ПРОГРАМНО-ТЕХНІЧНІ КОМПЛЕКСИ

С.Л. КРЫВЫЙ

УДК 51.681.3

АЛГОРИТМЫ РЕШЕНИЯ СИСТЕМ ЛИНЕЙНЫХ УРАВНЕНИЙ В КОЛЬЦАХ ВЫЧЕТОВ

Аннотация. Предложены полиномиальные алгоритмы построения базиса множества решений системы линейных однородных и неоднородных диофантовых уравнений в кольце вычетов по модулю некоторого числа при условии известного разложения модуля на простые множители.

Ключевые слова: кольцо вычетов, линейные диофантовые уравнения, базис множества решений.

ВВЕДЕНИЕ

В настоящей статье рассматриваются улучшенные алгоритмы построения базиса множества решений систем линейных диофантовых уравнений в кольце вычетов по модулю составного числа m по сравнению с теми алгоритмами, которые приводились в [1]. В основе предлагаемых алгоритмов лежит *TSS*-метод [2, 3]. Сложность предлагаемых алгоритмов определяется сложностью проблемы разложения модуля m на простые множители. Если такое разложение имеет место, то предлагаемые алгоритмы имеют полиномиальную оценку сложности. Рассматриваемые алгоритмы применяются к решению задачи о математическом сейфе [4, 5].

ПОСТАНОВКА ЗАДАЧИ

Кольцом вычетов Z_m по модулю числа m называется алгебра $Z_m = (D = \{0, 1, \ldots, m-1\}, \Omega = \{+, \cdot, -, ^{-1}, 0, 1\})$, где знаки + и $\cdot$ представляют бинарные операции сложения и умножения по модулю m, знаки $-$ и $^{-1}$ представляют унарные операции взятия противоположного и обратного элементов относительно операций + и $\cdot$ соответственно, 0 и 1 — нульарные операции, т.е. аддитивный нуль и мультипликативная единица.

Из свойств операций в кольце Z_m вытекает справедливость тождества

$$(\forall x,\ y \in Z_m)x + y = 0 = m \to x = -y.$$

Отсюда следует, что когда $x = m - y$ в кольце Z_m, то $-y = x - m$, что дает возможность заменять положительное число x на отрицательное число $-y = x - m$ и наоборот. Такие элементы x и $-y$ будем называть дополнениями (x дополняет $-y$ до нуля и наоборот).

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 в кольце Z_m при $a \neq 0$ сравнение $ax \equiv b \pmod m$ не всегда имеет решение. Оно будет иметь решение, если НОД(a, m) = d и d — делитель числа b.

Рассмотрим систему линейных диофантовых уравнений (СЛДУ) в кольце Z_m

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

где $a_{ij}, b_i \in Z_m$.

Решением СЛДУ (1) называется такой вектор $c=(c_1,c_2,\ldots,c_n)$, при подстановке которого вместо x в $L_i(x)$ получаем тождество $L_i(c)\equiv b_i \pmod m$ для всех $i=1,2,\ldots,q$. СЛДУ называется однородной (СЛОДУ), если все b_i равны нулю, в противном случае СЛДУ называется неоднородной (СЛНДУ).

Если M — множество решений системы S, то для СЛОДУ нулевой вектор всегда будет ее решением. Это решение называют тривиальным, а любое решение системы S, отличное от нулевого, называется нетривиальным. СЛОДУ S называем несовместной, если она имеет только тривиальное решение, в противном случае S называется совместной системой.

Пусть модуль имеет разложение на простые множители: $m=p_1^{k_1}p_2^{k_2}\cdots p_r^{k_r}$, где $p_1<p_2<\ldots<p_r$. Тогда по системе S построим систему с $r\cdot s$ уравнениями вида

$$S'=\begin{cases}S_1\begin{cases}L_1(x)=a_{11}x_1+\ldots+a_{1q}x_q-b_1x_0=0,\\ L_2(x)=a_{21}x_1+\ldots+a_{2q}x_q-b_2x_0=0,\\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\\ L_s(x)=a_{s1}x_1+\ldots+a_{sq}x_q-b_sx_0=0\end{cases}\pmod{p_1^{k_1}},\\ S_2\begin{cases}L_1(x)=a_{11}x_1+\ldots+a_{1q}x_q-b_1x_0=0,\\ L_2(x)=a_{21}x_1+\ldots+a_{2q}x_q-b_2x_0=0,\\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\\ L_s(x)=a_{s1}x_1+\ldots+a_{sq}x_q-b_sx_0=0\end{cases}\pmod{p_2^{k_2}},\\ \vdots\\ S_r\begin{cases}L_1(x)=a_{11}x_1+\ldots+a_{1q}x_q-b_1x_0=0,\\ L_2(x)=a_{21}x_1+\ldots+a_{2q}x_q-b_2x_0=0,\\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\\ L_s(x)=a_{s1}x_1+\ldots+a_{sq}x_q-b_sx_0=0\end{cases}\pmod{p_r^{k_r}}.\end{cases} \tag{2}$$

Теорема 1. Системы S и S' эквивалентны.

Действительно, если x — решение системы S, то оно будет решением каждой из подсистем 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 из ее подсистем по модулю $p_i^{k_i}$, а значит, и решением системы S по модулю m, поскольку числа $p_i^{k_i}$ взаимно простые и их произведение равно m.

Пусть $x=(a_1,a_2,\ldots,a_q,1)$ — решение подсистемы вида

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

Рассмотрим вектор $m_1 x$, где $m_1 = \dfrac{m}{p_1^{k_1}}$, который будет решением системы S'. Действительно, для второй системы S_2, аналогичной предыдущей по модулю $p_2^{k_2}$, получаем для любого ее уравнения L_i

$$L_i(m_1 x) = m_1 L_i(x) = m_1 d_i \equiv 0 \pmod{p_2^{k_2}},$$

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

Аналогично если y — решение S_2, то $m_2 y$, где $m_2 = \dfrac{m}{p_2^{k_2}}$, будет решением системы S' и т.д. для любой из систем $S_3, \ldots, S_r$. По этим решениям необходимо построить частное решение системы S.

