Теорія оптимальних рішень

УДК 519.8

АГАИ АГ ГАМИШ ЯКУБ

РЕШЕНИЕ ЗАДАЧИ О МАТЕМАТИЧЕСКОМ СЕЙФЕ С ОДНОТИПНЫМИ ЗАМКАМИ ДЛЯ СОСТАВНОГО МОДУЛЯ К

Рассматривается разрешимость задачи о математическом сейфе с однотипными замками для составного модуля. В зависимости от соотношений числа строк и столбцов основной матрицы получаем различные условия для нахождения решений исходной задачи.

Пусть $\Im_n$ – квадратная матрица порядка n, состоящая из единиц, а E_n – единичная матрица того же порядка. Тогда условие решения задачи о математическом сейфе на матрицах* запишется в виде системы уравнений

$$A\vec{x}+\vec{b}\equiv 0(\mathrm{mod}K), \qquad (1)$$

где A – квадратная матрица порядка $m\times n$, состоящая из m^2 подматриц

$$A=\begin{pmatrix} \Im_n & E_n & E_n & \dots & E_n \\ E_n & \Im_n & E_n & \dots & E_n \\ E_n & E_n & \Im_n & \dots & E_n \\ \dots & \dots & \dots & \dots & \dots \\ E_n & E_n & E_n & \dots & \Im_n \end{pmatrix}. \qquad (2)$$

Если K – не простое число, то несмотря на выполнение необходимых условий для чисел m и n, могут возникать ситуации, когда задача не имеет решения. В этом случае надо найти необходимую коррекцию начального состояния сейфа, чтобы задача имела решение. Рассмотрим последовательно все возможные варианты:

$$(W_1)\ m+n\neq 1(\mathrm{mod}\,K),$$

$$n\neq 1(\mathrm{mod}\,K),\ m\neq 1(\mathrm{mod}\,K)$$

а) $НОД(m+n-1,K)=d>1;$

$$НОД(m-1,K)=НОД(n-1,K)=1.$$

---

* *Агаи Аг Гамиш Якуб*. Задача о математическом сейфе на матрицах // Теорія оптимальних рішень. – 2013. – С. 124 – 130.

Чтобы слагаемое в ((21) из [*]), имеющее в знаменателе число $m+n-1$ можно было

$$t(m+n-1)\equiv\sum(b)\ (\mathrm{mod}\,K). \tag{3}$$

Однако при условиях а) и для произвольных b_{ij} это не всегда возможно. Решение может существовать только при ограничении

$$\sum(b)\equiv 0(\mathrm{mod}\,d). \tag{4}$$

Тогда (3) будет иметь d решений вида

$$t=\left[t_1+\frac{K}{d}(s-1)\right](\mathrm{mod}\,K), \tag{5}$$

где $s=1,2,...,d$, а t_1 – решение уравнения

$$t_1\left(\frac{m+n-1}{d}\right)\equiv\frac{\sum(b)}{d}\left(\mathrm{mod}\,\frac{K}{d}\right). \tag{6}$$

Задача имеет d решений и запишется в виде

$$x_{ij}\equiv\left[b_{ij}-\frac{\sigma_i}{n-1}-\frac{\lambda_j}{m-1}+\left(\frac{1}{m-1}+\frac{1}{n-1}\right)t_1+\frac{K}{d}(s-1)\right](\mathrm{mod}\,K), \tag{7}$$

где $s=1,2,...,d$.

Пример 1. Пусть $K=9$, $m=2$, $n=5$. Начальное состояние сейфа задано матрицей B. Параметры удовлетворяют условиям (W_1), а $НОД(m+n-1,K)=$ $=НОД(6,9)=3>1$. Сумма всех элементов матрицы B равна $41\neq 0(\mathrm{mod}\,3)$. Введем коррекцию и получим матрицу B' (элемент коррекции в рамке).

$$B=\begin{pmatrix}7&5&5&5&5\\2&2&4&2&\boxed{4}\end{pmatrix},\quad B'=\begin{pmatrix}7&5&5&5&5\\2&2&4&2&5\end{pmatrix}.$$

