УДК 51.681.3

С.Л. КРЫВЫЙ

ЧИСЛЕННЫЕ МЕТОДЫ РЕШЕНИЯ ЗАДАЧИ О МАТЕМАТИЧЕСКОМ СЕЙФЕ

Аннотация. Приведены численные методы решения задачи о математическом сейфе с произвольным конечным числом позиций замков. Методы базируются на *TSS*-алгоритмах построения множества базисных решений систем линейных диофантовых уравнений в конечных полях и кольцах.

Ключевые слова: диофантовые уравнения, конечные поля, конечные кольца, системы линейных уравнений, базис решений.

ВВЕДЕНИЕ

Первое упоминание задачи о математическом сейфе было в работе [1]. Математическим сейфом называется система $Z = (z_1, z_2, \dots, z_n)$ взаимосвязанных замков, когда при повороте ключа в одном замке такой же поворот происходит и в замках, связанных с данным. Математический сейф может задаваться двумя способами: с помощью прямоугольной матрицы, элементы которой соответствуют замкам, а значения ее элементов — позициям замков, т.е. в виде матрицы $Z = || z_{ij} ||$, $i = 1, \dots, m$, $j = 1, \dots, n$, а также с помощью графа, вершины которого соответствуют замкам. При матричном задании математического сейфа каждый замок z_{ij} взаимосвязан с теми замками, которые расположены в той же строке и том же столбце. А при задании математического сейфа с помощью графа связанными с данным замком являются те замки, которые соответствуют расположенным в смежных вершинах. Исходное состояние сейфа Z задается матрицей $B = || b_{ij} ||$. Каждый замок может находиться в одной из нескольких позиций. Всех возможных позиций конечное число: $0, 1, \dots, k-1$. Замок открыт, когда он находится в позиции 0. В любой другой позиции замок считается закрытым. Если в каком-то замке осуществляется поворот ключа, то все замки, которые связаны с данным замком, увеличивают свои позиции на единицу по модулю k.

1. ПОСТАНОВКА ЗАДАЧИ

Необходимо решить следующую задачу. Исходя из начального состояния сейфа, представленного матрицей $B = || b_{ij} ||$, где $b_{ij} \in \{0, 1, \dots, k-1\}$, найти такую последовательность замков и число поворотов ключа в них, чтобы сейф перешел в положение открытого, т.е. когда все замки находятся в позиции 0. Приведем вначале задание математического сейфа с помощью матрицы и методы решения задачи над различными областями.

Рассмотрим математическую постановку задачи. Пусть матрица $X = || x_{ij} ||$ является решением задачи, где x_{ij} — число поворотов ключа в замке z_{ij}. Тогда условие того, что элемент b_{ij} преобразуется матрицей X в нуль, представляется соотношением

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

где $i = 1, \dots, m$, $j = 1, \dots, n$.

Обозначим $\bar{x} = (x_{11}, \dots, x_{1n}, x_{21}, \dots, x_{2n}, \dots, x_{m1}, \dots, x_{mn})$ вектор-столбец, полученный из матрицы X последовательной записью ее строк. Аналогично из матрицы B получим вектор-столбец $\bar{b}$. Кроме того, пусть $\mathcal{J}_n$ — матрица размера $n \times n$, состоящая из единиц, E_n — единичная матрица того же размера. Тогда решение задачи о математическом сейфе сводится к преобразованию (1) для всей

матрицы B и записывается в виде системы уравнений

$$A\bar{x} + \bar{b} \equiv 0 \pmod{k}, \tag{2}$$

где матрица A размера $mn \times mn$ состоит из m^2 клеток:

$$A = \begin{bmatrix} \mathcal{J}_n & E_n & E_n & \cdots & \cdots & E_n \\ E_n & \mathcal{J}_n & E_n & \cdots & \cdots & E_n \\ E_n & E_n & \mathcal{J}_n & \cdots & \cdots & E_n \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ E_n & E_n & E_n & \cdots & \cdots & \mathcal{J}_n \end{bmatrix}. \tag{3}$$

Далее рассматривается задача о сейфе над конечными кольцами и полями, а также ее вариации над этими областями.

Кольцом вычетов по модулю составного числа m называется алгебра $Z_m = (A = \{0, 1, \ldots, m-1\}, \Omega = \{+, \cdot, -, {}^{-1}, 0, 1\})$, где + и $\cdot$ есть бинарные ассоциативные, коммутативные операции сложения и умножения по модулю m, связанные законом дистрибутивности, операция – и операция $^{-1}$ являются унарными операциями взятия противоположного и обратного элементов относительно операций + и $\cdot$ соответственно, 0 и 1 — нульарные операции — аддитивный нуль и мультипликативная единица [2].

Кольцо вычетов Z_m называется примарным, если модуль m является степенью простого числа p, т.е. $m = p^t$, где $t > 1$, $t \in N$. Поскольку m не обязательно простое число, то сравнение $ax \equiv b \pmod{m}$ в кольце Z_m при $a \neq 0$ не всегда имеет решение. Решение возможно, если НОД$(a, m) = 1$ или НОД$(a, m) = d$ и d — делитель числа b.

Полем вычетов по модулю m называется ассоциативно-коммутативное кольцо вычетов, в котором мультипликативная полугруппа является группой. Известно, что кольцо вычетов по модулю m будет полем, если модуль m — простое число. Поле вычетов обозначим $\mathcal{F}_m$.

Дополнением элемента a в кольце Z_m или в поле $\mathcal{F}_p$ называется элемент b такой, что $a + b \equiv 0 \pmod{m}$. Очевидно, что сравнения $a_{11}x_1 + \ldots + a_{1j}x_j + \ldots + a_{1n}x_n \equiv 0 \pmod{m}$ и $a_{11}x_1 + \ldots - b_{1j}x_j + \ldots + a_{1n}x_n \equiv 0 \pmod{m}$ эквивалентны, т.е. каждое решение первого уравнения является решением второго и наоборот.

Если $m = p$ — простое число, то в поле $\mathcal{F}_p$ при $a \neq 0$ сравнение $ax \equiv b \pmod{p}$ всегда имеет решение и это решение единственно.

Рассмотрим поле $\mathcal{F}_{p^k}$ по модулю неприводимого полинома $q(x)$ степени k над полем $\mathcal{F}_p$. Построение такого поля сводится к вычислению остатков от деления полиномов, получаемых при умножении элементов поля (полиномов степени, меньшей k) на неприводимый над полем $\mathcal{F}_p$ полином $q(x)$. Поле $\mathcal{F}_{p^k}$ состоит из p^k элементов и имеет характеристику p. В качестве примеров такого типа полей приведем таблицы операций полей $\mathcal{F}_{2^2}$ и $\mathcal{F}_{3^2}$, которые строятся с помощью неприводимых полиномов $x^2 + x + 1$ и $x^2 + x + 2$ над полями $\mathcal{F}_2$ и $\mathcal{F}_3$ соответственно и заданы таблицами сложения (табл. 1, 3) и таблицами умножения (табл. 2, 4). (Построение таких полей детально описано в [2].) В табл. 1, 2 полином x обозначен числом 2, а полином $x + 1$ — числом 3.

Таблица 1

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

Таблица 2

*	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	3	1
3	0	3	1	2

Таблица 3

+	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

Таблица 4

*	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

В табл. 3, 4 полином x обозначен числом 3, полином $x+1$ — числом 4, полином $x+2$ — числом 5, полином $2x$ — числом 6, полином $2x+1$ — числом 7, полином $2x+2$ — числом 8.

2. *TSS*-МЕТОД РЕШЕНИЯ СИСТЕМ ЛИНЕЙНЫХ ДИОФАНТОВЫХ УРАВНЕНИЙ

TSS-метод решения систем линейных однородных диофантовых уравнений (СЛОДУ) и неоднородных уравнений (СЛНДУ) в конечных кольцах и полях рассматривался в работах [3–5]. Приведем краткое описание *TSS*-метода решения СЛНДУ.

