідає дані СЛНДР, утворює базис множини всіх розв'язків початкової СЛНДР.

Приклад 8. Знайти базис множини всіх розв'язків у кільці Z_{24} для СЛНДР

$$S = \begin{cases} 2x + 3y + 8z + 6u = 20, \\ 4x + 6y + 2z + 3u = 22, \\ 2x + 3y + 2z + 2u = 16. \end{cases}$$

Розв'язання. Від цієї СЛНДР переходимо до розширеної СЛОДР

$$S = \begin{cases} 2x + 3y + 8z + 6u + 4v = 0, \\ 4x + 6y + 2z + 3u + 2v = 0, \\ 2x + 3y + 2z + 2u + 8v = 0, \end{cases}$$

у якої останній стовпчик відповідає вільним членам з додатковим невідомим v. Базис множини розв'язків даної СЛОДР знайдений у попередньому прикладі

$$B = 8 \cdot B_1 \cup 3 \cdot B_2 = \{(0,8,0,0,0), (8,0,0,8,8), (15,6,0,0,0), (0,0,6,6,9), (0,0,12,0,0)\}.$$

Виділяємо вектор (8,0,0,8,8) і вектор (0,0,6,6,9) з ненульовими останніми координатами і будуємо порівняння $8x + 9y = 1 (mod 24)$ за цими останніми координатами виділених векторів. Це порівняння має розв'язок (-1,1) = (23,1), якому відповідає окремий розв'язок початкової СЛОДН $x^1 = (16,0,6,22)$. Тоді загальний розв'язок початкової СЛНДР набуває вигляду: $x = x^1 + a(0,8,0,0) + b(15,6,0,0) + c(0,0,12,0)$, де $a, b, c \in Z_{24}$ – довільні сталі. ♠

Можна запропонувати і такий спосіб пошуку загального розв'язку СЛНДР, який виконується за такою послідовністю кроків:

1) $i = 1$;

2) Знайти окремий розв'язок x^1 ЛНДР $L_i(x) = b_i$. Якщо x^1 не існує, то (СТОП: розв'язків немає), інакше на крок 3);

3) Побудувати базис $B_i = \{e_{i1}, e_{i2}, \ldots, e_{iw}\}$ ЛОДР, яке відповідає ЛНДР $L_i(x) = b_i$;

4) Знайти $c = L_{i+1}(x^1), c_1 = L_{i+1}(e_{i1}), \ldots, c_w = L_{i+1}(e_{iw})$, де $e_{ij} \in B_i$, $j = 1,2,\ldots,w$;

5) Знайти окремий розв'язок y^1 ЛНДР

$$c_1 y_1 + \ldots + c_w y_w = b_{i+1} - c. \tag{21}$$

Якщо y^1 не існує, то (СТОП: розв'язків немає), інакше на крок 6);

6) Побудувати базис $B_{i'}$ ЛОДР, яке відповідає (21);

7) Побудувати базис B_{i+1} для ЛНДР $L_{i+1}(x) = b_{i+1}$, виходячи з $B_{i'}$;

8) Якщо $i+1 < r$, то ($i = i+1$; на крок 4)), інакше (СТОП: друкувати B_{i+1}).

Правильність цієї процедури випливає з доведених вище теорем і лем.

Приклад 9, а) знайти в кільці Z_{12} загальний розв'язок СЛНДР

$$S = \begin{cases} 2x_1 + 3x_2 + 8x_3 + 6x_4 + 4x_5 = 8 \\ 4x_1 + 3x_2 + 6x_3 + 6x_4 + 8x_5 = 6 \end{cases}.$$

Розв'язання. Розширена СЛОДР для даної СЛНДР має вигляд:

$$S' = \begin{cases} 2x_1 + 3x_2 + 8x_3 + 6x_4 + 4x_5 + 4x_6 = 0, \\ 4x_1 + 3x_2 + 6x_3 + 6x_4 + 8x_5 + 6x_6 = 0. \end{cases}$$

Оскільки розклад 12 на прості множники має вигляд $m = 12 = 3 \cdot 4$, то побудова базиса множини розв'язків розширеної СЛОДР розпадається на дві підсистеми:

$$S_1 = \begin{cases} 2x_1 + 0x_2 + 2x_3 + 0x_4 + 1x_5 + 1x_6 = 0, \\ 1x_1 + 0x_2 + 0x_3 + 0x_4 + 2x_5 + 0x_6 = 0, \end{cases}$$

розв'язки якої шукаються в полі F_3 і

$$S_2 = \begin{cases} 2x_1 + 3x_2 + 0x_3 + 2x_4 + 0x_5 + 0x_6 = 0, \\ 0x_1 + 3x_2 + 2x_3 + 2x_4 + 0x_5 + 2x_6 = 0, \end{cases}$$

розв'язки якої шукаються в примарному кільці Z_4.

