УДК 51.681.3

С.Л. КРЫВЫЙ

АЛГОРИТМ ПОСТРОЕНИЯ БАЗИСА МНОЖЕСТВА РЕШЕНИЙ СИСТЕМ ЛИНЕЙНЫХ ДИОФАНТОВЫХ УРАВНЕНИЙ В КОЛЬЦЕ ЦЕЛЫХ ЧИСЕЛ

Ключевые слова: *кольцо целых чисел, линейные диофантовые уравнения, предбазис, базис множества решений.*

Линейные диофантовые уравнения и системы таких уравнений часто встречаются в различных прикладных областях науки о вычислениях. К решению таких уравнений и их систем сводятся задачи линейного целочисленного программирования, распознавания образов и математических игр [1, 2], криптографии [3], унификации [4], распараллеливания циклов [5] и т.д. При этом множеством, к которому принадлежат коэффициенты уравнений, является либо множество целых чисел, либо кольцо вычетов, либо поле вычетов по модулю некоторого числа, а множеством, в котором ищутся решения, является либо кольцо целых чисел, либо множество натуральных чисел, либо конечные поля и кольца вычетов. Алгоритмы поиска решений систем линейных диофантовых уравнений в множестве натуральных чисел описаны во многих публикациях [6–12]. В настоящей статье рассматривается алгоритм решения систем линейных диофантовых уравнений в кольце целых чисел. В основе предлагаемого алгоритма лежит TSS-метод, который применялся для построения минимального порождающего множества решений системы линейных однородных диофантовых уравнений в множестве натуральных чисел [1].

1. ПРЕДВАРИТЕЛЬНЫЕ СВЕДЕНИЯ

Системой линейных диофантовых уравнений (СЛДУ) в кольце целых чисел Z будем называть систему вида

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

где $a_{ij}, b_i, x_i \in Z$, $i=1,\ldots,n$, $j=1,\ldots,q$. Решением СЛДУ (1) называется такой вектор $c=(c_1,c_2,\ldots,c_n)$, который при подстановке вместо x_j значений c_j в $L_i(x)$ обращает $L_i(c)\equiv b_i$ в тождество для всех $i=1,2,\ldots,q$. СЛДУ называется однородной (СЛОДУ), если все b_i равны нулю; в противном случае — неоднородной (СЛНДУ).

2. *TSS*-МЕТОД РЕШЕНИЯ СЛОДУ

Рассмотрим СЛОДУ S вида (1), $e_1=(1,0,\ldots,0)$, $e_2=(0,1,\ldots,0),\ldots,e_n=(0,\ldots,0,1)$ — единичные векторы, которые называются векторами канонического базиса множества Z^n.

Пусть M — множество решений системы S. Поскольку она однородная, то нулевой вектор всегда является ее решением и называется тривиальным, а всякое решение системы S, отличное от нулевого, — нетривиальным.

СЛОДУ S будет несовместна, если множество M состоит только из тривиального решения, в противном случае S совместна.

TSS-метод, о котором речь пойдет дальше, и его реализация для систем уравнений над множеством натуральных чисел подробно описаны в [1]. Рассмотрим модификацию этого метода для случая кольца целых чисел Z.

Случай линейного однородного диофантового уравнения (ЛОДУ). Пусть дано ЛОДУ

$$L(x)=a_1x_1+\ldots+a_ix_i+\ldots+a_nx_n=0, \tag{2}$$

где $a_i, x_i \in Z,\ i=1,\ldots,n.$

Рассмотрим множество векторов канонического базиса $M_0=\{e_1,\ldots,e_n\}$ и функцию $L(x)=a_1x_1+a_2x_2+\ldots+a_nx_n$ ЛОДУ (2). Не ограничивая общности, предположим, что в функции $L(x)$ первым ненулевым коэффициентом будет a_1 и $a_1>0$. Построим множество векторов

$$B=\{e_1=(-a_2, a_1, 0,\ldots,0),\ e_2=(-a_3, 0, a_1, 0,\ldots,0),$$
$$e_{q-1}=(-a_q, 0, 0,\ldots,0, a_1)\}\cup M_0,$$

