ТЕМА №2. РЕШЕНИЕ УРАВНЕНИЙ В ЦЕЛЫХ ЧИСЛАХ

ТЕОРЕТИЧЕСКАЯ ЧАСТЬ

Пусть задано уравнение следующего вида:

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

где a_i, c – целые и требуется найти целочисленные решения x_i. Такое уравнение называется *линейным диофантовым уравнением с* n *неизвестными*.

Очевидно, что для разрешимости уравнения (13) в целых числах необходимо, чтобы правая часть уравнения делилась на наибольший общий делитель коэффициентов a_i, т.е. выполнялось условие

$$c \,\vdots\, НОД\left(a_1, a_2, \ldots, a_n\right). \tag{14}$$

Для нахождения решений уравнения (13) можно использовать обобщение классического алгоритма Евклида для нахождения наибольшего общего делителя. Составим матрицу B размером $(n+1)\times n$:

$$B = \begin{pmatrix} a_1 & a_2 & \cdots & a_n \\ 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \end{pmatrix}.$$

Далее преобразуем матрицу по следующему алгоритму:

1. Выбираем в первой строке матрицы B наименьший по абсолютной величине ненулевой элемент a_i.
2. Выбираем номер $j \neq i$ такой, что $a_j \neq 0$.
3. Делим с остатком a_j на a_i, то есть находим такие целые q и r, что $a_j = qa_i + r$, $0 \le r < |a_i|$.
4. Вычитаем из j-го столбца матрицы B i-й столбец, умноженный на q.
5. Если в первой строке более одного ненулевого числа, то переходим на шаг 1.

В результате матрица B принимает вид

$$B=\begin{pmatrix} 0 & \cdots & 0 & d & 0 & \cdots & 0 \\ b_{11} & \cdots & b_{1,k-1} & b_{1k} & b_{1,k+1} & \cdots & b_{1n} \\ \vdots & \ddots & \vdots & \vdots & \vdots & \iddots & \vdots \\ b_{n1} & \cdots & b_{n,k-1} & b_{nk} & b_{1,k+1} & \cdots & b_{nn} \end{pmatrix},$$

где $d = НОД\left(a_1, a_2, \ldots, a_n\right)$, а для коэффициентов b_{ij} выполняются следующие соотношения:

$$a_1 b_{1k} + a_2 b_{2k} + \ldots + a_n b_{nk} = d, \tag{15}$$

$$a_1 b_{1j} + a_2 b_{2j} + \ldots + a_n b_{nj} = 0, \text{ при } j \neq k. \tag{16}$$

Умножим уравнение (15) на c/d

$$a_1\left(\frac{c}{d} b_{1k}\right) + a_2\left(\frac{c}{d} b_{2k}\right) + \ldots + a_n\left(\frac{c}{d} b_{nk}\right) = c.$$

Поскольку из условия (14) выражения в скобках являются целыми, то мы получили частное решение уравнения (13). Что означает, что условие (14) является не только необходимым, но и достаточным.

Общее решение уравнения (13) с учетом (16) можно записать в виде

$$x_i = \frac{c}{d} b_{ik} + t_1 b_{i1} + \ldots + t_{k-1} b_{i,k-1} + t_{k+1} b_{i,k+1} + \ldots + t_n b_{in}, \tag{17}$$

где $t_1, \ldots t_{k-1}, t_{k+1}, \ldots t_n$ – свободные переменные, принимающие произвольные целые значения.

Пример 1. Решим уравнение $36x + 13y = 2$.
Составим матрицу B и преобразуем ее в соответствии с алгоритмом

$$B=\begin{pmatrix} 36 & 13 \\ 1 & 0 \\ 0 & 1 \end{pmatrix} \sim \begin{pmatrix} 10 & 13 \\ 1 & 0 \\ -2 & 1 \end{pmatrix} \sim \begin{pmatrix} 10 & 3 \\ 1 & -1 \\ -2 & 3 \end{pmatrix} \sim \begin{pmatrix} 1 & 3 \\ 4 & -1 \\ -11 & 3 \end{pmatrix} \sim \begin{pmatrix} 1 & 0 \\ 4 & -13 \\ -11 & 36 \end{pmatrix}$$

Оставшееся в первой строке число является наибольшим общим делителем коэффициентов. Поскольку он равен 1, то на него делится правая часть и, следовательно, уравнение имеет решения в целых числах. Используя формулу (17), их можно записать в виде

$$x = 2 \cdot 4 + t \cdot (-13) = 8 - 13t,$$

$$y = 2 \cdot (-11) + t \cdot 36 = -22 + 36t.$$

Пример 2. Решим уравнение $3x + 6y = 2$.

Составим матрицу B и преобразуем ее в соответствии с алгоритмом:

$$B = \begin{pmatrix} 3 & 6 \\ 1 & 0 \\ 0 & 1 \end{pmatrix} \sim \begin{pmatrix} 3 & 0 \\ 1 & -2 \\ 0 & 1 \end{pmatrix}.$$

В этом случае НОД коэффициентов равен 3, и так как правая часть уравнения на него не делится, то решений в целых числах нет.