Обозначим $e_i = m_i x_i$, где x_i — решение системы S_i, $i = 1, 2, \ldots, r$.

Лемма 1. Векторы $e_1, e_2, \ldots, e_r$ линейно независимы над кольцом Z_m.

Для доказательства представим векторы e_i в координатной форме

$$e_1 = (c_{11}, c_{12}, \ldots, c_{1q}),\ e_2 = (c_{21}, c_{22}, \ldots, c_{2q}), \ldots, e_k = (c_{k1}, c_{k2}, \ldots, c_{kq})$$

и допустим, что существуют числа $a_1, a_2, \ldots, a_k$, где $a_i < p_i^{k_i}$, такие, что

$$a_1 e_1 + a_2 e_2 + \ldots + a_k e_k \equiv 0 \pmod{m}$$

или, что то же самое,

$$a_2 e_2 + \ldots + a_k e_k \equiv b_1 e_1 \pmod{m},$$

где b_1 — дополнение a_1 в кольце Z_m и $a_1 e_1 \not\equiv 0 \pmod{m}$. Принимая во внимание координатную форму векторов e_i, $i = 1, 2, \ldots, k$, получаем систему

$$S_1' = \begin{cases} a_2 m_2 c_{21}' + \ldots + a_k m_k c_{k1} \equiv b_1 m_1 c_{11}', \\ a_2 m_2 c_{22}' + \ldots + a_k m_k c_{k2} \equiv b_1 m_1 c_{12}', \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ a_2 m_2 c_{2q}' + \ldots + a_k m_k c_{kq} \equiv b_1 m_1 c_{1q}' \end{cases} \pmod{p_1^{k_1}},$$

где c_{ij}' — координаты векторов x_i, $i = 1, 2, \ldots, r$.

Из вида сравнений системы S_1' вытекает, что левая часть каждого из них кратна $p_1^{k_1}$, как и сам модуль m. Но тогда система S_1' будет иметь решение только в случае кратности числа $b_1 m_1$ (а значит, кратности $a_1 c_{1i}$) числу $p_1^{k_1}$. Но если все числа $a_1 c_{1i}$ кратны $p_1^{k_1}$, то получаем $a_1 e_1 \equiv 0 \pmod{m}$, что противоречит предположению $a_1 e_1 \not\equiv 0 \pmod{m}$. Полученное противоречие показывает несовместность системы S_1', а это свидетельствует о линейной независимости совокупности векторов $e_1, e_2, \ldots, e_k$. Лемма доказана.

Для построения искомого частного решения системы S составим сравнение вида

$$m_1 e_1 + m_2 e_2 + \ldots + m_r e_r \equiv 1 \pmod{m}. \tag{3}$$

Пусть $u = (b_1, b_2, \ldots, b_r)$ — решение этого сравнения; тогда вектор

$$v = b_1 e_1 + b_2 e_2 + \ldots + b_r e_r$$

будет искомым частным решением системы S.

Заметим, что сравнение (3) будет иметь решение только в случае $\text{НОД}(b_1, \ldots, b_r) = 1$. Это вытекает из следующего утверждения.

Теорема 2. СЛНДУ (1) совместна тогда и только тогда, когда сравнение (3) имеет решение.

Доказательство. Если сравнение (3) имеет решение, то расширенная СЛОДУ для данной СЛНДУ имеет решение, в котором последняя координата равна единице. Тогда, отбрасывая в этом решении последнюю координату, получаем частное решение СЛНДУ.

Пусть СЛНДУ совместна и x^1 — ее частное решение. Тогда расширенная СЛОДУ для данной СЛНДУ в своем базисе будет иметь векторы, последние координаты которых отличны от нуля и для которых сравнение (3) имеет решение. В противном случае это противоречило бы совместности СЛНДУ. Теорема доказана.

Из этой теоремы следует, что если в разложении модуля m все простые множители имеют первую степень и СЛНДУ, на которые распадается исходная СЛНДУ в кольце Z_m, совместны, то и исходная система также совместна.

Пусть x^1 — частное решение СЛНДУ S и $x_1, x_2, \ldots, x_s$ — базисные решения СЛОДУ, которая соответствует S. Тогда общее решение системы S' принимает вид

$$y = x^1 + a_1 x_1 + a_2 x_2 + \ldots + a_s x_s. \tag{4}$$

Следовательно, возникает необходимость решить систему вида S'. А решение такой системы сводится к решению подсистем S_i по модулю $p_i^{k_i}$ либо в полях вычетов по модулю простого числа (в случае $k_i = 1$ для некоторого $i \in [1, r]$), либо к решению систем в примарных кольцах (в случае $k_i > 1$).

TSS-МЕТОД РЕШЕНИЯ СЛОДУ НАД ПРИМАРНЫМИ КОЛЬЦАМИ

Рассмотрим вначаде ЛОДУ

$$L(x) = a_1 x_1 + \ldots + a_i x_i + \ldots + a_n x_n = 0, \tag{5}$$

где a_i, $x_i \in Z_m$, $i = 1, \ldots, n$. Допустим, что $a_i \neq 0$, тогда имеет место такое простое утверждение.

Лемма 2. Если $c = (c_1, \ldots, c_n)$ — решение ЛОДУ (5) в Z_m, то оно будет решением ЛОДУ $a_1 x_1 + \ldots - b_i x_i + \ldots + a_n x_n = 0$, где $-b_i$ — дополнение коэффициента a_i, т.е. $-b_i = a_i - m$, $i = 1, \ldots, n$ [1].

Рассмотрим ЛОДУ, которое удовлетворяет следующему условию.