где $M_0=\{e_r:\ L(e_r)=0\}$, причем если для некоторого $a_i\neq 0$ наибольший общий делитель (НОД) $(a_i, a_1)\neq 1$, то сократим координаты такого вектора на этот НОД. Выбранный ненулевой коэффициент a_1 назовем основным. Таким образом, можно считать, что все векторы в множестве B таковы, что a_i и a_1 взаимно просты. Иными словами, множество B строится путем комбинирования первого ненулевого коэффициента с остальными ненулевыми коэффициентами, взятыми с противоположными знаками, и пополнения векторами канонического базиса, которые соответствуют нулевым коэффициентам ЛОДУ (2). Построенное таким образом множество будем называть *TSS-множеством, или предбазисом.* Очевидно, что векторы из множества B выступают решениями ЛОДУ (2), а само множество B замкнуто относительно сложения, вычитания и умножения на элемент из кольца Z.

Лемма 1. Пусть $x=(c_1, c_2,\ldots,c_q)$ — некоторое решение ЛОДУ (2), тогда если $x\notin B$, то x представляется в виде неотрицательной линейной комбинации вида

$$a_1x=c_2e_1+c_3e_2+\ldots+c_qe_{q-1},$$

где $e_i\in B,\ i=1,\ldots,q-1$.

Доказательство. Если $x=(c_1,\ldots,c_q)\in M$, то вектор

$$c_2e_1+c_3e_2+\ldots+c_qe_{q-1}=(-c_2a_2-c_3a_3-\ldots-c_qa_q, c_2a_1,\ldots,c_qa_1)=$$
$$=(c_1a_1, c_2a_1,\ldots,c_qa_1)=a_1(c_1, c_2,\ldots,c_q)=a_1x$$

в силу того, что x — решение ЛОДУ (2), т.е. $a_1c_1=-a_2c_2-a_3c_3-\ldots-a_qc_q$.

Заметим, что если некоторый вектор e_j из B является вектором канонического базиса и j-я координата вектора x равна c_j, то в представлении вектора x вектор e_j входит с коэффициентом a_1c_j.

Лемма доказана.

Из леммы вытекает полезное следствие.

Следствие 1. Если среди коэффициентов ЛОДУ имеется хотя бы один коэффициент, равный 1, то множество B — базис множества всех решений ЛОДУ.

Действительно, если $a_1=1$, то элементы множества B имеют вид

$$\{e_1=(-a_2, 1, 0,\ldots,0),\ e_2=(-a_3, 0, 1, 0,\ldots,0),\ e_{q-1}=(-a_q, 0, 0,\ldots,0, 1)\}\cup M_0,$$

т.е. в разложении произвольного решения x по векторам из множества B основной коэффициент согласно лемме 1 будет равным единице. А это и означает, что множество B будет базисом.

Пример 1. Построить TSS ЛОДУ $L(x)=3x_1+y-z+2u+v=0$. Предбазис, или TSS этого ЛОДУ имеет вид

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

Решения ЛОДУ $x_1 = (0,2,3,0,1)$, $x_2 = (1,1,0,-2,0)$ имеют представления $3x_1 = 2e_1 + 3e_2 + e_4$, $3x_2 = e_1 - 2e_3$. Если в качестве основного коэффициента выбрать $a_2 = 1$, то базисом множества всех решений для ЛОДУ будет множество

$$B = \{e_1 = (1,-3,0,0,0),\ e_2 = (0,1,1,0,0),\ e_3 = (0,-2,0,1,0),\ e_4 = (0,-1,0,0,1)\}.$$

В этом базисе векторы x_1 и x_2 имеют представление $x_1 = 3e_2 + e_4$, $x_2 = e_1 - 2e_3$.

Случай системы линейных однородных диофантовых уравнений. Рассмотрим теперь СЛОДУ

$$S = \begin{cases} L_1(x) = a_{11}x_1 + \ldots + a_{1n}x_n = 0, \\ L_2(x) = a_{21}x_1 + \ldots + a_{2n}x_n = 0, \\ \ldots \quad \ldots \quad \ldots \quad \ldots\ldots\ldots \quad \ldots \quad \ldots\ldots \\ L_q(x) = a_{q1}x_1 + \ldots + a_{qn}x_n = 0, \end{cases} \tag{3}$$

где a_{ij}, $x_i \in Z$, $i = 1,\ldots,q$, $j = 1,\ldots,n$.