Базис множини розв'язків системи S_1 складають вектори:

$$B_{1'} = \{(0,1,0,0,0,0),(1,0,0,0,1,0),(0,0,0,1,0,0),(0,0,1,0,0,1)\}.$$

Базис множини розв'язків системи S_2 складають вектори:

$$B_{2'} = \{(1,2,1,0,0,0),(1,2,0,0,0,1),(0,2,0,1,0,0),(0,0,0,0,1,0),(2,0,0,0,0,0)\}.$$

Тоді базис множини розв'язків розширеної СЛОДР для даної СЛНДР приймає вигляд:

$$B = 12/3B_{1'} \cup 12/4B_{2'} = 4B_{1'} \cup 3B_{2'} = \{s_1 = (0,4,0,0,0,0),$$
$$(s_2 = (4,0,0,0,4,0), s_3 = (0,0,4,0,0,4), s_4 = (0,0,0,4,0,0), v_1 = (3,6,3,0,0,0),$$
$$v_2 = (3,6,0,0,0,3), v_3 = (0,6,0,3,0,0), v_4 = (6,0,0,0,0,0), v_5 = (0,0,0,0,3,0)\}.$$

Складаємо порівняння за останніми координатами розв'язків s_3 і v_2: $3x + 4y \equiv 1 (mod\ 12)$. Це порівняння має єдиний розв'язок $(u_1, u_2) = (11,1)$, що дає окремий розв'язок СЛНДР

$$x^1 = 11(3,6,0,0,0) + (0,0,4,0,0) = (33,66,4,0,0) = (9,6,4,0,0).$$

Таким чином, загальний розв'язок СЛНДР має вигляд:

$$x = x^1 + a_1 s_1 + a_2 s_2 + a_3 s_4 + b_1 v_1 + b_2 v_3 + b_3 v_4 + b_4 v_5,$$

де $a_i \in F_3, b_j \in Z_4$.

б) знайти в кільці Z_{12} загальний розв'язок СЛНДР

$$S = \begin{cases} 2x_1 + 3x_2 + 8x_3 + 6x_4 + 4x_5 = 8, \\ 4x_1 + 3x_2 + 6x_3 + 6x_4 + 8x_5 = 5. \end{cases}$$

Розв'язання. Загальний розв'язок першого ЛНДР був знайдений в попередньому прикладі: $x = x^1 + \sum_{i=1}^{8} a_i e_i$, де $x^1 = (4,4,0,0,0)$, а

$$e_1 = (2,0,1,0,0),\ e_2 = (0,4,0,0,0),\ e_3 = (0,0,0,2,0),\ e_4 = (2,0,0,0,2),$$
$$e_5 = (3,6,0,0,0),\ e_6 = (0,2,0,1,0),\ e_7 = (0,0,3,0,0),\ e_8 = (0,0,0,0,3).$$

Підставляючи ці вектори в друге рівняння СЛНДР, дістаємо такі значення: $L_2(x^1) = 4$, а на решті векторів – значення 2, 0, 0, 0, 6, 0, 6, 0. Будуємо рівняння (для простоти пропущені нульові коефіцієнти) $2y_1 + 6y_2 + 6y_3 = 5 - 4 = 1$. Отримане рівняння не має розв'язків, оскільки НСД модуля і коефіцієнтів дорівнює 2, а 2 не ділить вільний член 1. Отже, початкова СЛНДР несумісна. ♠

Зауважимо, що наведені алгоритми мають поліноміальні оцінки часової складності за умови відомого розкладу модуля на прості множники. Проблема розкладу натурального числа на прості множники (яка називається *проблемою факторизації*) є однією з важливих проблем теорії чисел. Існує декілька алгоритмів її розв'язання: алгоритм Полларда, Полларда – Штрассена, решета числового поля [8]. Найбільш ефективним алгоритмом в даний час є останній з алгоритмів. Всі ці алгоритми мають експоненціальні оцінки часової складності, найкраща з яких для заданого числа n має вигляд $O(2^{c\sqrt{\ln n \ln\ln n}})$.