Условие 1. Среди коэффициентов ЛОДУ существует коэффициент, который взаимно прост с модулем m.

Допустим, что в данном ЛОДУ таким коэффициентом является первый ненулевой коэффициент a_k, $k = 1, 2, \ldots, n$. Рассмотрим множество единичных векторов $M_0 = \{e_1, \ldots, e_n\}$ и функцию $L(x) = a_1 x_1 + a_2 x_2 + \ldots + a_n x_n$ — левую часть ЛОДУ (5). Заменим в функции $L(x)$ первый ненулевой коэффициент a_k, который взаимно прост с модулем, его отрицательным дополнением $-b_k$ и построим множество векторов, комбинируя его с остальными ненулевыми коэффициентами ЛОДУ,

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

где $M_0 = \{e_r : L(e_r) = 0\}$, $a_j \neq 0$ является k-й координатой, а b_k является j-й координатой в векторах из множества B. Иными словами, множество B строится комбинированием дополнения произвольного ненулевого коэффициента, удовлетворяющего условию 1 и взятого с отрицательным знаком, с остальными ненулевыми коэффициентами и пополняется единичными векторами, которые соответствуют нулевым коэффициентам ЛОДУ (5). Построенное таким образом множество будем называть *TSS*-множеством. Очевидно, что векторы из множества B являются решениями ЛОДУ (5).

В работе [1] были установлены такие свойства решений из *TSS*.

Теорема 3. Множество B решений ЛОДУ (5), построенное комбинированием дополнения первого ненулевого коэффициента, удовлетворяющего условию 1 и взятого с отрицательным знаком, с остальными ненулевыми коэффициентами и пополненное единичными векторами, которые соответствуют нулевым коэффициентам ЛОДУ (5), является базисом множества всех решений этого ЛОДУ.

Сложность алгоритма пропорциональна величине l^3, где $l = \max(s, n)$, $s = \log m$ — количество двоичных разрядов числа m, а n — число неизвестных в ЛОДУ.

Из этой теоремы очевидным образом вытекает следствие.

Следствие 1. Если модуль m является простым числом, то множество B решений ЛОДУ (5) является базисом множества всех решений этого ЛОДУ.

Сложность алгоритма пропорциональна величине l^3, где $l = \max(t, n)$, t — число разрядов простого числа m, а n — число неизвестных в ЛОДУ [1].

Действительно, если модуль m — простое число, то условие 1 выполняется автоматически.

Пусть имеем ЛНДУ

$$a_1x_1 + \ldots + a_kx_k + \ldots + a_nx_n = b, \tag{6}$$

в котором коэффициент a_k взаимно прост с модулем m. Найдем решение сравнения

$$a_k y \equiv b \pmod m,$$

которое при данных условиях будет единственным. Пусть этим решением будет c, а вектор $x^1 = (0, \ldots, 0, c, 0, \ldots, 0)$ будет решением (6). Применяя *TSS*-метод к ЛОДУ, которое соответствует ЛНДУ (6), находим базис B множества его решений.

Пусть $x^1 = (c_1, c_2, \ldots, c_n)$ — некоторое частное решение (6), найденное описанным выше способом, а $B = \{e_1, e_2, \ldots, e_m\}$ — базис множества решений ЛОДУ

$$a_1x_1 + a_2x_2 + \ldots + a_nx_n = 0. \tag{7}$$

Теорема 4. Произвольное решение ЛНДУ (6) представляется в виде $u = x^1 + \sum_{i=1}^{m} b_i e_i$, где x^1 — частное решение ЛНДУ (6), а $e_1, \ldots, e_m$ — базисные векторы множества решений ЛОДУ (7), которое соответствует ЛНДУ (6) [1].

Рассмотрим ЛОДУ над примарными кольцами. В общем случае приведенные выше способы решения ЛОДУ и ЛНДУ не применимы.

Рассмотрим ЛОДУ над примарным кольцом Z_m

$$L(x) = a_1x_1 + \ldots + a_ix_i + \ldots + a_nx_n = 0, \tag{8}$$

где a_i, $x_i \in Z_m$, $m = p^t$, $t > 1$, $t \in N$, $i = 1, \ldots, n$. Пусть НОД$(a_1, a_2, \ldots, a_n, m) = p^u$, тогда, сокращая коэффициенты в (8) на p^u, получаем ЛОДУ

$$b_1x_1 + b_2x_2 + \ldots + b_nx_n = 0 \tag{9}$$

над примарным кольцом $Z_{m'}$, где $m' = p^v$, $v = t - u$. Исходя из свойства полученного уравнения любое решение ЛОДУ (8) будет решением ЛОДУ (9). Обратное утверждение не имеет места. Действительно, пусть коэффициент b_1 в (9) взаимно прост с модулем m'. Тогда строим *TSS* этого ЛОДУ, которое в силу теоремы 3 является базисом его множества решений:

$$s_1 = (b_2, c, 0, 0, 0, \dots, 0),\ s_2 = (b_3, 0, c, 0, 0, \dots, 0),$$
$$s_3 = (b_4, 0, 0, c, 0, \dots, 0), \dots, s_{n-1} = (b_n, 0, 0, 0, \dots, 0, c),$$

где $c = p^v - b_1$ — дополнение коэффициента b_1, взятое с противоположным знаком. Поскольку кольцо Z_m с делителями нуля, то очевидным решением (8) будет вектор $s_n = (p^v, 0, 0, \dots, 0)$, который не выражается неотрицательной линейной комбинацией векторов из *TSS*, так как $c \cdot x \equiv 0 \pmod{p^v}$ тогда и только тогда, когда $x = p^v$ в силу взаимной простоты c и p^v. Однако имеет место следующее утверждение.

Теорема 5. Множество *TSS* уравнения (9), дополненное вектором $s_n = (p^v, 0, 0, \dots, 0)$, является базисом множества решений ЛОДУ (8).