Построим предбазис $B_1 = \{e_1^1, e_2^1, \ldots, e_{q-1}^1\}$ для первого уравнения $L_1(x) = 0$ и вычислим значения $L_2(e_i^1) = b_i$, где $e_i^1 \in B_1, b_i \in Z$. Составим уравнение

$$b_1 y_1 + \ldots + b_i y_i + \ldots + b_{q-1} y_{q-1} = 0 \tag{4}$$

и построим для него предбазис $B_1' = \{s_1, \ldots, s_{q-2}\}$. Векторам s_i из B_i' соответствуют векторы-решения $B_2 = \{e_1^2, \ldots, e_{q-2}^2\}$ СЛОДУ $L_1(x) = 0 \wedge L_2(x) = 0$.

Лемма 2. Множество векторов B_2 составляет предбазис СЛОДУ $L_1(x) = 0 \wedge \wedge L_2(x) = 0$, т.е. любое решение x этой СЛОДУ имеет представление $mx = l_1 e_1^2 + \ldots \ldots + l_{q-2} e_{q-2}^2$, где $e_i^2 \in B_2, l_i \in Z$, $i = 1,\ldots,q-2$, $m \in Z$.

Доказательство. Пусть x — произвольное решение СЛОДУ $L_1(x) = 0 \wedge \wedge L_2(x) = 0$. Поскольку x — решение $L_1(x) = 0$, то в силу леммы 1 x можно представить в виде

$$dx = a_1 e_1^1 + \ldots + a_{q-1} e_{q-1}^1,$$

где $e_i^1 \in B_1$, $a_i \in Z$, $i = 1,\ldots,q-1$. Тогда в силу того, что x — решение $L_2(x) = 0$, получаем $L_2(dx) = a_1 b_1 + \ldots + a_{q-1} b_{q-1} = 0$, где $b_j = L_2(e_j^1)$, $j = 1,\ldots,q-1$. Следовательно, вектор $a = (a_1,\ldots,a_{q-1})$ — решение ЛОДУ (4) и в силу леммы 1 получаем $ka = d_1 s_1 + \ldots + d_{q-2} s_{q-2}$, где $s_i \in B_1'$, $d_i \in Z$, $i = 1,\ldots,q-2$, а k — основной коэффициент ЛОДУ. Отсюда следует, что $kdx = d_1 e_1^2 + \ldots + d_{q-2} e_{q-2}^2$, где $e_i^2 \in B_2$, $i = 1,\ldots,q-2$, $m = k \cdot d$.

Лемма доказана.

С помощью математической индукции и лемм 1 и 2 докажем справедливость теоремы.

Теорема 1. *TSS* СЛОДУ (2) *B*, построенное описанным выше способом, является предбазисом множества всех решений СЛОДУ.

Пример 2. Найдем предбазис для СЛОДУ

$$S = \begin{cases} L_1(x) = 3x_1 + x_2 - x_3 + 2x_4 + x_5 = 0, \\ L_2(x) = 2x_1 + 3x_2 + 0x_3 - x_4 + 2x_5 = 0. \end{cases}$$

Базис для первого уравнения построен в примере 1:

$$B_1 = \{e_1^1 = (1,-3,0,0,0),\ e_2^1 = (0,1,1,0,0),\ e_3^1 = (0,-2,0,1,0),\ e_4^1 = (0,-1,0,0,1)\}.$$

Значения $L_2(x)$ на этих векторах равны соответственно $-7, 3, -7, -1$. Составляем уравнение $-7y_1 + 3y_2 - 7y_3 - y_4 = 0$ и строим предбазис множества решений ЛОДУ:

$$B_1' = \{s_1 = (3,7,0,0),\ s_2 = (-1,0,1,0),\ s_3 = (-1,0,0,7)\}.$$

Этим векторам соответствуют TSS-векторы (предбазис) исходной СЛОДУ

$$B_2 = \{e_1^2 = (3,-2,7,0,0),\ e_2^2 = (-1,1,0,1,0),\ e_3^2 = (-1,-4,0,0,7)\}.$$