Пусть дана СЛНДУ

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

над полем $\mathcal{F}_p$ и $e_1 = (1, 0, \ldots, 0, 0)$, $e_2 = (0, 1, \ldots, 0, 0), \ldots, e_q = (0, 0, \ldots, 0, 1)$ — единичные векторы из множества $\mathcal{F}_p^q$. Система

$$S = \begin{cases} L_1(x) = a_{11}x_1 + \ldots + a_{1q}x_q = 0, \\ L_2(x) = a_{21}x_1 + \ldots + a_{2q}x_q = 0, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ L_s(x) = a_{s1}x_1 + \ldots + a_{sq}x_q = 0 \end{cases} \tag{5}$$

называется СЛОДУ и соответствует вышеприведенной СЛНДУ *SN*. Поскольку решение СЛНДУ сводится к решению СЛОДУ, то достаточно рассмотреть способ решения СЛОДУ.

Возьмем первое уравнение

$$L_1(x) = a_{11}x_1 + a_{12}x_2 + \ldots + a_{1q}x_q = 0 \tag{6}$$

системы (5). Допустим, что $a_{1j} \neq 0$, заменим этот коэффициент его дополнением $-b_{1j}$. Построим множество решений $B_1 = \{e_k = (0, \ldots, 0, b_{1j}, 0, \ldots, 0, a_{1k}, 0, \ldots, 0\} \cup M_0$, где $M_0 = \{e_r : L_1(e_r) = 0\}$, $a_{1k} \neq 0$, а b_{1j} является k-й координатой в векторах из B_1.

Иными словами, множество B_1 строится путем комбинирования дополнения первого ненулевого коэффициента, взятого с отрицательным знаком, с остальными ненулевыми коэффициентами и пополненное векторами канонического базиса, которые соответствуют нулевым коэффициентам ЛОДУ (6). Построенное таким образом множество назовем *TSS*. Очевидно, что векторы из множества B_1 являются решениями ЛОДУ (6).

Возьмем функцию $L_2(x) = a_{21}x_1 + \ldots + a_{2q}x_q$ и рассмотрим ЛОДУ вида

$$L_2(e_1)y_1 + L_2(e_2)y_2 + \ldots + L_2(e_m)y_m = 0. \tag{7}$$

Заметим, что если все $L_2(e_i)=0$, то уравнение $L_2(x)$ линейно выражается через $L_1(x)$ и его можно удалить из СЛОДУ S. Поэтому будем предполагать, что все уравнения в S линейно независимы.

Найдем *TSS*-методом множество $B'=\{r_1, r_2, \dots, r_{m-1}\}$ решений ЛОДУ (7) и построим по векторам из B' соответствующие комбинации векторов из B_1. Обозначим это множество $M=\{s_1, s_2, \dots, s_{m-1}\}$. Продолжая эту процедуру, построим для всей СЛОДУ S множество решений M. В работе [5] было доказано, что *TSS*-множество M, построенное таким способом для СЛОДУ S вида (5), является базисом множества всех решений этой СЛОДУ.

Сложность построения базиса пропорциональна величине sl^3, где s — число уравнений в СЛОДУ, $l=\max(t, q)$, $t=\log p$ — количество двоичных разрядов модуля p, а q — количество неизвестных в СЛОДУ.

При оценке сложности элементарными считаются операции сложения и вычитания [3, 4].

Метод построения *TSS* (*TSS*-метод) решения СЛНДУ в поле $\mathcal{F}_p$ сводится к решению СЛОДУ. Действительно, пусть дана СЛНДУ

$$S=\begin{cases} L_1(x)=a_{11}x_1+\dots+a_{1n}x_n=b_1, \\ L_2(x)=a_{21}x_1+\dots+a_{2n}x_n=b_2, \\ \dots\dots\dots\dots\dots\dots\dots\dots\dots \\ L_s(x)=a_{s1}x_1+\dots+a_{sn}x_n=b_s, \end{cases} \pmod p \qquad (8)$$

где a_{ij}, b_i, $x_i \in \mathcal{F}_p$, $i=1,\dots,s$, $j=1,\dots,n$, $s\le n$. Поскольку обе части уравнения можно умножать на число, а сами уравнения складывать и вычитать, то преобразуем S к виду (полагая, что $b_s\ne 0$)

$$S'=\begin{cases} L'_1(x)=a'_{11}x_1+\dots+a'_{1n}x_n=0, \\ L'_2(x)=a'_{21}x_1+\dots+a'_{2n}x_n=0, \\ \dots\dots\dots\dots\dots\dots\dots\dots\dots \\ L'_{s-1}(x)=a'_{s-11}x_1+\dots+a'_{s-1n}x_n=0, \\ L_s(x)=a_{s1}x_1+\dots+a_{sn}x_n=b_s. \end{cases} \pmod p \qquad (9)$$

Пусть $B'=\{e'_1, e'_2, \dots, e'_m\}$ — базис множества решений СЛОДУ, состоящей из первых $s-1$ уравнения системы S', а $B=\{e_1, e_2, \dots, e_k\}$ — базис множества решений СЛОДУ, которая соответствует S'. Построим уравнение $L_s(e'_1)y_1+\dots$ $\dots+L_s(e'_m)y_m=b_s$. Если все $L_s(e_i)=0$, то данное уравнение не имеет решений, а значит, не имеет решений и исходная СЛНДУ (в этом случае $L_s(x)$ линейно зависит от $L'_1(x),\dots,L'_{s-1}(x)$). Если хотя бы одно значение $L_s(e_i)\ne 0$, то решение всегда существует, и если $y=(d_1,\dots,d_m)$ это решение, то вектор $x^1=d_1e'_1+\dots+d_me'_m$ является частным решением уравнения $L_s(x)=b_s$. Тогда общее решение СЛОДУ S', а значит, и системы S, представляется в виде $u=x^1+\sum\limits_{i=1}^{k} b_ie_i$, где $e_i\in B$, $i=1,2,\dots,k$.

Таким образом, имеет место следующая теорема.

Теорема 1. СЛНДУ S, все уравнения которой линейно независимы и ее размерность равна $s\times n$, всегда совместна над полем $\mathcal{F}_p$ и ее общее решение имеет вид $u=x^1+\sum\limits_{i=1}^{k} b_ie_i$, где x^1 — некоторое частное решение S, а e_i — базисные векторы множества решений СЛОДУ, которая соответствует данной СЛНДУ S.

Сложность построения общего решения СЛНДУ пропорциональна величине sl^3, где s — количество уравнений в системе, $l=\max(t, n)$, t — количество двоичных разрядов числа p, а n — количество неизвестных в СЛНДУ [3, 5].

Аналогично вычисляется базис множества решений в поле $\mathcal{F}_{p^k}$. Однако реализация *TSS*-метода в этом поле имеет некоторую особенность. Так, если в поле

вычетов для алгоритма необходимо указать только модуль и матрицу системы, то здесь кроме модуля и матрицы необходимо указывать таблицы сложения и умножения поля $\mathcal{F}_{p^k}$ (например, табл. 1–4).

Представим *TSS*-метод решения СЛНДУ в кольце вычетов по модулю составного числа. Принимая во внимание свойства кольца Z_m, рассмотрим СЛНДУ

$$S = \begin{cases} L_1(x) = a_{11}x_1 + \ldots + a_{1q}x_q = b_1, \\ L_2(x) = a_{21}x_1 + \ldots + a_{2q}x_q = b_2, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ L_s(x) = a_{s1}x_1 + \ldots + a_{sq}x_q = b_s, \end{cases} (\mathrm{mod}\ m) \qquad (10)$$

где $a_{ij}, b_i \in Z_m$.