2.6. Скінченні поля та системи лінійних рівнянь над цими полями

Відомо, що виходячи з поля лишків F_p можна побудувати скінченне поле, яке має p^n елементів [2, 8, 9]. Спосіб побудови такого поля грунтується на використанні незвідного полінома над полем F_p.

Означення 1. Поліном $f(x) \in G(x)$ називається незвідним над полем G, якщо він має додатний степінь, і з рівності $f(x) = g(x) \cdot h(x)$, де $g(x), h(x) \in G(x)$, випливає, що або поліном $g(x)$ є константою, або поліном $h(x)$ є константою.

Зауважимо, що для поліномів $f(x)$ і $g(x)$, де $g(x) \neq 0$ як і при діленні цілих чисел, має місце теорема про ділення поліномів з остачею

$$f(x) = g(x) \cdot h(x) + r(x), \tag{22}$$

де $g(x), r(x) \in G(x)$ і $deg(r) < deg(g)$. Це означає, що при діленні многочленів можна застосовувати алгоритм Евкліда, подібно до того як цим алгоритмом користуються при діленні цілих чисел.

Означення 2. Нехай $f(x), g(x), h(x) \in G(x)$, де $g(x) \neq 0$, задовольняють умові (22). Тоді поліном $r(x)$ називається остачею від ділення полінома $f(x)$ на поліном $g(x)$. Цей поліном позначається як $r = f \ (mod\ g)$. Остачі від ділення всіх поліномів із множини $G(x)$ за модулем полінома $g(x)$ називаються поліномами із множини $G(x)$ за модулем полінома $g(x)$. Множина всіх таких поліномів позначимо $G_g(x)$.

Очевидно, що степені всіх поліномів із $G_g(x)$ менші $deg(g)$.

Теорема 8. Нехай G – поле, а $f(x)$ – ненульовий поліном із $G(x)$. Тоді $G_f(x)$ буде полем тоді і тільки тоді, коли f незвідний поліном над полем $G(x)$ [8–10].

Незвідний поліном $f(x)$ називається **визначальним поліномом** поля $G_f(x)$.

Теорема 9. Нехай G скінченне поле, порядок якого p, де p – просте число, а f – незвідний поліном над полем G степеня n. Тоді $|G_f(x)| = p^n$.

Доведення. Із означення поля $G_f(x)$ випливає, що множина $G(x)$ складається із поліномів, степінь яких менший $n = deg(f)$, а їх коефіцієнти належать полю G. Але таких поліномів буде p^n. ■

Наслідок 2. Для кожного простого числа p і кожного $n \in N$ існує скінченне поле, яке складається із p^n елементів.

Побудова такого поля виконується за допомогою лишків від ділення незвідного полінома над полем F_p. Реалізація алгоритму побудови полів F_{p^k} з оцінками часової складності розглядалися в роботах [8, 9], тому розглянемо лише прості приклади побудови таких полів (див. [10, 11]).

Приклад 10, а) нехай F_2 – поле лишків за модулем 2. Поліном $f(x) = x^2 + x + 1$ незвідний над полем F_2. Множина $G_f^2(x)$ є полем, яке має 2^2 елементів. Їх степені менші 2 і тому довільний елемент y із цього поля буде таким: $y = b_1 x + b_0$, де $b_i \in F_2$, $i = 0,1$. Табл. 1, 2 Келі для поля G_f^2 набувають вигляду:

ТАБЛИЦЯ 1

+	0	1	x	$x+1$
0	0	1	x	$x+1$
1	1	0	$x+1$	x
x	x	$x+1$	0	1
$x+1$	$x+1$	x	1	0

ТАБЛИЦЯ 2

*	0	1	x	$x+1$
0	0	0	0	0
1	0	1	x	$x+1$
x	0	x	$x+1$	1
$x+1$	0	$x+1$	1	x

Якщо позначити поліноми x і $x+1$ числами 2 і 3 відповідно, то табл. 3, 4 Келі для операцій набувають вигляду:

ТАБЛИЦЯ 3

+	0	1	2	3
0	0	1	2	3
1	1	0	3	2
2	2	3	0	1
3	3	2	1	0

ТАБЛИЦЯ 4

·	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	3	1
3	0	3	1	2

б) аналогічним чином будується поле і друге поле F_{3^2} над полем лишків F_3 за допомогою незвідного полінома $x^2 + x + 2$ (табл.5 і 6):