Вычислим необходимые параметры:

$$\sigma_1=0;\sigma_2=6;\lambda_1=\lambda_3=0;\lambda_2=\lambda_4=7;\lambda_5=1;$$

$$-\frac{1}{m-1}\equiv -1\,(\mathrm{mod}\,9);\quad -\frac{1}{n-1}\equiv\frac{1}{4}\equiv -2\ (\mathrm{mod}\,9);$$

$$t_1\equiv\frac{\left(\frac{42}{3}\right)}{\left(\frac{6}{3}\right)}(\mathrm{mod}\,3)\equiv 1(\mathrm{mod}\,3).$$

$$x_{ij}=\left[b_{ij}+2\sigma_i-\lambda_j-1+3(s-1)\right];\ \ s=1,2,3.$$

После подстановки всех параметров получим 3 решения задачи.

$$X^{(1)}=\begin{pmatrix}6&6&4&6&3\\4&6&6&6&6\end{pmatrix},\ X^{(2)}=\begin{pmatrix}0&0&7&0&6\\7&0&0&0&0\end{pmatrix},\ X^{(3)}=\begin{pmatrix}3&3&1&3&0\\1&3&3&3&3\end{pmatrix}.$$

Проверим решение $X^{(2)}$ и $X^{(3)}$.

$$X^{(2)}:\left(\begin{array}{ccc|cc} 7 & 5 & 5 & 5 & 5 \\ \hline 2 & 2 & 4 & 2 & 5 \end{array}\right)\overset{+7}{\rightarrow}\left(\begin{array}{cccc|c} 5 & 3 & 3 & 3 & 3 \\ \hline 2 & 2 & 2 & 2 & 5 \end{array}\right)\overset{+6}{\rightarrow}\left(\begin{array}{c|cccc} 2 & 0 & 0 & 0 & 0 \\ \hline 2 & 2 & 2 & 2 & 2 \end{array}\right)\overset{+7}{=}\begin{pmatrix} 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix}.$$

$$X^{(3)}:\left(\begin{array}{c|cccc} 7 & 5 & 5 & 5 & 5 \\ \hline 2 & 2 & 4 & 2 & 5 \end{array}\right)\overset{+3}{\rightarrow}\left(\begin{array}{c|cccc} 1 & -1 & -1 & -1 & -1 \\ \hline 5 & 2 & 4 & 2 & 5 \end{array}\right)\overset{+3}{\rightarrow}\left(\begin{array}{cccc|c} 4 & 2 & 2 & 2 & 2 \\ \hline 5 & 5 & 4 & 2 & 5 \end{array}\right)\overset{+1}{\rightarrow}$$

$$\rightarrow\left(\begin{array}{cccc|c} 5 & 3 & 3 & 3 & 3 \\ \hline 5 & 5 & 5 & 2 & 5 \end{array}\right)\overset{+3}{\rightarrow}\left(\begin{array}{c|cccc} -1 & 6 & 6 & 6 & 6 \\ \hline 5 & 5 & 5 & 5 & 5 \end{array}\right)\overset{+1}{\rightarrow}\left(\begin{array}{c|cccc} 0 & 6 & 6 & 6 & 6 \\ \hline 6 & 6 & 6 & 6 & 6 \end{array}\right)\overset{+3}{\rightarrow}$$

$$\rightarrow\left(\begin{array}{cc|ccc} 0 & 0 & 6 & 6 & 6 \\ \hline 0 & 0 & 0 & 0 & 0 \end{array}\right)\overset{+3}{\rightarrow}\left(\begin{array}{ccc|cc} 0 & 0 & 0 & 6 & 6 \\ \hline 3 & 3 & 3 & 3 & 3 \end{array}\right)\overset{+3}{\rightarrow}\left(\begin{array}{cccc|c} 0 & 0 & 0 & 0 & 6 \\ \hline 6 & 6 & 6 & 6 & 6 \end{array}\right)\rightarrow\begin{pmatrix} 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix};$$

б) $НОД(n-1,K)=d>1$; $НОД(m-1,K)=НОД(m+n-1,K)=1$.