Пусть модуль имеет разложение на простые множители $m = p_1^{k_1} p_2^{k_2} \cdot p_r^{k_r}$. Тогда системе S соответствует эквивалентная ей система из $r \cdot s$ уравнений вида

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

Эквивалентность систем S и S' очевидна. Действительно, если x — решение системы S, то оно будет решением и каждой подсистемы по модулю $p_i^{k_i}$, поскольку модуль m делится на каждое из чисел $p_i^{k_i}$, $i = 1, 2 \ldots, r$. Если x — решение системы S', то оно будет решением каждой ее подсистемы по модулю $p_i^{k_i}$, а значит, и решением системы S по модулю m, поскольку числа $p_i^{k_i}$ взаимно просты и их произведение равно m.

Перейдем от системы S' к системе однородных уравнений:

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

Пусть x — решение системы вида

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

Рассмотрим вектор m_1x, где $m_1 = m / p_1^{k_1}$, который является решением системы S''. Действительно, для второй системы S_2, аналогичной системе по модулю $p_2^{k_2}$, получаем для любого ее уравнения L_i:

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

$i = 1, 2 \ldots, s$, так как m_1 кратно $p_2^{k_2}$.

Аналогично если y — решение S_2, то $m_2\,y$, где $m_2 = m / p_2^{k_2}$, будет решением системы S'', а значит, и для любой из систем $S_3, \ldots, S_r$. Тогда общее решение системы S'' принимает вид

$$x = m_1x_1 + m_2x_2 + \ldots + m_rx_r, \tag{12}$$

где x_i — решение системы S_i.

Пусть $e_i = m_ix_i$, где x_i — решение системы S_i, $i = 1, 2, \ldots, r$. Эти решения линейно независимы над кольцом Z_m и составляют базис множества решений системы [4, 5]. Таким образом, достаточно найти решение системы S', а решение такой системы сводится к решению систем или в полях вычетов по модулю простого числа (когда степень $k_i = 1$ для некоторого $i \in [1, r]$ и тогда кольцо Z_{k_i} будет полем), или в примарных кольцах по модулю степени простого числа.

Рассмотрим формирование множества решений в примарном кольце *TSS*-методом. Поскольку построение множества решений системы сводится к решению одного уравнения, то рассмотрим ЛОДУ общего вида над примарным кольцом Z_m

$$a_1x_1 + a_2x_2 + \ldots + a_nx_n = 0, \tag{13}$$

где a_i, $x_i \in Z_m$, $m = p^y$, $y > 1$, $y \in \mathcal{N}$ (множеству натуральных чисел), $i = 1, \ldots, n$. Если среди коэффициентов ЛОДУ есть коэффициент, который взаимно прост с модулем, то базис множества его решений вычисляется описанным выше *TSS*-методом. Если НОД $(a_1, a_2, \ldots, a_n, m) = p^u$ тогда, сокращая коэффициент уравнения (13) на p^u, получаем ЛОДУ

$$b_1x_1 + b_2x_2 + \ldots + b_nx_n = 0 \tag{14}$$

над примарным кольцом $Z_{m'}$, где $m' = p^v$, $v = y - u$.

Полученное уравнение имеет свойство: любое решение ЛОДУ (13) будет решением ЛОДУ (14). Обратное не имеет места. Действительно, пусть b_1 в (14) взаимно прост с модулем m'. Тогда *TSS* этого ЛОДУ будет базисом его множества решений:

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

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

где $c = b_1 - p^v$ — дополнение коэффициента b_1. Очевидным решением (13) в кольце Z_m будет вектор $s_n = (p^v, 0, 0, \ldots, 0) = (m / \text{НОД}\,(a_1, \ldots, a_n, m), 0, \ldots, 0)$, который не выражается в виде линейной комбинации векторов из *TSS*, так как $c \cdot x \equiv 0 \ (\mathrm{mod}\ p^v)$ тогда и только тогда, когда $x = p^v$ в силу взаимной простоты c и p^v.

Имеет место следующая теорема.

Теорема 2. *TSS* уравнения (14), среди коэффициентов которого есть коэффициент взаимно прост с модулем, дополненное вектором $s_n = (p^v, 0, 0, \dots, 0)$, составляет базис множества решений ЛОДУ (13) [4].

В общем случае если модуль m имеет разложение на простые множители $m = p_1^{k_1} p_2^{k_2} \dots p_r^{k_r}$, то процедура построения базиса множества решений СЛОДУ в кольце Z_m сводится к решению r подсистем. Каждая из этих подсистем решается независимо по модулям $p_i^{k_i}$ и строятся базисы $B_1, B_2, \dots, B_r$ соответственно. Затем строится базис $B = m/\, p_1^{k_1} B_1 \cup m/\, p_2^{k_2} B_2 \cup \dots \cup m/\, p_r^{k_r} B_r$, где qB_i означает умножение каждого вектора из B_i на q.

Принимая во внимание, что арифметическая сложность выполнения операций сложения и вычитания в кольце Z_m пропорциональна $s = \log(m+1)$, операций умножения и деления, как и вычисления НОД двух чисел, меньших m, выражается величиной s^2, то арифметическая сложность нахождения базиса множества решений СЛОДУ имеет такие составляющие:

- l^3 — решение одного ЛОДУ и решение одного промежуточного ЛОДУ;
- $n^2 l^3$ — вычисление значений и сокращение на НОД $L(x)$, а также построение комбинаций векторов, которые составляют базис множества решений ЛОДУ ($l = \max(n, s)$).

Следовательно, арифметическая сложность перехода от предыдущего к следующему ЛОДУ в одной подсистеме пропорциональна величине l^5, а поскольку такая процедура повторяется r раз, то получаем оценку $O(l^6)$, где $l = \max(n, s, r)$. Таким образом, имеет место следующая теорема.

Теорема 3. Множество B, построенное *TSS*-методом, является базисом множества решений СЛОДУ S''. Арифметическая сложность построения B пропорциональна величине $O(l^6)$, где $l = \max(n, s, r)$.

Рассмотрим базис M множества решений СЛОДУ S''. Выделим в этом базисе решения, в которых последняя координата не равна нулю. Пусть $d_1, d_2, \dots, d_t$ — значения этих координат. Составим сравнение

$$c_1 d_1 + c_2 d_2 + \dots + c_t d_t \equiv 1 \pmod{m}. \tag{15}$$

Если это сравнение имеет решение $(u_1, u_2, \dots, u_t)$, то СЛНДУ S' совместна и линейная комбинация

$$x^1 = u_1 x_1 + u_2 x_2 + \dots + u_t x_t$$

является частным решением СЛНДУ S'. Если вышеприведенное сравнение не имеет решений, то СЛНДУ S' также не имеет решений.

Таким образом, приведенный алгоритм решения СЛНДУ в кольце Z_m будет иметь полиномиальную оценку сложности, если имеется разложение модуля m на простые множители. В противном случае сложность решения будет включать решение проблемы факторизации модуля m, что снижает эффективность алгоритма.

3. РЕШЕНИЕ ЗАДАЧИ О МАТЕМАТИЧЕСКОМ СЕЙФЕ

Случай 1. Число состояний замков p — простое. Это значит, что решения системы (2) находим в поле вычетов по модулю p. Построение этого решения с использованием *TSS*-метода приведено в работах [3, 5]. Поэтому рассмотрим только примеры, иллюстрирующие работу *TSS*-алгоритма.