Доказательство. Пусть $x = (d_1, d_2, \dots, d_n)$ — произвольное решение ЛОДУ (8). Построим вектор $c = c_1 s_1 + c_2 s_2 + \dots + c_{n-1} s_{n-1} = (c_1 b_2 + \dots + c_{n-1} b_n, d_2, \dots, d_n)$, т.е. $d_i \equiv c_i \cdot c \pmod{m'}$, $i = 2, \dots, n$, и рассмотрим вектор

$$c - x - c_n s_n = (c_1 b_2 + \dots + c_{n-1} b_n - d_1', 0, \dots, 0) = (c_1 b_2 + \dots + c_{n-1} b_n + d_1'', 0, \dots, 0),$$

где d_1'' — дополнение $d_1' c_n \equiv d_1'' \pmod{m'}$. Полученный вектор является решением (8), а следовательно, является решением (9). Представим d_1'' в виде $b_1 d$: $b_1 d \equiv d_1'' \pmod{p^v}$ (такое представление единственно в силу взаимной простоты b_1 и p^v). Тогда $c - x - c_n s_n = (c_1 b_2 + \dots + c_{n-1} b_n + b_1 d'', 0, \dots, 0)$, и после подстановки $c - x$ в ЛОДУ (9) получаем $b_1 (b_1 d'' + b_2 c_1 + \dots + b_n c_{n-1}) \equiv 0 \pmod{p^v}$.

Следовательно, возможны два случая:

а) $b_1 d'' + b_2 c_1 + \dots, b_n c_{n-1} = up^k \equiv 0 \pmod{p^{t+1}}$;

б) $b_1 d'' + b_2 c_1 + \dots, b_n c_{n-1} = up^k \not\equiv 0 \pmod{p^{t+1}}$.

В случае а) доказательства не требуется. В случае б) для окончательного представления вектора x необходимо из вектора $x - c$ вычесть вектор us_n: $x - c - (c_n + u) s_n = 0$ и $x = c + (c_n + u) s_n$.

Теорема доказана.

Рассмотрим общий случай ЛОДУ, для которых не выполняется условие 1. Предположим, что модуль m имеет разложение на простые множители вида $m = p^c q^d$, и дано ЛОДУ

$$L(x) = a_1 x_1 + \dots + a_i x_i + \dots + a_n x_n = 0, \tag{10}$$

где $a_i, x_i \in Z_m$, $i = 1, \dots, n$. Построим по этому ЛОДУ два ЛОДУ:

$$L_1(x) = a_1' x_1 + a_2' x_2 + \dots + a_n' x_n = 0, \tag{11}$$

$$L_2(x) = b_1' x_1 + b_2' x_2 + \dots + b_n' x_n = 0, \tag{12}$$

где $a_i' \equiv a_i \pmod{p^c}$, $b_i' \equiv a_i \pmod{q^d}$, $i = 1, \dots, n$.

Имеет место простое утверждение.

Лемма 3. ЛОДУ (11) и (12) удовлетворяют условию 1, т.е. в каждом из этих уравнений существует по крайней мере один коэффициент, который взаимно прост с модулем p^c и q^d.

Действительно, рассмотрим произвольный ненулевой коэффициент a_i' ЛОДУ (11). Если a_i' и p^c взаимно простые, то доказательства не требуется. В противном случае все коэффициенты a_i' должны быть кратны p^u, $u < c$. Сокращая на НОД этих чисел, получаем уравнение, эквивалентное исходному, для которого выполняется условие 1. Доказательство для ЛОДУ (12) аналогично. Лемма доказана.

Отсюда вытекает, что ЛОДУ (11) и (12) удовлетворяют условию 1. Используя *TSS*-алгоритм, построим базисы множеств решений для обоих ЛОДУ. Пусть это будут соответственно множества

$$B_1' = \{e_1, e_2, \ldots, e_{n-1}\} \text{ и } B_2' = \{s_1, s_2, \ldots, s_{n-1}\}.$$

Построим множества

$$B_1 = \{e_1' = q^d e_1, e_2' = q^d e_2, \ldots, e_{n-1}' = q^d e_{n-1}\},$$

$$B_2 = \{s_1' = p^c s_1, s_2' = p^c s_2, \ldots, s_{n-1}' = p^c s_{n-1}\}.$$

Имеет место следующее утверждение.

Теорема 6. Множество $B = B_1 \bigcup B_2$ является базисом множества всех решений ЛОДУ (10).

Доказательство. Очевидно, что векторы из B являются решениями ЛОДУ (10).

Пусть $x = (x_1, \ldots, x_n)$ — произвольное решение ЛОДУ (10). Если $x_i < p^c$ и $x_i < q^d$ для всех $i = 1, 2, \ldots, n$, то x является решением ЛОДУ (11) и ЛОДУ (12) и, следовательно, представляется в виде неотрицательной линейной комбинации векторов из B_1 и B_2:

$$x = a_{11}e_1 + a_{12}e_2 + \ldots + a_{1n-1}e_{n-1} \text{ в } B_1$$

и

$$x = a_{21}s_1 + a_{22}s_2 + \ldots + a_{2n-1}s_{n-1} \text{ в } B_2.$$

Домножая первое разложение на q^d, а второе на p^c, получаем

$$q^d x = a_{11}'e_1' + a_{12}'e_2' + \ldots + a_{1n-1}'e_{n-1}' \text{ в } B_1',$$

$$p^c x = a_{21}'s_1' + a_{22}'s_2' + \ldots + a_{2n-1}'s_{n-1}' \text{ в } B_2',$$

где $a_{1i}' = a_{1i}q^d$, $d_i' = \text{НОД}(d_i, q^d)$, $a_{2i}' = a_{2i}p^c$.