Из второго соотношения вытекает, что $m-1\neq 0(\mathrm{mod}K)$.

Чтобы слагаемое, имеющее в знаменателе число $n-1$, можно было превратить в целое число, необходимо решить уравнение

$$(n-1)\,p_i\equiv\left(\frac{\sum(b)}{m+n-1}-\sigma_i\right)(\mathrm{mod}\,K),\ i=1,2,\ldots,m. \tag{8}$$

Данное решение может существовать только при ограничениях на матрицу B

$$\frac{\sum(b)}{m+n-1}\equiv\sigma_i\,(\mathrm{mod}\,d),\ i=1,2,\ldots,m. \tag{9}$$

Это дает $m-1$ зависимых значений для B. Будем считать, что это $m-1$ элементов в последнем столбце, т. е.

$$b_{in}\equiv\left(\sigma_1-\sum_{j=1}^{n-1}b_{ij}\right)(\mathrm{mod}\,d),\ i=2,3,\ldots,m. \tag{10}$$

Кроме того p_i, как всегда, удовлетворяют ограничениям. Тогда для каждого i уравнение имеет d решений вида

$$p_i\equiv\left[p_i^{(0)}+\frac{k}{d}(s_i-1)\right](\mathrm{mod}\ K), \tag{11}$$

где $s_i=1,2,\ldots,d$, а $p_i^{(0)}$ – решение уравнения

$$p_i^{(0)}\left(\frac{n-1}{d}\right)\equiv\frac{1}{d}\left(\frac{\sum(b)}{m+n-1}-\sigma_i\right)\left(\mathrm{mod}\,\frac{K}{d}\right). \tag{12}$$

В общем случае задача (2) имеет d^{m-1} решений и (8) запишется в виде:

$$x_{ij} \equiv b_{ij} + \frac{1}{m-1}\left(\frac{\sum(b)}{m+n-1} - \lambda_j\right) + p_i, \tag{13}$$

где $i = 1, 2, \ldots, m$, а p_i находится из (11) и (12).

Пример 2. Пусть $K = 9$, $m = 5$, $n = 4$, а матрица B представлена далее. Здесь $d = 3 = НОД(n-1, K)$. Находим $\sigma_1 \equiv -1 (\mathrm{mod}\, 3)$. Проверяем условие (10). Оно выполняется для всех строк, кроме последней. Необходимо исправить элемент b_{mn} (он в рамке). В результате получаем необходимую матрицу B':

$$B = \begin{pmatrix} 0 & 4 & 1 & 0 \\ 6 & 8 & 4 & 5 \\ 4 & 5 & 0 & 5 \\ 1 & 8 & 2 & 6 \\ 3 & 3 & 2 & \boxed{1} \end{pmatrix}, \quad B' = \begin{pmatrix} 0 & 4 & 1 & 0 \\ 6 & 8 & 4 & 5 \\ 4 & 5 & 0 & 5 \\ 1 & 8 & 2 & 6 \\ 3 & 3 & 2 & 0 \end{pmatrix}.$$

Проведем расчеты: $\sum(b) \equiv 4 (\mathrm{mod}\, 9)$, $m + n - 1 = 8$, $\dfrac{\sum(b)}{m+n-1} \equiv 5 (\mathrm{mod}\, 9)$;

$$\sigma_1 = \sigma_2 = \sigma_3 \equiv 5 (\mathrm{mod}\, 9), \sigma_4 = \sigma_5 \equiv 8 (\mathrm{mod}\, 9).$$

Из уравнения (12) находим

$$p_i^{(0)} \equiv \left(\frac{5 - \sigma_i}{3}\right) (\mathrm{mod}\, 3),\ i = 1, 2, 3, 4, 5. \tag{14}$$