Рассмотрим нахождение целочисленных решений произвольной системы линейных диофантовых уравнений

$$\begin{cases} a_{11}x_1 + a_{12}x_2 + \ldots + a_{1n}x_n = c_1, \\ a_{21}x_1 + a_{22}x_2 + \ldots + a_{2n}x_n = c_2, \\ \vdots \\ a_{m1}x_1 + a_{m2}x_2 + \ldots + a_{mn}x_n = c_m, \end{cases} \qquad (18)$$

где a_{ij} и c_i – целые числа.

Для решения системы (18) вначале определим расширенную матрицу системы

$$B = \left(\begin{array}{c|c} A & -c \\ I & 0 \end{array} \right), \qquad (19)$$

где A – матрица коэффициентов a_{ij} системы (18) размером $m \times n$, I – единичная матрица размером $n \times n$, а c – вектор из коэффициентов c_i системы (18), размерности m.

С первыми n столбцами матрицы B можно производить следующие действия:

- переставлять их;
- вычитать из одного столбца другой, умноженный на целое число.

Также можно вычитать один из первых n столбцов из последнего и переставлять какие-либо из первых m строк матрицы B.

С помощью этих действий преобразуем матрицу B таким образом, чтобы верхние m строк имели трапециевидный вид

$$B=\begin{pmatrix} \tilde{a}_{11} & 0 & \cdots & 0 & 0 & \cdots & 0 & 0 \\ \tilde{a}_{21} & \tilde{a}_{22} & \ddots & & \vdots & & \vdots & \vdots \\ \vdots & \vdots & \ddots & \ddots & \vdots & & \vdots & \vdots \\ \tilde{a}_{k1} & \tilde{a}_{k2} & \cdots & \tilde{a}_{kk} & 0 & \cdots & 0 & 0 \\ \vdots & \vdots & & \vdots & \vdots & \ddots & \vdots & \vdots \\ \tilde{a}_{m1} & \tilde{a}_{m2} & \cdots & \tilde{a}_{mk} & 0 & \cdots & 0 & 0 \\ b_{11} & b_{12} & \cdots & b_{1k} & b_{1,k+1} & \cdots & b_{1n} & f_1 \\ \vdots & \vdots & & \vdots & \vdots & & \vdots & \vdots \\ b_{n1} & b_{n2} & \cdots & b_{nk} & b_{n,k+1} & \cdots & b_{nn} & f_n \end{pmatrix}. \qquad (20)$$

Если на каком-либо шаге невозможно сделать элемент последнего столбца нулевым, то система (18) не имеет решений в целых числах.

В случае, если матрицу удалось преобразовать к виду (20), общее решение системы (18) можно записать в виде

$$x_i = f_i + t_1 b_{i,k+1} + \ldots + t_{n-k} b_{in}\,. \qquad (21)$$

Пример 3. Найдем решение системы

$$\begin{cases} 3x+4y=8, \\ 7x+5z=6. \end{cases}$$

Для этого запишем матрицу B и преобразуем ее к виду (20)

$$B=\begin{pmatrix} 3 & 4 & 0 & -8 \\ 7 & 0 & 5 & -6 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix} \sim \begin{pmatrix} 3 & 1 & 0 & -8 \\ 7 & -7 & 5 & -6 \\ 1 & -1 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix} \sim \begin{pmatrix} 0 & 1 & 0 & -8 \\ 28 & -7 & 5 & -6 \\ 4 & -1 & 0 & 0 \\ -3 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix} \sim$$

$$\sim \begin{pmatrix} 1 & 0 & 0 & 0 \\ -7 & 28 & 5 & -62 \\ -1 & 4 & 0 & -8 \\ 1 & -3 & 0 & 8 \\ 0 & 0 & 1 & 0 \end{pmatrix} \sim \cdots \sim \begin{pmatrix} 1 & 0 & 0 & 0 \\ -7 & 1 & 0 & -62 \\ -1 & 8 & -20 & -8 \\ 1 & -6 & 15 & 8 \\ 0 & -11 & 28 & 0 \end{pmatrix} \sim \begin{pmatrix} 1 & 0 & 0 & 0 \\ -7 & 1 & 0 & 0 \\ -1 & 8 & -20 & 488 \\ 1 & -6 & 15 & -364 \\ 0 & -11 & 28 & -682 \end{pmatrix}$$

Используя формулу (21), можно записать общее решение

$$x = 488 - 20t,$$
$$y = -364 + 15t,$$
$$z = -682 + 28t.$$

Чтобы привести решение к более простому виду, можно сделать замену $\tilde{t} = t + 24$

$$x = 8 - 20\tilde{t},$$
$$y = -4 + 15\tilde{t},$$
$$z = -10 + 28\tilde{t}.$$

Пример 4. Найдем решение системы

$$\begin{cases} 3x + 6y = 8, \\ 7x + 5z = 6. \end{cases}$$

Для этого запишем матрицу B и попробуем привести ее к виду (20):

$$B = \begin{pmatrix} 3 & 6 & 0 & -8 \\ 7 & 0 & 5 & -6 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix} \sim \begin{pmatrix} 3 & 0 & 0 & -8 \\ 7 & -14 & 5 & -6 \\ 1 & -2 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix}.$$

Поскольку уже в первой строке нельзя сделать последний элемент нулевым, система не имеет решений в целых числах.