Пусть имеем сейф в поле $\mathcal{F}_3$ с матрицей

$$B = \begin{pmatrix} 2 & 0 & 2 & 2 \\ 1 & 2 & 2 & 1 \end{pmatrix}.$$

Тогда $\bar{b} = (2, 0, 2, 2, 1, 2, 2, 1)$ и система уравнений $A\bar{x} + \bar{b} \equiv 0 \pmod 3$ имеет вид

$$A\bar{x}+\bar{b}=\begin{cases}1\ 1\ 1\ 1\ 1\ 0\ 0\ 0\ 2\\ 1\ 1\ 1\ 1\ 0\ 1\ 0\ 0\ 0\\ 1\ 1\ 1\ 1\ 0\ 0\ 1\ 0\ 2\\ 1\ 1\ 1\ 1\ 0\ 0\ 0\ 1\ 2\\ 1\ 0\ 0\ 0\ 1\ 1\ 1\ 1\ 1\\ 0\ 1\ 0\ 0\ 1\ 1\ 1\ 1\ 2\\ 0\ 0\ 1\ 0\ 1\ 1\ 1\ 1\ 2\\ 0\ 0\ 0\ 1\ 1\ 1\ 1\ 1\ 1\end{cases}\equiv 0\pmod 3.$$

Применяя *TSS*-алгоритм для решения этой системы, находим решение СЛНДУ

$$x=(0,2,2,0,0,2,0,0),\ \text{т.е. } x_{11}=0,\ x_{12}=2,\ x_{13}=2,$$
$$x_{14}=0,\ x_{21}=0,\ x_{22}=2,\ x_{23}=0,\ x_{24}=0.$$

Этому решению соответствуют такие преобразования матрицы B:

$$\begin{pmatrix}2\ 0\ 2\ 2\\ 1\ 2\ 2\ 1\end{pmatrix}\to(x_{12}=2)\begin{pmatrix}1\ 2\ 1\ 1\\ 1\ 1\ 2\ 1\end{pmatrix}\to(x_{13}=2)\begin{pmatrix}0\ 1\ 0\ 0\\ 1\ 1\ 1\ 1\end{pmatrix}\to(x_{22}=2)\begin{pmatrix}0\ 0\ 0\ 0\\ 0\ 0\ 0\ 0\end{pmatrix}.$$

Эта же задача по модулю 13 имеет решение $x_{11}=8$, $x_{12}=7$, $x_{13}=7$, $x_{14}=8$, $x_{21}=7$, $x_{22}=9$, $x_{23}=7$, $x_{24}=7$, в чем можно убедиться непосредственной проверкой.

Следует заметить, что в случае, когда число $m+n-1$, где $m\times n$ — размер матрицы B, кратно модулю, а сумма коэффициентов матрицы B не кратна модулю, то задача о сейфе не имеет решения. Это следует из теоремы 1. Действительно, задача о сейфе с матрицей B по модулю 5,

$$A\bar{x}+\bar{b}=\begin{cases}1\ 1\ 1\ 1\ 1\ 0\ 0\ 0\ 2\\ 1\ 1\ 1\ 1\ 0\ 1\ 0\ 0\ 0\\ 1\ 1\ 1\ 1\ 0\ 0\ 1\ 0\ 2\\ 1\ 1\ 1\ 1\ 0\ 0\ 0\ 1\ 2\\ 1\ 0\ 0\ 0\ 1\ 1\ 1\ 1\ 1\\ 0\ 1\ 0\ 0\ 1\ 1\ 1\ 1\ 2\\ 0\ 0\ 1\ 0\ 1\ 1\ 1\ 1\ 2\\ 0\ 0\ 0\ 1\ 1\ 1\ 1\ 1\ 1\end{cases}\equiv 0\pmod 5,$$

не имеет решения, поскольку $m+n-1=2+4-1=5$ (это значит, что последняя строка матрицы A линейно зависит от предыдущих строк), а сумма элементов матрицы B равна 12 и не кратна пяти.

Случай 2. Число состояний замков p^k, где p — простое число и область, над которой решается система, представляет поле $\mathcal{F}_{p^k}$. Рассмотрим случай поля $\mathcal{F}_{2^2}$, поскольку все выкладки для больших значений p и k аналогичны.

Пусть имеем сейф в поле $\mathcal{F}_{2^2}$ с матрицей

$$B=\begin{pmatrix}1\ 2\ 3\\ 0\ 1\ 1\end{pmatrix}.$$

Тогда $\bar{b}=(1,2,3,0,1,1)$ и система $A\bar{x}+\bar{b}\equiv 0$ в поле $\mathcal{F}_{2^2}$ принимает вид

$$A\bar{x}+\bar{b}=\begin{cases}1\ 1\ 1\ 1\ 0\ 0\ 1\\ 1\ 1\ 1\ 0\ 1\ 0\ 2\\ 1\ 1\ 1\ 0\ 0\ 1\ 3\\ 1\ 0\ 0\ 1\ 1\ 1\ 0\\ 0\ 1\ 0\ 1\ 1\ 1\ 1\\ 0\ 0\ 1\ 1\ 1\ 1\ 1\end{cases}\equiv 0. \qquad (16)$$

Применяя *TSS*-алгоритм для решения системы (16), получаем для первого ее уравнения

$$(1, 0, 0, 0, 0,0, 1),\ (0, 1, 0, 0, 0, 0, 1),\ (0, 0, 1, 0, 0, 0, 1),$$

$$(0, 0, 0, 1, 0, 0, 1),\ (0, 0, 0, 0, 1, 0, 0),\ (0, 0, 0, 0, 0, 1, 0).$$

Значения левой части второго уравнения системы (16), вычисленные по таблицам сложения и умножения в поле $\mathcal{F}_{2^2}$ (см. табл. 1, 2), равны 3, 3, 3, 2, 1, 0. По этим значениям путем комбинирования первого решения с остальными получаем решения первого и второго уравнений системы (16):

$$(1, 1, 0, 0, 0, 0, 0),\ (1, 0, 1, 0, 0, 0, 0),\ (1, 0, 0, 2, 0, 0, 3),$$

$$(1, 0, 0, 0, 3, 0, 1),\ (0, 0, 0, 0, 0, 1, 0).$$

Значения левой части третьего уравнения равны 0, 0, 3, 2, 1. По этим значениям комбинированием последнего решения с третьим и четвертым получаем решения первых трех уравнений системы:

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

Значения левой части четвертого уравнения равны 1, 1, 0, 0. По этим значениям комбинированием первого со вторым решением получаем решения первых четырех уравнений системы:

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

Значения левой части пятого уравнения равны 1, 2, 0. По этим значениям получаем решения первых пяти уравнений системы:

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

Значения левой части шестого уравнения равны 0, 0. Это значит, что оба векторы являются решениями исходной системы. Второе решение действительно является решением системы (16), а первое решение становится решением в случае умножения на 2 согласно таблицам сложения и умножения поля $\mathcal{F}_{2^2}$. В результате получим вектор (2, 3, 3, 3, 0, 1, 1) — второе решение системы (16).

Непосредственной проверкой можно убедиться, что полученные решения действительно открывают сейф. Для первого решения имеем

$$\begin{pmatrix}1&2&3\\0&1&1\end{pmatrix}\to(x_{11}=1)\begin{pmatrix}0&3&2\\1&1&1\end{pmatrix}\to(x_{22}=3)\begin{pmatrix}0&0&2\\2&2&2\end{pmatrix}\to(x_{23}=2)\begin{pmatrix}0&0&0\\0&0&0\end{pmatrix}.$$

Для второго решения имеем

$$\begin{pmatrix}1&2&3\\0&1&1\end{pmatrix}\to(x_{11}=2)\begin{pmatrix}3&0&1\\2&1&1\end{pmatrix}\to(x_{12}=3)\begin{pmatrix}0&3&2\\2&2&1\end{pmatrix}\to$$

$$\to(x_{13}=3)\begin{pmatrix}3&0&1\\2&2&2\end{pmatrix}\to(x_{21}=3)\begin{pmatrix}0&0&1\\1&1&1\end{pmatrix}\to(x_{33}=1)\begin{pmatrix}0&0&0\\0&0&0\end{pmatrix}.$$

Для получения решения задачи о сейфе в этом поле необходимо выполнение условия: если $m+n-1\equiv 0 \pmod p$, то $\sum\limits_{i=1}^{mn-1} b_i \equiv b_{mn} \pmod p$, где сумма вычисляется по таблицам поля $\mathcal{F}_{p^k}$. Действительно, если $m+n-1\equiv 0 \pmod p$, то последнее уравнение системы (16) является суммой (линейной комбинацией) предыдущих уравнений этой системы. Отсюда следует справедливость условия.