Отсюда $p_1^{(0)} = p_2^{(0)} = p_3^{(0)} \equiv 0 (\mathrm{mod}\, 3)$; $p_3^{(0)} = p_4^{(0)} \equiv -1 (\mathrm{mod}\, 3)$. Решение, если положить все $s_i = 1$, запишется в виде:

$$x_{ij} \equiv b_{ij} + 2\lambda_j - 1 + p_i^{(0)}$$

или

$$X = \begin{pmatrix} 0 & 5 & 0 & 4 \\ 6 & 0 & 3 & 0 \\ 4 & 6 & 8 & 0 \\ 0 & 8 & 0 & 0 \\ 2 & 3 & 0 & 3 \end{pmatrix} \begin{matrix} \\ \\ \\ \\ \textcircled{-3} \end{matrix} \rightarrow X' = \begin{pmatrix} 0 & 5 & 0 & 4 \\ 6 & 0 & 3 & 0 \\ 4 & 6 & 8 & 0 \\ 0 & 8 & 0 & 0 \\ 8 & 0 & 6 & 0 \end{pmatrix}.$$

В матрице X не удовлетворялось условие (14), так как сумма $\sum_{i=1}^{5} p_i =$ $= \sum_{i=1}^{5} p_i^{(0)} = -2 (\mathrm{mod}\, 9)$, а должна равняться $-5 (\mathrm{mod}\, 9)$. Поэтому из последней строки вычитается 3, что и дает матрицу X'. Здесь, как и в случае для простого K,

возникает проблема оптимизации X, чтобы она содержала максимальное количество нулевых элементов. Поэтому при согласовании равенства (8) необходимо выбирать строки, в которых наибольшее количество элементов, кратных d. Проверим решение X'.

$$B' = \left(\begin{array}{c|ccc} 0 & 4 & 1 & 0 \\ \hline 6 & 8 & 4 & 5 \\ 4 & 5 & 0 & 5 \\ 2 & 8 & 2 & 6 \\ 3 & 3 & 2 & 0 \end{array}\right) \overset{+5}{\rightarrow} \left(\begin{array}{ccc|c} 5 & 0 & 6 & 5 \\ \hline 6 & 4 & 4 & 5 \\ 4 & 1 & 0 & 5 \\ 1 & 4 & 2 & 6 \\ 3 & 8 & 2 & 0 \end{array}\right) \overset{+4}{\rightarrow} \left(\begin{array}{c|ccc} 0 & 4 & 1 & 0 \\ \hline 6 & 4 & 4 & 0 \\ \hline 4 & 1 & 0 & 0 \\ 1 & 4 & 2 & 1 \\ 3 & 8 & 2 & 4 \end{array}\right) \overset{+6}{\rightarrow} \left(\begin{array}{ccc|c} 6 & 4 & 1 & 0 \\ \hline 3 & 1 & 1 & 6 \\ \hline 1 & 2 & 0 & 0 \\ 7 & 4 & 2 & 1 \\ 0 & 8 & 2 & 4 \end{array}\right) \overset{+3}{\rightarrow}$$

$$\rightarrow \left(\begin{array}{c|ccc} 6 & 4 & 4 & 0 \\ 6 & 4 & 4 & 0 \\ \hline 1 & 1 & 3 & 0 \\ \hline 7 & 4 & 5 & 1 \\ 0 & 8 & 5 & 4 \end{array}\right) \overset{+4}{\rightarrow} \left(\begin{array}{c|ccc} 1 & 4 & 4 & 0 \\ 1 & 4 & 4 & 0 \\ \hline 5 & 5 & 7 & 4 \\ \hline 2 & 4 & 5 & 1 \\ 4 & 8 & 5 & 4 \end{array}\right) \overset{+6}{\rightarrow} \left(\begin{array}{cc|cc} 1 & 1 & 4 & 0 \\ 1 & 1 & 4 & 0 \\ \hline 2 & 2 & 4 & 1 \\ \hline 2 & 1 & 5 & 1 \\ 4 & 5 & 5 & 4 \end{array}\right) \overset{+8}{\rightarrow} \left(\begin{array}{cc|cc} 1 & 1 & 3 & 0 \\ 1 & 1 & 3 & 0 \\ 1 & 1 & 3 & 0 \\ \hline 2 & 1 & 4 & 1 \\ \hline 4 & 5 & 5 & 4 \end{array}\right) \overset{+8}{\rightarrow}$$