Если при построении предбазиса уравнения $-7y_1 + 3y_2 - 7y_3 - y_4 = 0$ комбинирование вести по последнему значению (т.е. по –1), то получаем такой базис множества всех решений данной СЛОДУ:

$$\{e_1^2 = (1,4,0,0,-7),\ e_2^2 = (0,-2,1,0,3),\ e_3^2 = (0,5,0,1,-7)\}.$$

Принимая во внимание следствие 1, результат теоремы 1 можно усилить введением избыточности в предбазис на основании того, что значения коэффициентов в уравнении $L_1(x) = a_{11}x_1 + a_{12}x_2 + \ldots + a_{1n}x_n = 0$ взаимно просты. Благодаря этому всегда можно добиться, чтобы среди значений $L_1(x)$ была единица. Не ограничивая общности, будем предполагать, что НОД(a_{11}, a_{12}, a_{13}) = 1, т.е. первые три коэффициента взаимно просты в $L_1(x)$. Тогда существуют числа d_1, d_2, d_3 такие, что на векторе $y = (d_1, d_2, d_3, 0, \ldots, 0)$ значение $L_1(y) = 1$. Добившись этого, вычислим значения $L_1(x)$ на векторах канонического базиса. Построим предбазис B_1, комбинируя вектор y с остальными векторами для получения предбазиса. Заметим, что векторы из B_1 имеют вид

$$e'_1 = -a_{11}y + e_1,\ e'_2 = -a_{12}y + e_2,$$
$$e'_3 = -a_{13}y + e_3,\ e'_4 = -a_{14}y + e_4, \ldots, e'_n = -a_{1n}y + e_n, \tag{5}$$

где e_i — векторы канонического базиса, a_{ij} — коэффициенты в уравнении $L_1(x) = 0$. В координатной форме векторы e'_i имеют следующий вид:

$$e'_1 = (-a_{11}d_1 + 1, -a_{11}d_2, -a_{11}d_3, 0, \ldots, 0),$$
$$e'_2 = (-a_{12}d_1, -a_{12}d_2 + 1, -a_{12}d_3, 0, \ldots, 0),$$
$$e'_3 = (-a_{13}d_1, -a_{13}d_2, -a_{13}d_3 + 1, 0, \ldots, 0),$$
$$e'_4 = (-a_{14}d_1, -a_{14}d_2, -a_{14}d_3, 1, \ldots, 0),$$
$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$
$$e'_n = (-a_{1n}d_1, -a_{1n}d_2, -a_{1n}d_3, 0, \ldots, 1).$$

Имеет место теорема 2.

Теорема 2. TSS ЛОДУ (2) B_1, построенное описанным выше способом, является базисом множества всех решений этого ЛОДУ.

Сложность построения базиса пропорциональна величине l^3, где l — максимальное из чисел m и n, n — число неизвестных в ЛОДУ, а m — максимальная длина двоичного представления коэффициентов ЛОДУ.

Доказательство. Пусть $x = (c_1, c_2, \ldots, c_n)$ — решение ЛОДУ $L_1(x) = 0$. Тогда вектор x имеет представление

$$x = c_1e'_1 + c_2e'_2 + c_3e'_3 + c_4e'_4 + \ldots + c_ne'_n =$$
$$([-c_1a_{11}d_1 + c_1 - c_2a_{12}d_1 - c_3a_{13}d_1 - c_4a_{14}d_1 - \ldots - c_na_{1n}d_1],$$
$$[-c_1a_{11}d_2 - c_2a_{12}d_2 + c_2 - c_3a_{13}d_2 - c_4a_{14}d_2 - \ldots - c_na_{1n}d_2],$$
$$[-c_1a_{11}d_3 - c_2a_{12}d_3 - c_3a_{13}d_3 + c_3 - c_4a_{14}d_3 - \ldots - c_na_{1n}d_3],\ c_4, \ldots, c_n) =$$
$$= (c_1, c_2, c_3, c_4, \ldots, c_n)$$

в силу того, что $L(x) = a_{11}c_1 + a_{12}c_2 + \ldots + a_{1n}c_n = 0$.

Сложность данного алгоритма определяется сложностью расширенного алгоритма Евклида, который вместе с НОД вычисляет и линейную комбинацию, представляющую этот НОД. Известно (см. [3]), что эта сложность выражается величиной $O(m\log m)$, где m — длина двоичной записи максимального из коэффициентов ЛОДУ. Этот алгоритм применяется не более n раз и тогда имеем оценку $O(mn\log m)$. Построение базиса B_1 требует не больше n^3 операций. Следовательно, общая оценка временной сложности алгоритма выражается величиной $O(l^3)$, где $l=\max(m,n)$.