Например, приведенная выше задача о сейфе, в которой последнее значение свободного члена равно 2 (а не 1), не имеет решения в поле $\mathcal{F}_{2^2}$, поскольку $m+n-1=1+1+1+1\equiv 0 \pmod 2$ и $\sum_{i=1}^{5} b_i \equiv 1$, а последнее уравнение, являющееся суммой предыдущих пяти уравнений, равно двум. Полученное противоречие свидетельствует о несовместности системы (16). Действительно, комбинация решений

$$s_1 = (1, 2, 2, 2, 0, 3, 3),\ \ s_2 = (1, 0, 0, 0, 3, 2, 1)$$

для значений 2 и 3 (результат подстановки в последнее уравнение) дает решение $2s_1 + s_2 = (3, 3, 3, 3, 3, 3, 0)$, которое не является решением задачи о сейфе.

Случай 3. Число m — составное и область, над которой решается система (2), является кольцом вычетов по модулю m.

Пусть имеем сейф в кольце Z_{12} с матрицей

$$B = \begin{pmatrix} 4 & 5 & 2 \\ 1 & 3 & 1 \end{pmatrix}.$$

Тогда система (2) принимает вид

$$A\bar{x} + \bar{b} = \begin{cases} x_{11} + x_{12} + x_{13} + x_{21} + 4 = 0, \\ x_{11} + x_{12} + x_{13} + x_{22} + 5 = 0, \\ x_{11} + x_{12} + x_{13} + x_{23} + 2 = 0, \\ x_{11} + x_{21} + x_{22} + x_{23} + 1 = 0, \\ x_{12} + x_{21} + x_{22} + x_{23} + 3 = 0, \\ x_{13} + x_{21} + x_{22} + x_{23} + 1 = 0. \end{cases} \pmod{12}$$

Применяя *TSS*-алгоритм для решения этой системы, получаем решения

$$s_1 = (0, 6, 0, 6, 9, 0, 9),\ \ s_2 = (4, 8, 4, 4, 0, 0, 4).$$

Из этих решений нужно получить решение, в котором последняя координата равна 1, что соответствует исходным позициям замков. Для этого решаем сравнение $9x + 4y \equiv 1 \pmod{12}$. Очевидным решением этого сравнения есть $x = 1,\ y = -2$ или с учетом дополнения $x = 1,\ y = 10$. Линейная комбинация $s_1 + 10s_2$ дает решение задачи о математическом сейфе $z = (4, 2, 4, 10, 9, 0)$. Действительно,

$$\begin{pmatrix} 4 & 5 & 2 \\ 1 & 3 & 1 \end{pmatrix} \to (x_{11} = 4) \begin{pmatrix} 8 & 9 & 6 \\ 5 & 3 & 1 \end{pmatrix} \to (x_{12} = 2) \begin{pmatrix} 10 & 11 & 8 \\ 5 & 5 & 1 \end{pmatrix} \to (x_{13} = 4) \begin{pmatrix} 2 & 3 & 0 \\ 5 & 5 & 5 \end{pmatrix} \to$$

$$\to (x_{21} = 10) \begin{pmatrix} 0 & 3 & 0 \\ 3 & 3 & 3 \end{pmatrix} \to (x_{22} = 9) \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}.$$

4. ВАРИАЦИИ ЗАДАЧИ О МАТЕМАТИЧЕСКОМ СЕЙФЕ

Случай 4. Рассмотрим задачу о сейфе в поле вычетов $\mathcal{F}_k$, который считается открытым при определенной комбинации всех замков (исключая нулевые позиции). Тогда система (2) принимает вид

$$A\bar{x} + \bar{b} \equiv \bar{c} \pmod k, \tag{17}$$

где $\bar{c}$ — состояния замков, при которых сейф считается открытым.

Очевидно, что данная задача сводится к рассмотренным выше случаям, поскольку система (17) преобразуется к СЛОДУ

$$A\bar{x} + \bar{d} \equiv 0 \pmod k, \tag{18}$$

где $\bar{d} = \bar{b} - \bar{c}$.

Сложность вычисления переборным методом вектора $\bar{d}$, когда не известны открывающие комбинации, пропорциональна величине k^{mn}, где $m \times n$ — размер мат-

рицы A. Очевидно, что при небольших значениях k, m, n вычисление вектора $\bar{d}$ не составляет особого труда. Однако если модуль k достаточно большой, то даже при небольших значениях m и n задача усложняется. Например, если $k=101$, $m=4$, $n=5$, то сложность переборного метода составляет $P=101^{20}\approx 10^{41}\approx 2^{123}$, а это уже достаточно большое количество комбинаций, которое необходимо в наихудшем случае выполнить.

Если в задаче не известен модуль, то сложность возрастает в k раз.

Пусть дана матрица сейфа

$$B=\begin{pmatrix}14 & 0 & 0\\ 0 & 0 & 0\\ 0 & 0 & 11\end{pmatrix},$$

а задача решается в поле по модулю 17 с открывающей сейф матрицей (комбинацией)

$$c=\begin{pmatrix}1 & 2 & 3\\ 4 & 5 & 6\\ 7 & 8 & 9\end{pmatrix}.$$

Тогда СЛНДУ $A\bar{x}+\bar{b}\equiv\bar{c}\ (\mathrm{mod}\,17)$ принимает вид

$$A\bar{x}+\bar{b}=\begin{cases}1\ 1\ 1\ 1\ 0\ 0\ 1\ 0\ 0\ 14 = 1\\ 1\ 1\ 1\ 0\ 1\ 0\ 0\ 1\ 0\ 0 = 2\\ 1\ 1\ 1\ 0\ 0\ 1\ 0\ 0\ 1\ 0 = 3\\ 1\ 0\ 0\ 1\ 1\ 1\ 1\ 0\ 0\ 0 = 4\\ 0\ 1\ 0\ 1\ 1\ 1\ 0\ 1\ 0\ 0 = 5\\ 0\ 0\ 1\ 1\ 1\ 1\ 0\ 0\ 1\ 0 = 6\\ 1\ 0\ 0\ 1\ 0\ 0\ 1\ 1\ 1\ 0 = 7\\ 0\ 1\ 0\ 0\ 1\ 0\ 1\ 1\ 1\ 0 = 8\\ 0\ 0\ 1\ 0\ 0\ 1\ 1\ 1\ 1\ 11 = 9\end{cases}(\mathrm{mod}\,17).$$

После преобразования этой СЛНДУ к СЛОДУ получаем

$$A\bar{x}+\bar{d}=\begin{cases}1\ 1\ 1\ 1\ 0\ 0\ 1\ 0\ 0\ 13 = 0\\ 1\ 1\ 1\ 0\ 1\ 0\ 0\ 1\ 0\ 15 = 0\\ 1\ 1\ 1\ 0\ 0\ 1\ 0\ 0\ 1\ 14 = 0\\ 1\ 0\ 0\ 1\ 1\ 1\ 1\ 0\ 0\ 13 = 0\\ 0\ 1\ 0\ 1\ 1\ 1\ 0\ 1\ 0\ 12 = 0\\ 0\ 0\ 1\ 1\ 1\ 1\ 0\ 0\ 1\ 11 = 0\\ 1\ 0\ 0\ 1\ 0\ 0\ 1\ 1\ 1\ 10 = 0\\ 0\ 1\ 0\ 0\ 1\ 0\ 1\ 1\ 1\ 9 = 0\\ 0\ 0\ 1\ 0\ 0\ 1\ 1\ 1\ 1\ 2 = 0\end{cases}(\mathrm{mod}\,17).$$