$$\rightarrow \left(\begin{array}{c|ccc} 1 & 0 & 3 & 0 \\ 1 & 0 & 3 & 0 \\ 1 & 0 & 3 & 0 \\ 1 & 0 & 3 & 0 \\ \hline 4 & 4 & 4 & 4 \end{array}\right) \overset{+8}{\rightarrow} \left(\begin{array}{cc|cc} 0 & 0 & 3 & 0 \\ 0 & 0 & 3 & 0 \\ 0 & 0 & 3 & 0 \\ 0 & 0 & 3 & 0 \\ \hline 3 & 3 & 3 & 3 \end{array}\right) \overset{+6}{\rightarrow} b_{fin}.$$

Аналогично решается задача при $НОД(m-1,K)=d>1$, $НОД(m+n-1,K)=$ $=НОД(n-1,K)=1$, если параметры m и n поменять местами;

в) $НОД(m+n-1,K)=d_1>1$, $НОД(n-1,K)=d_2$, $НОД(m-1,K)=1$.

В этом случае должны одновременно выполняться условия для матрицы B как в случаях а) и б):

$$\sum(b) \equiv 0 \pmod{d_1},$$

$$\frac{\sum(b)}{m+n-1} \equiv \sigma_i \pmod{d_2},\ i=1,2,\ldots,m. \qquad (15)$$

Первое уравнение должно давать решение следующего вида:

$$t(m+n-1) \equiv \sum(b) \pmod{K},$$

где $t = t_0 + \left(\frac{K}{d_1}\right) \cdot r, \quad (r = 0,1,\ldots d_1 - 1)$, а t_0 – решение уравнения

$$t_0\left(\frac{m+n-1}{d_1}\right) \equiv \frac{\sum(b)}{d_1}\left(\mathrm{mod}\ \frac{K}{d_1}\right). \tag{16}$$

Остальные уравнения (15) должны давать решения уравнениям такого вида:

$$p_i(n-1) \equiv (t - \sigma_i)(\mathrm{mod}\, K), \tag{17}$$

где $p_i = p_i^{(0)} + \left(\frac{K}{d_2}\right) \cdot s_i,\ s_i \in \{0,1,\ldots,d_2 - 1\}$, а $p_i^{(0)}$ – решение уравнения

$$p_i^{(0)}\left(\frac{n-1}{d_2}\right) \equiv \left(\frac{t-\sigma_i}{d_2}\right)\left(\mathrm{mod}\,\frac{K}{d_2}\right). \tag{18}$$

Кроме того, уравнение (8) превратится в следующее:

$$\sum_{i=1}^{m} p_i + t \equiv 0(\mathrm{mod}\ K). \tag{19}$$

Тогда

$$x_{ij} \equiv \left[b_{ij} + \frac{t-\lambda_j}{m-1} + p_i + \frac{K}{d_1} \cdot r_1\right](\mathrm{mod}\, K), \tag{20}$$

где $i = 1,2,\ldots,m;\ j = 1,2,\ldots,n.$

Будем традиционно представлять все элементы последнего столбца, кроме b_{ij} зависимыми, т. е.

$$b_{in} \equiv \sum_{j=1}^{n} b_{1j} - \sum_{j=1}^{n-1} b_{ij}. \tag{21}$$

А значение t выбираем из условия

$$t \equiv \sigma_1(\mathrm{mod}\, d_2). \tag{22}$$

Пример 3. Пусть $m = 6,\ n = 4$ и $K = 6,$ а матрица B представлена далее. Поскольку $\sigma_1 = 2,$ то элемент b_{54} не удовлетворяет условию (21). После исправления получаем матрицу B':

$$B = \begin{pmatrix} 1 & 1 & 4 & 2 \\ 1 & 1 & 4 & 2 \\ 1 & 5 & 0 & 2 \\ 1 & 1 & 4 & 2 \\ 0 & 2 & 4 & \textcircled{1} \\ 3 & 3 & 0 & 2 \end{pmatrix} \to B' = \begin{pmatrix} 1 & 1 & 4 & 2 \\ 1 & 1 & 4 & 2 \\ 1 & 5 & 0 & 2 \\ 1 & 1 & 4 & 2 \\ 0 & 2 & 4 & 2 \\ 3 & 3 & 0 & 2 \end{pmatrix}.$$