Теорема доказана.

Из этой теоремы вытекает такое следствие.

Следствие 2. Временная сложность построения базиса множество всех решений СЛОДУ вида (3) пропорциональна величине $O(ql^3)$, где q — число уравнений СЛОДУ, а $l=\max(m,n)$.

Заметим, что первые три вектора e'_1, e'_2, e'_3 в представлении (5) линейно зависимы. Действительно, в силу того, что $a_{11}d_1+a_{12}d_2+a_{13}d_3=1$, имеем

$$d_1e'_1+d_2e'_2+d_3e'_3=0,$$

а используя координатное представление векторов, получаем

$$\begin{gathered}d_1e'_1+d_2e'_2+d_3e'_3=(a_{12}d_1d_2+a_{13}d_1d_3,\ -a_{11}d_1d_2, -a_{11}d_3, 0,\dots,0)+\\ +(-a_{12}d_1d_2, a_{11}d_1d_2+a_{13}d_2d_3, -a12d_2d_3, 0\dots,0)+\\ +(-a_{13}d_1d_3, -a_{13}d_2d_3, a_{11}d_1d_3+a_{12}d_2d_3, 0\dots,0)=0.\end{gathered}$$

Таким образом, один из векторов e'_1, e'_2, e'_3 можно удалить из базиса решений.

3. *TSS*-МЕТОД РЕШЕНИЯ СЛНДУ

Пусть S — СЛНДУ вида (1) и $b_q\neq 0$. Выполняя элиминацию свободных членов в первых $q-1$ уравнениях, преобразуем исходную СЛНДУ к виду

$$S'=\begin{cases} L'_1(x) &= a'_{11}x_1 + \dots + a'_{1n}x_n = 0,\\ L'_2(x) &= a'_{21}x_1 + \dots + a'_{2n}x_n = 0,\\ \dots & \dots\ \dots\ \dots\ \dots\ \dots\ \dots\ \dots \\ L'_{q-1}(x) &= a'_{q-11}x_1 + \dots + a'_{q-1n}x_n = 0,\\ L'_q(x) &= a'_{q1}x_1 + \dots + a'_{qn}x_n = b_q.\end{cases} \tag{6}$$

Построим базис множества решений СЛОДУ, состоящей из $q-1$ первых уравнений системы (6). Пусть это будут векторы $\{s_1,\dots,s_k\}$. Найдем значения $L_q(s_j)=a_j$, $j=1,\dots,k$, для которых верна следующая теорема.

Теорема 3. СЛНДУ вида (6) (а вместе с ней и СЛНДУ (1)) совместна тогда и только тогда, когда ЛНДУ $a_1y_1+a_2y_2+\dots+a_ky_k=b_q$ имеет хотя бы одно решение в множестве целых чисел.

Доказательство. Если уравнение $a_1y_1+a_2y_2+\dots+a_ky_k=b_q$ имеет решение $(c_1,c_2,\dots,c_k)$, то очевидно, что вектор $s=c_1s_1+c_2s_2+\dots+c_ks_k$ — решение СЛНДУ.

Если СЛНДУ совместна и $s=(k_1,k_2,\dots,k_n)$ — ее решение, то представим s в виде линейной комбинации через базисные векторы подсистемы, состоящей из первых $q-1$ однородных уравнений системы (6), т.е. $s=c_1s_1+c_2s_2+\dots+c_ks_k$. Тогда $L_q(s)=c_1a_1+c_2a_2+\dots+c_ks_k=b_q$ должно иметь ходя бы одно решение, поскольку s — решение СЛНДУ.

Теорема доказана.

Известно, что общее решение СЛНДУ имеет вид $y=x+\sum_{i=1}^{k}a_ix_i$, где x — частное решение СЛНДУ, x_i — базисные решения соответствующей СЛОДУ, a_i — произвольные целые числа, а k — количество базисных решений. Таким образом, для полного решения СЛНДУ необходимо построить базис множества решений ее СЛОДУ и найти одно из решений СЛНДУ. Поиск такого решения, как следует из изложенного выше, сводится к поиску решения уравнения $a_1 y_1 + a_2 y_2 + \ldots + a_k y_k = b_q$. Это решение можно найти, например, методом наименьшего коэффициента.