Решением этой системы есть вектор $y=(3,13,5,1,13,5,15,10,6,5)$. Для построения решения задачи о сейфе необходимо решить сравнение $5z\equiv 1\ (\mathrm{mod}\,17)$. Решением этого сравнения есть $z=7$. Умножая вектор y на $z=7$, получаем решение задачи о сейфе: $x=(4,6,1,7,6,1,3,2,8)$. Действительно,

$$\begin{pmatrix}14 & 0 & 0\\ 0 & 0 & 0\\ 0 & 0 & 11\end{pmatrix}\to(x_{11}=4)\begin{pmatrix}1 & 4 & 4\\ 4 & 0 & 0\\ 4 & 0 & 11\end{pmatrix}\to(x_{12}=6)\begin{pmatrix}7 & 10 & 10\\ 4 & 6 & 0\\ 4 & 6 & 11\end{pmatrix}\to(x_{13}=1)\begin{pmatrix}8 & 11 & 11\\ 4 & 6 & 1\\ 4 & 6 & 12\end{pmatrix}\to$$

$$\to(x_{21}=7)\begin{pmatrix}15 & 11 & 11\\ 11 & 13 & 8\\ 11 & 6 & 12\end{pmatrix}\to(x_{22}=6)\begin{pmatrix}15 & 0 & 11\\ 0 & 2 & 14\\ 11 & 12 & 12\end{pmatrix}\to(x_{23}=1)\begin{pmatrix}15 & 0 & 12\\ 0 & 2 & 15\\ 11 & 12 & 13\end{pmatrix}\to$$

$$\to (x_{31}=3)\begin{pmatrix}1 & 0 & 12\\ 4 & 3 & 15\\ 14 & 15 & 16\end{pmatrix}\to (x_{32}=2)\begin{pmatrix}1 & 2 & 12\\ 4 & 5 & 15\\ 16 & 0 & 1\end{pmatrix}\to (x_{33}=8)\begin{pmatrix}1 & 2 & 3\\ 4 & 5 & 6\\ 7 & 8 & 9\end{pmatrix}.$$

Случай 5. Рассмотрим задачу о сейфе в поле $\mathcal{F}_{p^k}$, который считается открытым при определенной комбинации замков.

Сложность вычисления вектора $\bar{d}$ (когда не известны открывающие комбинации) в наихудшем случае переборным методом пропорциональна величине $(p^k)^{mn} = p^{kmn}$, что уже при небольших значениях p, m, n, k составляет большие трудности вычислительного характера. Например, при $p=3$, $m=2$, $n=4$, $k=5$ получаем 3^{40} вариантов для анализа. Эта сложность может возрасти, если таблицы сложения и умножения поля $\mathcal{F}_{p^k}$ задавать с точностью до обозначения ее элементов. В этом случае необходимо найти изоморфизм между таблицами для поля $\mathcal{F}_{3^2}$ (см. табл. 3, 4). Например, перенумеруем элементы этого поля следующим образом: полином x обозначим числом 8, полином $x+1$ — числом 7, полином $x+2$ — числом 6, полином $2x$ — числом 5, полином $2x+1$ — числом 4, полином $2x+2$ — числом 3. Тогда таблицы сложения и умножения поля имеют вид табл. 5 и табл. 6 соответственно. Даже при $p=3$ число изоморфизмов составляет $(3^2-3)! = 6! = 720 \approx 3^6$.

Таблица 5

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

Таблица 6

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

Если в задаче помимо неизвестной открывающей комбинации не известен и модуль поля, то задача еще больше усложняется. В этом случае необходимо найти модуль поля и само поле, что требует дополнительных временных и вычислительных затрат.

Случай 6. Рассмотрим задачу о сейфе, решения которой находим в кольце вычетов по модулю составного числа m при неизвестной комбинации замков, открывающей сейф.

Пусть задача о сейфе решается в кольце по модулю 15 с матрицей

$$B=\begin{pmatrix}14 & 2 & 3\\ 4 & 5 & 6\\ 7 & 8 & 11\end{pmatrix}$$

и с открывающей сейф матрицей

$$c=\begin{pmatrix}0 & 2 & 3\\ 4 & 5 & 6\\ 7 & 8 & 0\end{pmatrix}.$$

Тогда СЛНДУ $A\bar{x}+\bar{b}\equiv\bar{c}\ (\mathrm{mod}\,15)$ принимает вид

$$A\bar{x}+\bar{b}=\begin{cases}1\ 1\ 1\ 1\ 0\ 0\ 1\ 0\ 0\ 14\ =\ 0\\ 1\ 1\ 1\ 0\ 1\ 0\ 0\ 1\ 0\ \ 2\ =\ 2\\ 1\ 1\ 1\ 0\ 0\ 1\ 0\ 0\ 1\ \ 3\ =\ 3\\ 1\ 0\ 0\ 1\ 1\ 1\ 1\ 0\ 0\ \ 4\ =\ 4\\ 0\ 1\ 0\ 1\ 1\ 1\ 0\ 1\ 0\ \ 5\ =\ 5\\ 0\ 0\ 1\ 1\ 1\ 1\ 0\ 0\ 1\ \ 6\ =\ 6\\ 1\ 0\ 0\ 1\ 0\ 0\ 1\ 1\ 1\ \ 7\ =\ 7\\ 0\ 1\ 0\ 0\ 1\ 0\ 1\ 1\ 1\ \ 8\ =\ 8\\ 0\ 0\ 1\ 0\ 0\ 1\ 1\ 1\ 1\ 11\ =\ 0\end{cases}(\mathrm{mod}\,15).$$

После преобразования этой СЛНДУ к СЛОДУ получаем

$$A\bar{x}+\bar{d}=\begin{cases}1\ 1\ 1\ 1\ 0\ 0\ 1\ 0\ 0\ 14\ =\ 0\\ 1\ 1\ 1\ 0\ 1\ 0\ 0\ 1\ 0\ \ 0\ =\ 0\\ 1\ 1\ 1\ 0\ 0\ 1\ 0\ 0\ 1\ \ 0\ =\ 0\\ 1\ 0\ 0\ 1\ 1\ 1\ 1\ 0\ 0\ \ 0\ =\ 0\\ 0\ 1\ 0\ 1\ 1\ 1\ 0\ 1\ 0\ \ 0\ =\ 0\\ 0\ 0\ 1\ 1\ 1\ 1\ 0\ 0\ 1\ \ 0\ =\ 0\\ 1\ 0\ 0\ 1\ 0\ 0\ 1\ 1\ 1\ \ 0\ =\ 0\\ 0\ 1\ 0\ 0\ 1\ 0\ 1\ 1\ 1\ \ 0\ =\ 0\\ 0\ 0\ 1\ 0\ 0\ 1\ 1\ 1\ 1\ 11\ =\ 0\end{cases}(\mathrm{mod}\,15).$$

Решением этой системы есть вектор $x=(5,13,0,13,5,7,0,7,5)$, который открывает сейф. Действительно,

$$\begin{pmatrix}14&2&3\\4&5&6\\7&8&11\end{pmatrix}\to(x_{11}=5)\begin{pmatrix}4&7&8\\9&5&6\\12&8&11\end{pmatrix}\to(x_{12}=13)\begin{pmatrix}2&5&6\\9&3&6\\12&6&11\end{pmatrix}\to(x_{21}=13)\begin{pmatrix}0&5&6\\7&1&4\\10&6&11\end{pmatrix}\to$$

$$\to(x_{22}=5)\begin{pmatrix}0&10&6\\12&6&9\\10&11&11\end{pmatrix}\to(x_{23}=7)\begin{pmatrix}0&10&13\\4&13&11\\0&11&3\end{pmatrix}\to(x_{32}=7)\begin{pmatrix}0&2&13\\4&5&1\\2&3&10\end{pmatrix}\to$$

$$\to(x_{33}=5)\begin{pmatrix}0&2&3\\4&5&6\\7&8&0\end{pmatrix}.$$

Случай 7. Решения задачи о сейфе находим в кольце вычетов по модулю составного числа m при неизвестной комбинации замков, открывающей сейф, и матрице системы (15).