Проведем необходимые расчеты: $\sum(b)=48\equiv 0(\mathrm{mod}\ 6)$; $m+n-1=9\equiv$ $\equiv 3(\mathrm{mod}6)$; $НОД(n-1,K)=НОД(m+n-1,K)=3$.

Из соотношения

$$t_0\left(\frac{9}{3}\right)\equiv\left(\frac{48}{3}\right)(\mathrm{mod}\ 2).$$

Находим $t_0\equiv 0(\mathrm{mod}\,2)$, а $t\equiv 2r\ (r=0,1,2)$. Так как $\sigma_1=2$, то и $t\equiv 2(\mathrm{mod}6)$; $\frac{1}{m-1}=\frac{1}{5}\equiv -1(\mathrm{mod}\ 6)$. Полагаем $p_i\equiv r_i\equiv 0(\mathrm{mod}6)$, тогда

$$x_{ij}\equiv\left(b_{ij}+\lambda_j-2\right)(\mathrm{mod}\,6).$$

В результате получаем матрицу X':

$$X'=\begin{pmatrix}0&0&0&0\\0&0&0&0\\0&4&2&0\\0&0&0&0\\5&1&0&0\\2&2&2&0\end{pmatrix}\begin{matrix}\\\\\\\\\\-2\end{matrix}\rightarrow X=\begin{pmatrix}0&0&0&0\\0&0&0&0\\0&4&2&0\\0&0&0&0\\5&1&0&0\\0&0&0&4\end{pmatrix}.$$

Но условие (19) в X' для p_6 не выполняется. Оно будет выполнено, если вычесть из последней строки 2, что приводит к искомой матрице X. Проверим данное решение

$$B'=\begin{pmatrix}1&1&4&2\\1&1&4&2\\\hline 1&5&0&2\\\hline 1&1&4&2\\0&2&4&2\\3&3&0&2\end{pmatrix}\overset{+4}{\rightarrow}\begin{pmatrix}1&5&4&2\\1&5&4&2\\\hline 5&3&4&0\\\hline 1&5&4&2\\0&0&4&2\\3&1&0&2\end{pmatrix}\overset{+2}{\rightarrow}\begin{pmatrix}1&5&0&2\\1&5&0&2\\1&5&0&2\\1&5&0&2\\\hline 0&0&0&2\\\hline 3&1&2&2\end{pmatrix}\overset{+5}{\rightarrow}$$

$$\rightarrow\begin{pmatrix}0&5&0&2\\0&5&0&2\\0&5&0&2\\0&5&0&2\\\hline 5&5&5&1\\\hline 2&1&2&2\end{pmatrix}\overset{+1}{\rightarrow}\begin{pmatrix}0&0&0&2\\0&0&0&2\\0&0&0&2\\0&0&0&2\\0&0&0&2\\\hline 2&2&2&2\end{pmatrix}\overset{+4}{\rightarrow}b_{fin}.$$

Аналогично решается задача при условиях:

$$НОД(m+n-1,K)=d_1>1;\ НОД(m-1,K)=d_2>1;\ НОД(n-1,K)=1.$$

Это достигается путем транспонирования матрицы B, т. е. перестановкой параметров m и n;

г) $НОД(m-1,K)=d_1>1;\ НОД(n-1,K)=d_2>1;\ НОД(m+n-1,K)=1.$

Последнее соотношение является следствием двух первых. Решение задачи будет существовать, если для матрицы B выполняются следующие ограничения:

$$\frac{\sum(b)}{m+n-1}\equiv\sigma_i\,(\mathrm{mod}\,d_2),\ i=1,2,\ldots,m;$$

$$\frac{\sum(b)}{m+n-1}\equiv\lambda_j\,(\mathrm{mod}\,d_1),\ j=1,2,\ldots,n. \tag{23}$$