К уравнению вида (13) можно свести задачу поиска решений сравнения первой степени

$$ax \equiv b \pmod{n}. \tag{22}$$

Такая запись означает, что остатки от деления на n правой и левой части уравнения совпадают, то есть x удовлетворяет условию $(ax - b) \vdots n$, которое можно записать в виде

$$ax + ny = b\,. \tag{23}$$

Пример 5. Уравнения в целых числах используются в криптографии, например, в широко распространенном несимметричном алгоритме шифрования *RSA*. Процесс шифрования и дешифрования этим алгоритмом можно описать с помощью следующий формул:

$$\begin{cases} y \equiv x^e \pmod n, \\ x \equiv y^d \pmod n, \end{cases} \tag{24}$$

где x – данные, которые требуется зашифровать, y – зашифрованные данные, а пары (e,n) и (d,n) называются открытым и закрытым ключом соответственно, то есть чтобы зашифровать данные, требуется знать открытый ключ, а чтобы их расшифровать – закрытый.

Идея алгоритма заключается в том, что, зная только открытый ключ, нельзя за обозримое время вычислить закрытый ключ и, следовательно, нельзя расшифровать данные. Можно показать, что если выбран некоторый открытый ключ (e,n), то для нахождения числа d, удовлетворяющего условиям (24), требуется решить уравнение

$$e \cdot d \equiv 1 \pmod{\varphi(n)}, \tag{25}$$

где $\varphi(n)$ – функция Эйлера, равная количеству натуральных чисел, меньших n и взаимно простых с ним, и предполагается, что число e выбрано взаимно простым с $\varphi(n)$. Для вычисления $\varphi(n)$ требуется знать разложение n на простые множители, поэтому, если выбрать в качестве n произведение двух достаточно больших простых чисел p и q, то нельзя вычислить $\varphi(n)$ за разумное время, не зная этих чисел.

Рассмотрим процесс генерации ключей на примере с малыми простыми числами. Возьмем $p = 23$ и $q = 29$, $e = 3$. Тогда

$$n = p \cdot q = 23 \cdot 29 = 667,$$

$$\varphi(n) = (p-1)(q-1) = 616.$$

Для нахождения d требуется решить сравнение

$$3x \equiv 1 \pmod{616},$$

которое, как упоминалось выше, эквивалентно уравнению

$$3x + 616y = 1.$$

Решим это уравнение, используя подход с расширенной матрицей (19)

$$\left(\begin{array}{cc|c} 3 & 616 & -1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{array}\right) \sim \left(\begin{array}{cc|c} 3 & 1 & -1 \\ 1 & -205 & 0 \\ 0 & 1 & 0 \end{array}\right) \sim \left(\begin{array}{cc|c} 0 & 1 & 0 \\ 616 & -205 & 411 \\ -3 & 1 & -2 \end{array}\right).$$

Таким образом получаем, что $d = 411$. Можно убедится, что сгенерированный открытый $(3, 667)$ и закрытый $(411, 667)$ ключи удовлетворяют условиям (24). Пусть $x = 123$. Тогда

$$y = x^e = 123^3 = 604,$$

$$y^d = 604^{411} = 123 = x,$$

все вычисления проводились в арифметике по модулю 667 (описание алгоритма возведения в степень в арифметике по модулю см. на стр.15).

ЗАДАЧИ ДЛЯ САМОКОНТРОЛЯ

1. Решите следующие уравнения в целых числах или убедитесь в отсутствии решения:

1) $x = 1$
2) $x + y = 1$
3) $3x = 5$
4) $2x + 3y = 5$
5) $2x + 2y = 5$
6) $4x + 8y = 16$

2. Решите следующие системы уравнений в целых числах или убедитесь в отсутствии решений:

1) $\begin{cases} x = 1 \\ y = 2 \\ z = 3 \end{cases}$
2) $\begin{cases} x + z = 1 \\ y = 2 \\ x + z = 3 \end{cases}$
3) $\begin{cases} x + z = 1 \\ y = 2 \\ 2x + 2z = 2 \end{cases}$
4) $\begin{cases} x + z = 1 \\ y = 2 \end{cases}$
5) $\begin{cases} x + z = 1 \\ y - z = 2 \end{cases}$
6) $\begin{cases} x + y + z = 1 \\ 2x + 2y + 2z = 4 \end{cases}$