Рассмотрим уравнение вида $q^d u + p^c v - 1 = 0$, в котором коэффициенты q^d, p^c взаимно просты. Данное уравнение имеет единственное решение (u_1, v_1). Тогда

$$(q^d u_1 + p^c v_1)x = x =$$

$$= u_1(a_{11}'e_1' + \ldots + a_{1n-1}'e_{n-1}') + v_1(a_{21}'s_1' + \ldots + a_{2n-1}'s_{n-1}'),$$

т.е. вектор x представляется в виде линейной комбинации векторов из $B = B_1 \bigcup B_2$.

Случай, когда некоторые координаты вектора x больше p^c и q^d, легко сводится к приведенному выше случаю. Для этого достаточно рассмотреть представление $x = x_{11} + p^c x_{12}$ в B_1 и $x = x_{21} + q^d x_{22}$ в B_2 где векторы x_{11} и x_{21} имеют координаты, меньшие p^c и q^d, и являются решениями ЛОДУ (11) и ЛОДУ (12) соответственно. Следовательно,

$$x = a_{11}e_1 + a_{12}e_2 + \ldots + a_{1n-1}e_{n-1} + p^c x_{12} \text{ в } B_1,$$

$$x = a_{21}s_1 + a_{22}s_2 + \ldots + a_{2n-1}s_{n-1} + q^d x_{22} \text{ в } B_2.$$

Но тогда имеют место представления

$$q^d x = a_{11}'e_1' + a_{12}'e_2' + \ldots + a_{1n-1}'e_{n-1}' + q^d p^c x_{12} =$$

$$= a_{11}'e_1' + a_{12}'e_2' + \ldots + a_{1n-1}'e_{n-1}' \text{ в } B_1,$$

$$p^c x = a_{21}'s_1' + a_{22}'s_2' + \ldots + a_{2n-1}'s_{n-1}' + p^c q^d x_{22} =$$

$$= a_{21}'s_1' + a_{22}'s_2' + \ldots + a_{2n-1}'s_{n-1}' \text{ в } B_2,$$

где $a'_{1i} = a_{1i} q^d$, $a'_{2i} = a_{2i} p^c$. Таким образом, задача свелась к рассмотренному выше случаю. ■

Если модуль m имеет представление $m = p_1^{k_1} p_2^{k_2} \dots p_r^{k_r}$, то множество всех решений ЛОДУ образует модуль V над кольцом Z_m. А множество решений, которые представляются линейными комбинациями векторов из B_i, $i = 1, \dots, r$, являются подмодулями V_i модуля V, которые порождены базисами B_i. Тогда модуль V разлается в прямую сумму подмодулей V_i, т.е. в данном случае

$$V = V_1 \oplus V_2 \oplus \dots \oplus V_r.$$

Это значит, что произвольный элемент $x \in V$ имеет вид $x = x_1 + x_2 + \dots + x_r$, где $x_i = d_1 s_{i1} + d_2 s_{i2} + \dots + d_{j_i} s_{ij_i}$ принадлежит V_i, $s_{ij_i} \in B_i$, а $d_1, d_2, \dots, d_{j_i}$ принадлежат Z_{M_i}, $M_i = \dfrac{m}{p_i^{k_i}}$, $i = 1, 2, \dots, r$.

Данная ситуация демонстрируется следующим примером.

Пример 1. Построить базис множества всех решений в кольце Z_{24} для ЛОДУ $2x + 3y + 8z + 6u + 4v = 0$.

Решение. Модуль $m = 24 = 3 \cdot 8$, отсюда получаем два ЛОДУ:

$$L_1(x) = 2x + 0y + 2z + 0u + v = 0 \text{ в поле } F_3,$$

$$L_2(x) = 2x + 3y + 0z + 6u + 4v = 0 \text{ в кольце } Z_8.$$

Строим базисы множеств решений этих ЛОДУ *TSS*-методом:

$$B'_1 = \{(2, 0, 1, 0, 0), (0, 1, 0, 0, 0), (1, 0, 0, 0, 1), (0, 0, 0, 1, 0)\},$$

$$B'_2 = \{(5, 2, 0, 0, 0), (0, 0, 1, 0, 0), (0, 6, 0, 5, 0), (0, 4, 0, 0, 5)\}.$$

Следовательно,

$$B_1 = 8 \cdot B'_1 = \{(16, 0, 8, 0, 0), (0, 8, 0, 0, 0), (8, 0, 0, 0, 8), (0, 0, 0, 8, 0)\},$$

$$B_2 = 3 \cdot B'_2 = \{(15, 6, 0, 0, 0), (0, 0, 3, 0, 0), (0, 18, 0, 15, 0), (0, 12, 0, 0, 15)\}.$$

Отсюда получаем базис множества решений ЛОДУ

$$B = B_1 \bigcup B_2 = \{(16, 0, 8, 0, 0), (0, 8, 0, 0, 0), (8, 0, 0, 0, 8), (0, 0, 0, 8, 0),$$

$$(15, 6, 0, 0, 0), (0, 0, 3, 0, 0), (0, 18, 0, 15, 0), (0, 12, 0, 0, 15)\}.$$

Так, решения (0, 0, 0, 4, 0) и (3, 0, 1, 1, 1) имеют следующие представления через базисные решения:

$$(0, 0, 0, 4, 0) = 2(0, 0, 0, 8, 0) + 4(0, 18, 0, 15, 0) = (0, 72, 0, 76, 0),$$

$$(3, 0, 1, 1, 1) = 2(16, 0, 8, 0, 0) + 2(8, 0, 0, 0, 8) + 2(0, 0, 0, 8, 0) + 5(15, 6, 0, 0, 0) +$$

$$+ 3(0, 0, 3, 0, 0) + 7(0, 18, 0, 15, 0) + 7(0, 12, 0, 0, 15) = (75, 240, 25, 121, 121).$$

Конец примера.