Отсюда вытекают еще два равенства

$$\begin{gathered}\sigma_i\,(\mathrm{mod}\,d_2)\equiv\lambda_j\,(\mathrm{mod}\,d_1),\\ n\lambda_j\,(\mathrm{mod}\,d_1)\equiv m\sigma_i\,(\mathrm{mod}\,d_2),\\ i=1,2,\ldots,m;\ j=1,2,\ldots n.\end{gathered} \tag{24}$$

При этих условиях будем считать заданным первый столбец матрицы B, а все элементы последней строки, кроме первого, и все элементы последнего столбца как зависимые, которые подвержены корректировке. Отсюда

$$\begin{gathered}b_{mj}\equiv\left(\lambda_1-\sum_{i=1}^{m-1}b_{ij}\right)(\mathrm{mod}\,d_1),\\ b_{in}\equiv\left(\lambda_1-\sum_{j=1}^{n-1}b_{ij}\right)(\mathrm{mod}\,d_2).\end{gathered} \tag{25}$$

Если все эти условия выполняются, то решение задачи необходимо начинать с решения двух уравнений

$$\begin{gathered}p_i(n-1)\equiv\left(\frac{\sum(b)}{m+n-1}-\sigma_i\right)(\mathrm{mod}\,K),\ i=1,2,\ldots,m;\\ q_j(m-1)\equiv\left(\frac{\sum(b)}{m+n-1}-\lambda_j\right)(\mathrm{mod}\,K),\ j=1,2,\ldots,n.\end{gathered} \tag{26}$$

Первое уравнение имеет решение

$$p_i=p_i^{(0)}+\frac{K}{d_2}s_i\text{, где } p_i^{(0)}\text{ – решение уравнения}$$

$$p_i^{(0)}\left(\frac{n-1}{d_2}\right)\equiv\frac{1}{d_2}\left(\frac{\sum(b)}{m+n-1}-\sigma_i\right)\left(\mathrm{mod}\,\frac{K}{d_2}\right), \tag{27}$$

а $s_i \in \{0,1,\ldots,d_2-1\}, i=1,2,\ldots,m.$

Второе уравнение имеет решение

$$q_j = q_j^{(0)} + \frac{K}{d_1} r_j, \text{ где } q_j^{(0)} - \text{решение уравнения}$$

$$q_j^{(0)}\left(\frac{m-1}{d1}\right) \equiv \frac{1}{d_1}\left(\frac{\sum(b)}{m+n-1} - \lambda_j\right)\left(\operatorname{mod}\frac{K}{d_1}\right), \tag{28}$$

а $r_j \in \{0,1,\ldots,d_1-1\}, j=1,2,\ldots,n.$

Задача имеет $d_1^{m-1} \cdot d_2^{n-1}$ решений вида

$$x_{ij} \equiv \left(b_{ij} + p_i + q_j\right)\left(\operatorname{mod} K\right),$$

где

$$\sum_{i=1}^{m} p_i \equiv \sum_{j=1}^{n} q_j \equiv -\frac{\sum(b)}{m+n-1}\left(\operatorname{mod} K\right). \tag{29}$$

Пример 4. Пусть $m=4, n=8, K=21,$ а матрица начального состояния сейфа задана далее.

$$B = \begin{pmatrix} 0 & 0 & 11 & 7 & 0 & 6 & 0 & 0 \\ 3 & 3 & 0 & 16 & 3 & 14 & 3 & 2 \\ 0 & 0 & 11 & 6 & 0 & 7 & 0 & 1 \\ 0 & 0 & 13 & 13 & 0 & 19 & 0 & 0 \end{pmatrix} \rightarrow B' = \begin{pmatrix} 0 & 0 & 11 & 7 & 0 & 6 & 0 & 0 \\ 3 & 3 & 0 & 16 & 3 & 14 & 3 & 3 \\ 0 & 0 & 11 & 6 & 0 & 7 & 0 & 0 \\ 0 & 0 & 14 & 13 & 0 & 18 & 0 & 0 \end{pmatrix}.$$