Пусть задача о сейфе решается в кольце по модулю 27 с матрицей

$$B=\begin{pmatrix}1&2&0\\0&0&0\\0&0&0\end{pmatrix}$$

и с открывающей сейф матрицей

$$c=\begin{pmatrix}1&2&3\\4&5&6\\7&8&9\end{pmatrix}.$$

Кроме того, матрица A системы имеет вид

$$A=\begin{vmatrix}1&1&1&3&0&0&2&0&0\\1&1&1&0&3&0&0&2&0\\1&1&1&0&0&3&0&0&2\\1&0&0&3&3&3&2&0&0\\0&1&0&3&3&3&0&2&0\\0&0&1&3&3&3&0&0&2\\1&0&0&3&0&0&2&2&2\\0&1&0&0&3&0&2&2&2\\0&0&1&0&0&3&2&2&2\end{vmatrix}.$$

Тогда СЛНДУ $A\bar{x}+\bar{b}\equiv\bar{c}\pmod{27}$ принимает вид

$$A\bar{x}+\bar{b}=\begin{cases}1\ 1\ 1\ 3\ 0\ 0\ 2\ 0\ 0\ 1=1\\1\ 1\ 1\ 0\ 3\ 0\ 0\ 2\ 0\ 2=2\\1\ 1\ 1\ 0\ 0\ 3\ 0\ 0\ 2\ 0=3\\1\ 0\ 0\ 3\ 3\ 3\ 2\ 0\ 0\ 0=4\\0\ 1\ 0\ 3\ 3\ 3\ 0\ 2\ 0\ 0=5\\0\ 0\ 1\ 3\ 3\ 3\ 0\ 0\ 2\ 0=6\\1\ 0\ 0\ 3\ 0\ 0\ 2\ 2\ 2\ 0=7\\0\ 1\ 0\ 0\ 3\ 0\ 2\ 2\ 2\ 0=8\\0\ 0\ 1\ 0\ 0\ 3\ 2\ 2\ 2\ 0=9\end{cases}\pmod{27}.$$

Решением этой системы есть вектор $x=(4,5,18,20,20,7,24,24,24,18)$, который не открывает сейфа (в чем можно убедиться). Для того чтобы сейф открывался, необходимо решение преобразовать следующим образом:

- первые три координаты, которые соответствую коэффициентам 1, остаются неизменными;
- вторые три координаты, которые соответствую коэффициентам 3, умножаются на 3 по модулю 27;
- третьи три координаты, которые соответствуют коэффициентам 2, умножаются на 2 по модулю 27.

В результате получаем решение $a=(4,5,18,6,6,21,21,21,9)$, которое открывает сейф. Действительно,

$$\begin{pmatrix}1&2&0\\0&0&0\\0&0&0\end{pmatrix}\to(x_{11}=4)\begin{pmatrix}5&6&4\\4&0&0\\4&0&0\end{pmatrix}\to(x_{12}=5)\begin{pmatrix}10&11&9\\4&5&0\\4&5&0\end{pmatrix}\to(x_{13}=18)\begin{pmatrix}1&2&0\\4&5&18\\4&5&18\end{pmatrix}\to$$

$$\to(x_{21}=6)\begin{pmatrix}7&2&0\\10&11&24\\10&5&18\end{pmatrix}\to(x_{22}=6)\begin{pmatrix}7&8&0\\16&17&3\\10&11&18\end{pmatrix}\to(x_{23}=21)\begin{pmatrix}7&8&21\\10&11&24\\10&11&12\end{pmatrix}\to$$

$$\to(x_{31}=21)\begin{pmatrix}1&8&21\\4&11&24\\4&5&6\end{pmatrix}\to(x_{32}=21)\begin{pmatrix}1&2&21\\4&5&24\\25&26&0\end{pmatrix}\to(x_{33}=9)\begin{pmatrix}1&2&3\\4&5&6\\7&8&9\end{pmatrix}.$$

Пусть задача о сейфе решается, как и раньше, в кольце по модулю 27 с матрицей

$$B=\begin{pmatrix}6&6&0\\0&0&0\\0&0&0\end{pmatrix}$$

и с открывающей сейф матрицей

$$c=\begin{pmatrix}0&0&6\\0&3&0\\0&3&0\end{pmatrix}.$$

Кроме того, матрица A системы имеет вид

$$A=\begin{vmatrix}1&3&2&1&0&0&1&0&0\\1&3&2&0&3&0&0&3&0\\1&3&2&0&0&2&0&0&2\\1&0&0&1&3&2&1&0&0\\0&3&0&1&3&2&0&3&0\\0&0&2&1&3&2&0&0&2\\1&0&0&1&0&0&1&3&2\\0&3&0&0&3&0&1&3&2\\0&0&2&0&0&2&1&3&2\end{vmatrix}.$$

Тогда СЛНДУ $A\bar{x}+\bar{b}\equiv\bar{c}\pmod{27}$ принимает вид

$$A\bar{x}+\bar{b}=\begin{cases}1&3&2&1&0&0&1&0&0&6&=&0\\1&3&2&0&3&0&0&3&0&6&=&0\\1&3&2&0&0&2&0&0&2&0&=&6\\1&0&0&1&3&2&1&0&0&0&=&0\\0&3&0&1&3&2&0&3&0&0&=&3\\0&0&2&1&3&2&0&0&2&0&=&0\\1&0&0&1&0&0&1&3&2&0&=&0\\0&3&0&0&3&0&1&3&2&0&=&3\\0&0&2&0&0&2&1&3&2&0&=&0\end{cases}\pmod{27}.$$

Решением этой системы есть вектор $x=(0,19,24,12,13,9,12,13,9)$, который не открывает сейфа (в чем можно убедиться). Для того чтобы сейф открывался, необходимо решение преобразовать следующим образом:

- первая, четвертая и седьмая координаты, которые соответствуют коэффициенту 1, остаются неизменными;
- вторая, пятая и восьмая координаты, которые соответствуют коэффициенту 3, умножаются на 3 по модулю 27;
- третья, шестая и девятая координаты, которые соответствуют коэффициенту 2, умножаются на 2 по модулю 27.

В результате получаем решение $a=(0,3,21,12,12,18,12,12,18)$, которое открывает сейф. Действительно,

$$\begin{pmatrix}6&6&0\\0&0&0\\0&0&0\end{pmatrix}\to(x_{12}=3)\begin{pmatrix}9&9&3\\0&3&0\\0&3&0\end{pmatrix}\to(x_{13}=21)\begin{pmatrix}3&3&24\\0&3&21\\0&3&21\end{pmatrix}\to(x_{21}=12)\begin{pmatrix}15&3&24\\12&15&6\\12&3&21\end{pmatrix}\to$$

$$\to(x_{22}=12)\begin{pmatrix}15&15&24\\24&0&18\\12&15&21\end{pmatrix}\to(x_{23}=18)\begin{pmatrix}15&15&15\\15&18&9\\12&15&12\end{pmatrix}\to(x_{31}=12)\begin{pmatrix}0&15&15\\0&18&9\\24&0&24\end{pmatrix}\to$$

$$\to(x_{32}=12)\begin{pmatrix}0&0&15\\0&3&9\\9&12&9\end{pmatrix}\to(x_{33}=18)\begin{pmatrix}0&0&6\\0&3&0\\0&3&0\end{pmatrix}.$$

Система (17) будет несовместной, если хотя бы по одному из модулей разложения она несовместна или сравнение (15) не имеет решений. Сложностные оценки возрастают на величину 2^m, поскольку необходимо найти также матрицу A.