TSS-МЕТОД РЕШЕНИЯ ОБЩЕГО ВИДА СЛОДУ

Из приведенных теорем вытекает процедура построения базиса множества решений СЛОДУ (1) в кольце Z_m, которая состоит в разбиении СЛОДУ S на r подсистем $S_1, \dots, S_r$ по модулям $p_1^{k_1}, \dots, p_r^{k_r}$ соответственно. Каждая из этих подсистем решается отдельно *TSS*-алгоритмом, находятся базисы $B_1, \dots, B_r$ со-

ответственно для $S_1, \dots, S_r$, а затем строится базис $B = \frac{m}{p_1^{k_1}} B_1 \cup \dots \cup \frac{m}{p_r^{k_r}} B_r$, где $\frac{m}{p_i^{k_i}} B_i$ означает умножение каждого вектора из B_i на $\frac{m}{p_i^{k_i}}$.

Пример 2. Построить базис множества всех решений СЛОДУ

$$S = \begin{cases} 2x + 3y + 8z + 6u + 4v = 0, \\ 4x + 6y + 2z + 3u + 2v = 0, \\ 2x + 3y + 2z + 2u + 8v = 0 \end{cases} \pmod{120}.$$

Решение. В результате разложения модуля $m = 120 = \dot{3} \cdot 5 \cdot 8$ получаем три СЛОДУ:

$$S_1 = \begin{cases} L_{11} = 2x + 0y + 2z + 0u + 1v = 0, \\ L_{12} = 1x + 0y + 2z + 0u + 2v = 0, \\ L_{13} = 2x + 0y + 2z + 2u + 2v = 0 \end{cases} \pmod{3},$$

$$S_2 = \begin{cases} L_{21} = 2x + 3y + 3z + 1u + 4v = 0, \\ L_{22} = 4x + 1y + 2z + 3u + 2v = 0, \\ L_{23} = 2x + 3y + 2z + 2u + 3v = 0 \end{cases} \pmod{5},$$

$$S_3 = \begin{cases} L_{31} = 2x + 3y + 0z + 6u + 4v = 0, \\ L_{32} = 4x + 6y + 2z + 3u + 2v = 0, \\ L_{33} = 2x + 3y + 2z + 2u + 0v = 0 \end{cases} \pmod{8}.$$

Решения СЛОДУ S_1 ищем в поле F_3, СЛОДУ S_2 — в поле F_5, а СЛОДУ S_3 — в примарном кольце Z_8.

Базисы B_1' СЛОДУ S_1 и B_2' СЛОДУ S_2 находятся *TSS*-алгоритмом в полях Z_2 и Z_3, который описан в работе [4]. Эти базисы состоят из векторов $B_1' = \{(0, 1, 0, 0, 0), (1, 0, 0, 1, 1)\}$ и $B_2' = \{(1, 1, 0, 0, 0), (0, 0, 0, 3, 3)\}$.

Рассмотрим *TSS*-алгоритм построения базиса B_3' для СЛОДУ S_3. Строим базис множества решений для ЛОДУ $L_{31} = 0$ описанным выше способом. Для этого заменим коэффициент 3 его дополнением $-5 = 3 - 8$ и строим базисные решения:

$$B_{31} = \{(5, 2, 0, 0, 0), (0, 0, 1, 0, 0), (0, 6, 0, 5, 0), (0, 4, 0, 0, 5)\}.$$

Подставляя найденные решения из B_{31} в L_{32}, находим значения: 0, 2, 3, 2. Составляем уравнение $0x + 2y + 3z + 2u = 0 \pmod 8$. Заменяем коэффициент 3 его дополнением -5 и находим решения: (1, 0, 0, 0), (0, 5, 2, 0), (0, 0, 2, 5). Этим решениям соответствуют базисные решения:

$$B_{32} = \{(5, 2, 0, 0, 0), (0, 4, 5, 2, 0), (0, 0, 0, 2, 1)\}.$$

Значения L_{33} на векторах из B_{32}: 0, 2, 4, и поскольку НОД $(0, 2, 4) = 2$, то решениями уравнения $0x + y + 2z = 0 \pmod 4$ будут векторы (1, 0, 0), (0, 2, 1) и (0, 4, 0). Этим решениям соответствуют базисные решения

$$B_3' = B_{33} = \{(5, 2, 0, 0, 0), (0, 0, 2, 6, 1)\} \cup \{(0, 0, 4, 0, 0)\}.$$

Домножая векторы из B_1' на $2^3 \cdot 5^1 = 40$, получаем базис множества решений для системы S_1:

$$B_1 = \{(0, 40, 0, 0, 0), (40, 0, 0, 40, 40)\}.$$

Домножая векторы из B_2' на $2^3 \cdot 3 = 24$, получаем базис множества решений для системы S_2:

$$B_2 = \{(24, 24, 0, 0, 0), (0, 0, 0, 72, 72)\}.$$

Домножая векторы из B_3' на $3^1 \cdot 5^1 = 15$, получаем базис для системы S_3:

$$B_3 = \{(75, 30, 0, 0, 0), (0, 0, 30, 90, 15), (0, 0, 60, 0, 0)\}.$$

Таким образом, окончательно базис множества решений для данной СЛОДУ принимает вид

$$B = B_1 \cup B_2 \cup B_3 = (0, 40, 0, 0, 0), (40, 0, 0, 40, 40), (24, 24, 0, 0, 0),$$

$$(0, 0, 0, 72, 72), (15, 30, 0, 0, 0), (0, 0, 30, 90, 15), (0, 0, 60, 0, 0)\}.$$

Конец примера.

Принимая во внимание, что арифметическая сложность выполнения операций сложения и вычитания в кольце Z_m пропорциональна s (s — максимальная разрядность чисел), сложность операций умножения и деления, как и вычисления НОД двух чисел, меньших m, пропорциональна s^2, то арифметическая сложность построения 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 $L(x)$ на НОД;
- $n^2 l^3$ — построение комбинаций векторов, которые составляют базис множества решений ЛОДУ ($l = \max(n, s, r)$).