ТАБЛИЦЯ 5

+	0	1	2	3	4	5	6	7	8
0	0	1	2	3	4	5	6	7	8
1	1	2	0	4	5	3	7	8	6
2	2	0	1	5	3	4	8	6	7
3	3	4	5	6	7	8	0	1	2
4	4	5	3	7	8	6	1	2	0
5	5	3	4	8	6	7	2	0	1
6	6	7	8	0	1	2	3	4	5
7	7	8	6	1	2	0	4	5	3
8	8	6	7	2	0	1	5	3	4

ТАБЛИЦЯ 6

·	0	1	2	3	4	5	6	7	8
0	0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7	8
2	0	2	1	6	8	7	3	5	4
3	0	3	6	7	1	4	5	8	2
4	0	4	8	1	5	6	2	3	7
5	0	5	7	4	6	2	8	1	3
6	0	6	3	5	2	8	7	4	1
7	0	7	5	8	3	1	4	2	6
8	0	8	4	2	7	3	1	6	5

де x позначене числом 3, $x+1$ – числом 4, $x+2$ – числом 5, $2x$ – числом 6, $2x+1$ – числом 7, $2x+2$ – числом 8. ♠

Застосування TSS-алгоритма в таких полях, на відміну від поля, розглянутого вище F_p, вимагає наявності таблиць операцій додавання і множення.

Приклад 11. Розв'язати в полі F_{2^2} СЛОДР

$$Ax = \begin{cases} 1\ 1\ 1\ 1\ 0\ 0\ 1 \\ 1\ 1\ 1\ 0\ 1\ 0\ 2 \\ 1\ 1\ 1\ 0\ 0\ 1\ 3 \\ 1\ 0\ 0\ 1\ 1\ 1\ 0 \\ 0\ 1\ 0\ 1\ 1\ 1\ 1 \\ 0\ 0\ 1\ 1\ 1\ 1\ 1 \end{cases} \equiv 0, \qquad (23)$$

Розв'язання. Застосовуючи TSS-алгоритм, дістаємо розв'язки першого рівняння

(1,0,0,0,0,0,1), (0,1,0,0,0,0,1), (0,0,1,0,0,0,1),
(0,0,0,1,0,0,1), (0,0,0,0,1,0,0), (0,0,0,0,0,1,0).

Значення лівої частині другого рівняння, обчислені за таблицями додавання і множення в полі F_{2^2}, дорівнюють: 3,3,3,2,1,0. За цими значеннями комбінуванням першого розв'язку з рештою, дістаємо розв'язки першого і другого рівнянь системи:

(1,1,0,0,0,0,0), (1,0,1,0,0,0,0), (2,0,0,3,0,0,1), (1,0,0,0,3,0,1), (0,0,0,0,0,1,0).

Значення лівої частини третього рівняння дорівнюють: 0,0,1,2,1. За цими значениям комбінуванням останнього розв'язку з третім і четвертим, отримуємо розв'язки перших трьох рівнянь системи:

(1,1,0,0,0,0,0), (1,0,1,0,0,0,0), (2,0,0,3,0,1,1), (1,0,0,0,3,2,1).

Значення лівої частини четвертого рівняння: 1,1,0,0. За цими значеннями комбінуванням першого з другим розв'язком, дістаємо розв'язки перших чотирьох рівнянь системи:

(0,1,1,0,0,0,0), (2,0,0,3,0,1,1), (1,0,0,0,3,2,1).

Значення лівої частини п'ятого рівняння: 1,3,0. За цими значеннями комбінуванням першого з другим розв'язком, дістаємо розв'язки перших п'яти рівнянь системи:

(2,3,3,3,0,1,1), (1,0,0,0,3,2,1).

Значення лівої частини шостого рівняння: 0,0. Це означає, що обидва вектори є розв'язками початкової системи. ♠

Добре відомо, що скінченні поля однакових порядків ізоморфні між собою. Отже, наведені методи розв’язання систем лінійних рівнянь застосовні в довільному такому полі.

Висновки. В першій частині роботи наведено формулювання задачі про математичний сейф та її редукція до задачі розв’язання систем лінійних рівнянь у скінченних кільцях та полях. Розглянуто методи і алгоритми побудови базисів множини розв’язків систем лінійних рівнянь у скінченних кільцях і полях та наведені оцінки часової складності алгоритмів та особливості їх застосувань.