Таким образом, наиболее сложной задачей о сейфе при неизвестном модуле и неизвестных открывающей комбинации и матрице, по-видимому, есть задача о сейфе в поле $\mathcal{F}_{p^k}$ или в кольце Z_m.

5. ЗАДАНИЕ МАТЕМАТИЧЕСКОГО СЕЙФА С ПОМОЩЬЮ ГРАФА

При задании математического сейфа на графе $G=(V,E)$ замки в вершинах могут находиться в одной из позиций множества $\{0,1,\dots,k-1\}$. Если в вершине u замок находится в позиции i, то поворот ключа в этой вершине переводит в позицию $(i+1)\pmod k$ ее замок, а также и все замки вершин, смежных с вершиной u. Начальные позиции замков в вершинах задаются вектором $\bar b=(b_1,b_2,\dots,b_{|V|})$.

Решение задачи выполняется теми же алгоритмами, что и при решении задачи на матрицах. Однако при таком задании структура матрицы СЛОДУ $A\bar x+\bar b\equiv\bar c\pmod k$ может быть произвольной.

Пример 1. Пусть имеем граф $G=(V,E)$ (рис. 1) и вектор $\bar b=(1,2,1,1,3)$. Строим СЛОДУ $A\bar x+\bar b\equiv 0\pmod k$ для задачи, заданной этим графом ($k=5$):

$$A=\left\{\begin{array}{c|ccccc|c} & 1 & 2 & 3 & 4 & 5 & \bar b \\ \hline 1 & 1 & 1 & 1 & 0 & 1 & 1 \\ 2 & 1 & 1 & 1 & 0 & 0 & 2 \\ 3 & 1 & 1 & 1 & 1 & 0 & 1 \\ 4 & 0 & 0 & 1 & 1 & 1 & 1 \\ 5 & 1 & 0 & 0 & 1 & 1 & 3 \end{array}\right. \equiv 0\pmod 5.$$

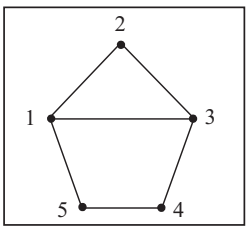

Рис. 1. Граф $G=(V,E)$

Решением данной СЛОДУ является вектор $\bar x=(0,1,2,1,1)$

$$\begin{array}{c} 1\ 2\ 1\ 1\ 3, \\ \downarrow b_2=1 \\ 2\ 3\ 2\ 1\ 3, \\ \downarrow b_3=2 \\ 4\ 0\ 4\ 3\ 3, \\ \downarrow b_4=1 \\ 4\ 0\ 0\ 4\ 4, \\ \downarrow b_5=1 \\ 0\ 0\ 0\ 0\ 0. \end{array}$$

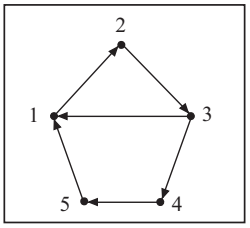

Рис. 2. Орграф G

Таким образом, сейф открыт.

Пример 2. Рассмотрим орграф G (рис. 2), где $\bar b=(1,2,1,1,3)$ и $\bar c=(1,3,0,2,6)$. Строим СЛНДУ $A\bar x+\bar b\equiv\bar c\pmod k$ для задачи, заданной этим графом ($k=15$):

$$A=\left\{\begin{array}{c|ccccc|cc} & 1 & 2 & 3 & 4 & 5 & \bar b & \bar c \\ \hline 1 & 1 & 1 & 0 & 0 & 0 & 1 & =1 \\ 2 & 0 & 1 & 1 & 0 & 0 & 2 & =3 \\ 3 & 1 & 0 & 1 & 1 & 0 & 1 & =0 \\ 4 & 0 & 0 & 0 & 1 & 1 & 1 & =2 \\ 5 & 1 & 0 & 0 & 0 & 1 & 3 & =6 \end{array}\right. \pmod{15}.$$

Решением данной СЛОДУ является вектор $\bar x=(0,0,1,13,3)$. Выполнив повороты ключа по столбцам матрицы, получим открывающую комбинацию позиций замков в вершинах орграфа:

$$\begin{array}{c} 1\ 2\ 1\ 1\ 3, \\ \downarrow b_3=1 \\ 1\ 3\ 2\ 1\ 3, \\ \downarrow b_4=13 \\ 1\ 3\ 0\ 14\ 3, \\ \downarrow b_5=3 \\ 1\ 3\ 0\ 2\ 6. \end{array}$$

ЗАКЛЮЧЕНИЕ

Предложены алгоритмы решения задачи о математическом сейфе в разных вариациях и над различными областями. Наиболее сложной задачей о сейфе при неизвестных модуле и открывающей комбинации замков является задача в поле $\mathcal{F}_{p^k}$ и кольца вычетов по составному модулю. Отличие задач о математическом сейфе на графах от аналогичной на матрицах состоит в том, что структура матрицы системы уравнений может быть произвольной.

СПИСОК ЛИТЕРАТУРЫ

1. Донец Г.А. Решение задачи о сейфе на (0, 1)-матрицах. *Кибернетика и системный анализ*. 2002. № 1. С. 98–105.
2. Сергієнко І.В., Кривий С.Л., Провотар О.І. Алгебраїчні аспекти інформаційних технологій. Ч. 1. Київ: Інтерсервіс, 2018. 410 с.
3. Крывый С.Л. Алгоритмы решения систем линейных диофантовых уравнений в полях вычетов. *Кибернетика и системный анализ.* 2007. № 2. С. 15–23.
4. Крывый С.Л. Алгоритмы решения систем линейных диофантовых уравнений в кольцах вычетов. *Кибернетика и системный анализ.* 2007. № 6. С. 27–40.
5. Кривий С.Л. Лінійні діофантові обмеження та їх застосування. Чернівці; Київ: Букрек, 2015. 224 с.

Надійшла до редакції 09.10.2018

С.Л. Кривий

ЧИСЕЛЬНІ МЕТОДИ РОЗВ'ЯЗАННЯ ЗАДАЧІ ПРО МАТЕМАТИЧНИЙ СЕЙФ

Анотація. Наведено чисельні методи розв'язання задачі про математичний сейф з довільним скінченним числом позицій засувів. Методи ґрунтуються на *TSS*-алгоритмах побудови множини базисних розв'язків систем лінійних діофантових рівнянь в скінченних полях і кільцях.

Ключові слова: діофантові рівняння, скінченні поля, скінченні кільця, системи лінійних рівнянь, базис розв'язків.

S.L. Kryvyi

THE NUMERICAL METHODS TO SOLVE PROBLEMS OF MATHEMATICAL SAFE

Abstract. The numerical metods to solve problems of mathematical safe with an arbitrary finite number of position of bolts is presented. The basis of the methods are *TSS*-algorithms for solving systems of linear Diophantine equations in finite fields and rings.

Keywords: Diophantine equations, finite fields, finite rings, systems of linear equations, basis of solutions.

Крывый Сергей Лукьянович,
доктор физ.-мат. наук, профессор, профессор кафедры Киевского национального университета имени Тараса Шевченко, e-mail: sl.krivoi@gmail.com.