Следовательно, арифметическая сложность перехода от предыдущего к следующему ЛОДУ в одной подсистеме пропорциональна величине l^5, где $l = \max(n, s, r)$, $s = \log m$. Такая процедура повторяется r раз, в результате имеем $O(l^6)$, где $l = \max(n, s, k, r)$. Таким образом, имеет место следующее утверждение.

Теорема 7. Множество B, построенное *TSS*-методом, является базисом множества решений СЛОДУ (1). Арифметическая сложность построения B пропорциональна величине $O(l^6)$, где $l = \max(n, s, k, r)$.

TSS-МЕТОД РЕШЕНИЯ СЛНДУ

Построение базиса множества решений СЛНДУ сводится к построению базиса множества решений расширенной СЛОДУ вида (2), которая соответствует СЛНДУ. Найдя базис множества решений расширенной СЛОДУ, построим в нем решения $x_1, \ldots, x_t$, в которых последняя координата равна единице (если для некоторой подсистемы такого решения не существует, то исходная СЛНДУ несовместна). Составляем сравнение

$$c_1 m_1 + \ldots + c_t m_t \equiv 1 \pmod{m}, \tag{13}$$

и если оно имеет решение $(u_1, \ldots, u_t)$, то СЛНДУ совместна и линейная комбинация

$$x^1 = u_1 x_1 + \ldots + u_t x_t$$

представляет частное решение СЛНДУ, остальные векторы из базиса СЛОДУ будут решениями СЛОДУ, которая соответствует данной СЛНДУ.

Правильность описанной процедуры вытекает из доказанных выше теорем и лемм. Характеристику временной сложности определяет теорема 7.

Рассмотрим иллюстрирующий пример.

Пример 3 (задача о математическом сейфе [5]). Математическим сейфом называется система $S(Z, b, A, k)$, где $Z = \{z_{11}, z_{12}, \ldots, z_{m-1n}, z_{mn}\}$ — множество замков, расположенных в виде прямоугольной матрицы A размера $m \times n$, которая определяет вектор состояния замков $b = (b_1, b_2, \ldots, b_{mn})$, где $b_i \in \{0, 1, \ldots, k-1\}$, а $k \in N$ — модуль кольца вычетов Z_k, в котором решается задача. В результате одного поворота ключа a_{ij} по часовой стрелке все замки в строке i и столбце j матрицы A переходят из состояния b в состояние $(b+1) \pmod{k}$. Сейф считается откры-

тым, если он находится в состоянии $b = (0, 0, \dots, 0)$. Решение задачи состоит в нахождении для каждого замка z_{ij} такого количества поворотов x_{ij} ключом, чтобы сейф открылся. Пусть $X = ||\, x_{ij} \,||$ — решение задачи, где x_{ij} равно числу поворотов ключа в замке z_{ij}. Тогда сейф откроется, если $\sum\limits_{t=1}^{n} x_{it} + \sum\limits_{t=1,\, t\neq i}^{m} x_{tj} + b_{ij} \equiv 0 \pmod{k}$.

Обозначим $x = (x_{11}, x_{12}, \dots, x_{1n}, x_{21}, x_{22}, \dots, x_{2n}, \dots, x_{mn-1}, x_{mn})$ вектор-столбец, полученный из матрицы X последовательной записью ее строк.

Пусть требуется открыть сейф $Z = \{z_{11}, \dots, z_{24}\}$ в кольце вычетов по модулю $k = 6$ с матрицей

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

Решение. Строим СЛОДУ вида (поскольку в вычислениях фигурируют только коэффициенты матрицы системы, неизвестные x_{ij} в записи систем опускаются)

$$Cx = \begin{cases} 1\ 1\ 1\ 1\ 1\ 0\ 0\ 0\ 2 = 0, \\ 1\ 1\ 1\ 1\ 0\ 1\ 0\ 0\ 0 = 0, \\ 1\ 1\ 1\ 1\ 0\ 0\ 1\ 0\ 2 = 0, \\ 1\ 1\ 1\ 1\ 0\ 0\ 0\ 1\ 2 = 0, \\ 1\ 0\ 0\ 0\ 1\ 1\ 1\ 1\ 1 = 0, \\ 0\ 1\ 0\ 0\ 1\ 1\ 1\ 1\ 2 = 0, \\ 0\ 0\ 1\ 0\ 1\ 1\ 1\ 1\ 2 = 0, \\ 0\ 0\ 0\ 1\ 1\ 1\ 1\ 1\ 1 = 0 \end{cases} \pmod 6,$$

которая соответствует вектору $b = (2, 0, 2, 2, 1, 2, 2, 1)$, полученному из матрицы A. Решение такой СЛНДУ сводится к решению СЛОДУ в поле F_2 и поле F_3, поскольку модуль $k = 6$ имеет разложение на простые множители: $k = 2 \cdot 3$. Решаем СЛОДУ

$$Cx = \begin{cases} 1\ 1\ 1\ 1\ 1\ 0\ 0\ 0\ 2 = 0, \\ 1\ 1\ 1\ 1\ 0\ 1\ 0\ 0\ 0 = 0, \\ 1\ 1\ 1\ 1\ 0\ 0\ 1\ 0\ 2 = 0, \\ 1\ 1\ 1\ 1\ 0\ 0\ 0\ 1\ 2 = 0, \\ 1\ 0\ 0\ 0\ 1\ 1\ 1\ 1\ 1 = 0, \\ 0\ 1\ 0\ 0\ 1\ 1\ 1\ 1\ 2 = 0, \\ 0\ 0\ 1\ 0\ 1\ 1\ 1\ 1\ 2 = 0, \\ 0\ 0\ 0\ 1\ 1\ 1\ 1\ 1\ 1 = 0 \end{cases} \begin{matrix} \pmod 2, \\ \pmod 3. \end{matrix} \quad Cx = \begin{cases} 1\ 1\ 1\ 1\ 1\ 0\ 0\ 0\ 2 = 0, \\ 1\ 1\ 1\ 1\ 0\ 1\ 0\ 0\ 0 = 0, \\ 1\ 1\ 1\ 1\ 0\ 0\ 1\ 0\ 2 = 0, \\ 1\ 1\ 1\ 1\ 0\ 0\ 0\ 1\ 2 = 0, \\ 1\ 0\ 0\ 0\ 1\ 1\ 1\ 1\ 1 = 0, \\ 0\ 1\ 0\ 0\ 1\ 1\ 1\ 1\ 2 = 0, \\ 0\ 0\ 1\ 0\ 1\ 1\ 1\ 1\ 2 = 0, \\ 0\ 0\ 0\ 1\ 1\ 1\ 1\ 1\ 1 = 0 \end{cases}$$