В матрице B не выполняются условия (25). Элементы в кружках заменены другими, в результате чего получается нужная матрица B'. Проведем необходимые расчеты:

$$d_1 = НОД(m-1,K) = 3,\ d_2 = НОД(n-1,K) = 7,$$

$$\sum(b) \equiv 12\left(\operatorname{mod} 21\right),\ \frac{\sum(b)}{m+n-1} \equiv 3\left(\operatorname{mod} 21\right).$$

В соответствии в (23) имеем

$\sigma_i \equiv 3\left(\operatorname{mod} 7\right), \lambda_j \equiv \sigma_i\left(\operatorname{mod} 3\right) \equiv 0\left(\operatorname{mod} 3\right).$ Поэтому $p_i^{(0)} \equiv 0\left(\operatorname{mod} 3\right),$ а все $q_j^{(0)} \equiv$ $\equiv 0\left(\operatorname{mod} 7\right),$ кроме $q_3^{(0)} = -4, q_4^{(0)} = 1.$ Отсюда $p_i = 3s_i, q_j = q_j^{(0)} + 7r_j.$ Полагая в (29) $s_i = r_j = 0,$ получаем первое решение X':

$$X' = \begin{pmatrix} 0 & 0 & 7 & 8 & 0 & 6 & 0 & 0 \\ 3 & 3 & 17 & 17 & 3 & 14 & 3 & 3 \\ 0 & 0 & 7 & 7 & 0 & 7 & 0 & 0 \\ 0 & 0 & 10 & 14 & 0 & 18 & 0 & 0 \end{pmatrix} \begin{matrix} \\ -3 \\ \\ \\ \end{matrix} \rightarrow X = \begin{pmatrix} 0 & 0 & 0 & 15 & 0 & 6 & 0 & 0 \\ 0 & 0 & 7 & 0 & 0 & 11 & 0 & 0 \\ 0 & 0 & 14 & 0 & 7 & 0 & 0 & 0 \\ 0 & 0 & 3 & 0 & 0 & 18 & 0 & 0 \end{pmatrix}.$$

$$\begin{matrix} & & -7 & +7 & & & & \end{matrix}$$

Вторая матрица получится из первой, если путем подбора s_i и r_j попытаемся удовлетворить второе условие (29). Поскольку, $\sum_{j=1}^{n} q_j \equiv 3(\mathrm{mod}\ 3) \equiv 0(\mathrm{mod}\ 3)$, то здесь это условие удовлетворяется. Но чтобы побольше образовать нулей в X, положим $r_3 = -1$, а $r_4 = 1$. Чтобы $\sum_{i=1}^{m} p_i \equiv -3(\mathrm{mod}\ 2)$, положим $s_2 = -1$. Это и дает матрицу X. Теперь решение достигается за 8 шагов.

Агаі Аг Гаміш Якуб

РОЗВ'ЯЗАННЯ ЗАДАЧІ ПРО МАТЕМАТИЧНИЙ СЕЙФ З ОДНОТИПОВИМИ ЗАМКАМИ ДЛЯ СКЛАДЕНОГО МОДУЛЯ K

Розглядається розв’язність задачі про математичний сейф з однотиповими замками для складеного модуля. В залежності від співвідношень числа рядків і стовпців основної матриці отримуємо різні умови для знаходження рішень вихідної задачі.

Aghaei Agh Ghamish Yaghoub

SOLVING THE PROBLEM OF MATHEMATICAL SAFE WITH LOCKS OF THE SAME TYPE FOR COMPOSITE MODULE K

We consider the solvability of the mathematical safe with locks of the same type for the composite module. Depending on the ratio of the number of rows and columns of the main matrix we obtain different conditions for finding solutions of the original problem.

Получено 31.03.2014