Розглянуті методи і алгоритми будуть застосовані до розв’язання задачі про математичний сейф, що становить предмет розгляду другої частини даної роботи.

Список літератури

1. Донец Г.А. Решение задачи о сейфе на (0,1) – матрицах. *Кибернетика и системный анализ*. 2002. **38** (1). С. 98–105.
2. Калужнин Л.А. Введение в общую алгебру. М.: Наука, 1973. 447 с.

3. Крывый С.Л. Алгоритмы решения систем линейных диофантовых уравнений в кольцах вычетов. *Кибернетика и системный анализ*. 2016. **52** (5). С. 149–160.
4. Крывый С.Л. Алгоритмы решения систем линейных диофантовых уравнений в полях вычетов. *Кибернетика и системный анализ*. 2007. **43** (2). С. 15–23.
5. Кривий С.Л. Лінійні діофантові обмеження та їх застосування. Чернівці-Київ: Букрек, 2015. 224 с.
6. Коблиц Н. Курс теории чисел и криптографии. М.: Изд-во ТВП, 2001. 260 с.
7. Черемушкин А.В. Лекции по арифметическим алгоритмам в криптографии. М.: МЦНМО, 2002. 103 с.
8. Крывый С.Л., Гогерчак Г.И. Алгоритм решения систем линейных уравнений в поле F_p^k. *Проблемы управления и информатики*. 2019. 5. С. 5–24.
9. Lidl R., Niederreiter H. Finite fields. Encyclopedia of Mathematics and its Applications. Addison-Wesley, Reading MA, 1982. **20**. P. 273–280.
10. Menezes A.J., Van Oorschot P.C., Vanstons S.A. Handbook of Applied Cryptography. CRC Press, 1996. 661 p.
11. Гаврилкевич М.В., Солодовников В.И. Эффективные алгоритмы решения задач линейной алгебры над полем из двух элементов. *Обозрение прикладной промышленной математики*. 1995. **2** (3). С. 400 – 437.

Одержано 06.11.2020

Кривий Сергій Лук'янович,
доктор фізико-математичних наук, професор кафедри інтелектуальних програмних систем
Київського національного університету імені Тараса Шевченка, Київ,
https://orcid.org/0000-0003-4231-0691
sl.krivoi@gmail.com

Гогерчак Григорій Іванович,
аспірант факультету комп'ютерних наук та кібернетики
Київського національного університету імені Тараса Шевченка, Київ.
https://orcid.org/0000-0002-6898-2536
gogerchak.g@gmail.com

MSC 12F05, 68W05

S. Kryvyi [*], H. Hoherchak

The Mathematical Safe Problem and Its Solution (Part 1)

Taras Shevchenko National University of Kyiv, Ukraine
[*] *Correspondence: sl.krivoi@gmail.com*

Introduction. The problem of the mathematical safe arises in the theory of computer games and cryptographic applications. The article considers the formulation of the mathematical safe problem and the approach to its solution using systems of linear equations in finite rings and fields.

The purpose of the article is to formulate a mathematical model of the mathematical safe problem and its reduction to systems of linear equations in different domains; to consider solving the corresponding systems in finite rings and fields; to consider the principles of constructing extensions of residue fields and solving systems in the relevant areas.

Results. The formulation of the mathematical safe problem is given and the way of its reduction to systems of linear equations is considered. Methods and algorithms for solving this type of systems are considered, where exist methods and algorithms for constructing the basis of a set of solutions of linear equations and derivative methods and algorithms for constructing the basis of a set of solutions of systems of linear equations for residue fields, ghost rings, finite rings and finite fields. Examples are given to illustrate their work. The principles of construction of extensions of residue fields by the module of an irreducible polynomial, and examples of operations tables for them are considered. The peculiarities of solving systems of linear equations in such fields are considered separately. All the above algorithms are accompanied by proofs and estimates of their time complexity.

Conclusions. The considered methods and algorithms for solving linear equations and systems of linear equations in finite rings and fields allow to solve the problem of a mathematical safe in many variations of its formulation. The second part of the paper will consider the application of these methods and algorithms to solve the problem of mathematical safe in its various variations.

Keywords: mathematical safe, finite rings, finite fields, method, algorithm, solution.