Решением первой СЛОДУ является вектор $x_2 = (1, 0, 0, 1, 0, 0, 0, 0, 1)$, а второй СЛОДУ — вектор $x_3 = (0, 2, 2, 0, 0, 2, 0, 0, 1)$.

Домножаем первое решение на 3, а второе на 2, получаем векторы

$$x_2' = (3, 0, 0, 3, 0, 0, 0, 0, 3) \ \text{ и } \ x_3' = (0, 4, 4, 0, 0, 4, 0, 0, 2).$$

По последним координатам строим сравнение $3u + 2v \equiv 1 \pmod 6$. Это сравнение имеет решение $(u, v) = (1, 5)$. Строим линейную комбинацию $x' = x_2' + 5x_3' = (3, 2, 2, 3, 0, 2, 0, 0, 1)$, которая дает единственное решение исходной СЛНДУ $x = (3, 2, 2, 3, 0, 2, 0, 0)$ и решение задачи о сейфе со значениями $x_{11} = 3$, $x_{12} = 2$,

$x_{13}=2,\ x_{14}=3$ и $x_{22}=2$. Действительно,

$$\left(\begin{array}{c|c|c|c}3 & & & \\ \hline 2 & 0 & 2 & 2 \\ \hline 1 & 2 & 2 & 1\end{array}\right)\to\left(\begin{array}{c|c|c|c} & 2 & & \\ \hline 5 & 3 & 5 & 5 \\ \hline 4 & 2 & 2 & 1\end{array}\right)\to\left(\begin{array}{c|c|c|c} & & 2 & \\ \hline 1 & 5 & 1 & 1 \\ \hline 4 & 4 & 2 & 1\end{array}\right)\to\left(\begin{array}{c|c|c|c} & & & 3 \\ \hline 3 & 1 & 3 & 3 \\ \hline 4 & 4 & 4 & 1\end{array}\right)\to$$

$$\to\left(\begin{array}{c|c|c|c}0 & 4 & 0 & 0 \\ \hline 4 & 4 & 4 & 4 \\ \hline & 2 & & \end{array}\right)\to\left(\begin{array}{cccc}0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0\end{array}\right).$$

ЗАКЛЮЧЕНИЕ

Приведенные алгоритмы имеют полиномиальные оценки временной сложности при условии известного разложения модуля на простые множители. Проблема разложения натурального числа на простые множители (так называемая проблема факторизации) является одной из наиболее актуальных проблем теории чисел. Существует несколько алгоритмов ее решения: алгоритмы Полларда, Полларда–Штрассена, а также алгоритм решета числового поля [6], который в настоящее время является наиболее эффективным. Все эти алгоритмы имеют экспоненциальные оценки временной сложности, и поиск более эффективных алгоритмов факторизации продолжается.

СПИСОК ЛИТЕРАТУРЫ

1. Крывый С.Л. Алгоритмы решения систем линейных диофантовых уравнений в кольцах вычетов // Кибернетика и системный анализ. — 2007. — № 6. — С. 27–40.
2. Крывый С.Л. Алгоритмы решения систем линейных диофантовых уравнений в целочисленных областях // Кибернетика и системный анализ. — 2006. — № 2. — С. 3–17.
3. Крывый С.Л. Алгоритмы решения систем линейных диофантовых уравнений в полях вычетов // Кибернетика и системный анализ. — 2007. — № 2. — С. 15–23.
4. Донец Г.А. Решение задачи о сейфе на (0, 1)-матрицах // Кибернетика и системный анализ. — 2002. — № 1. — С. 98–105.
5. Донец Г.А., Агаи Аг Гамиш Якуб. Задача о математическом сейфе на матрицах. — Киев: Ин-т кибернетики им. В.М. Глушкова НАНУ, 2013. — С. 124–131.
6. Черемушкин А.В. Лекции по арифметическим алгоритмам в криптографии. — М.: МЦНМО, 2002. — 103 с.

Надійшла до редакції 08.02.2016

С.Л. Кривий

АЛГОРИТМИ РОЗВ'ЯЗАННЯ СИСТЕМ ЛІНІЙНИХ РІВНЯНЬ В КІЛЬЦЯХ ЛИШКІВ

Анотація. Запропоновано поліноміальні алгоритми побудови базису множини розв'язків системи лінійних однорідних і неоднорідних діофантових рівнянь в кільці лишків за модулем деякого числа при умові відомого розкладу модуля на прості множники.

Ключові слова: кільце лишків, лінійні діофантові рівняння, базис множини розв'язків.

S.L. Kryvyi

SOLUTION ALGORITHMS FOR SYSTEMS OF LINEAR EQUATIONS OVER RESIDUE RINGS

Abstract. The author proposes polynomial algorithms to construct the base of the set of solutions of a system of linear Diophantine homogeneous and inhomogeneous equations in residue ring modulo some number provided that prime factorization of the modulo is known.

Keywords: ring of residues, linear Diophantine equations, set of basis solutions.

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