Пример 3. Проверить на совместность СЛНДУ

$$S = \begin{cases} L_1(x) = 2x_1 - 3x_2 + x_3 + x_4 + 0x_5 = 1, \\ L_2(x) = 3x_1 + x_2 + x_3 + 0x_4 - x_5 = -2. \end{cases}$$

Преобразованная СЛНДУ имеет вид

$$S' = \begin{cases} L_1'(x) = 7x_1 - 5x_2 + 3x_3 + 2x_4 - x_5 = 0, \\ L_2(x) = 3x_1 + x_2 + x_3 + 0x_4 - x_5 = -2. \end{cases}$$

Базис ЛОДУ $L_1(x)' = 0$ составляют векторы (здесь не нужно вычислять НОД коэффициентов, поскольку имеется коэффициент, равный 1)

$$(1,0,0,0,7), (0,1,0,0,-5), (0,0,1,0,3), (0,0,0,1,2).$$

Значения $L_2(x)$ на этих векторах равны -4, 6, –2, –2, их наибольший общий делитель равен 2 и является делителем свободного члена $b_2 = -2$. Следовательно, СЛНДУ имеет решение, т.е. совместна.

Если дана система

$$S' = \begin{cases} L_1'(x) = 7x_1 - 5x_2 + 3x_3 + 2x_4 - x_5 = 0, \\ L_2(x) = 3x_1 + x_2 + x_3 + 0x_4 - x_5 = -3, \end{cases}$$

то она не имеет решений в кольце целых чисел, поскольку НОД(–4, 6, –2, –2) = 2 не делит свободный член -3 и поэтому уравнение $-4x + 6y - 2z - 2u = -3$ не имеет решений.

В заключение заметим, что приведенные оценки временных сложностей можно уточнять, если прослеживать все детали процесса вычислений, происходящего в TSS-алгоритме. В данной работе ограничимся установлением того, что эти алгоритмы полиномиальны в арифметической модели сложности.

СПИСОК ЛИТЕРАТУРЫ

1. Крывый С.Л. Алгоритмы решения систем линейных диофантовых уравнений в целочисленных областях // Кибернетика и системный анализ. — 2006. — № 2. — С. 3–17.
2. Донец Г.А. Решение задачи о сейфе на (0,1)-матрицах // Там же. — 2002. — № 1. — С. 98–105.
3. Черемушкин А.В. Лекции по арифметическим алгоритмам в криптографии. — М.: МЦНМО, 2002. — 103 с.
4. Baader F., Ziekmann J. Unification theory. Handbook of Logic in Artificial Intelligence and Logic Programming. — Oxford: University Press, 1994. — P. 1–85.
5. Allen R., Kennedy K. Automatic translation of FORTRAN program to vector form // ACM Transactions on Programming Languages and systems. — 1987. — **9**, N 4. — P. 491–542.
6. Contejan E., Ajili F. Avoiding slack variables in the solving of linear diophantine equations and inequations // Theoret. Comput. Sci. — 1997. — **173**. — P. 183–208.
7. Pottier L. Minimal solution of linear diophantine systems: bounds and algorithms // Proc. of the Fourth Intern. Conf. on Rewriting Techn. and Appl. — Como. — Italy. — 1991. — P. 162–173.
8. Domenjoud E. Outils pour la deduction automatique dans les theories associatives-commutatives // Thesis de Doctorat d'Universite: Universite de Nancy I. — 1991.
9. Clausen M., Fortenbacher A. Efficient solution of linear diophantine equations // J. Symbolic Comput. — 1989. — **8**, N 1, 2. — P. 201–216.
10. Romeuf J. F. A polinomial Algorithm for Solvin systems of two linear Diophantine equations // TCS. — 1990. — **74**, N 3. — P. 329–340.
11. Filgueiras M., Tomas A.P. A fast method for finding the basis of non-negative solutions to a linear diophantine equation // J. Symbolic Comput. — 1995. — **19**, N 2. — P. 507–526.
12. Comon H. Constraint solving on terms: Automata techniques (Preliminary lecture notes). Intern. Summer School on Constraints in Comput. Logics: Gif-sur-Yvette, France, September 5–8. — 1999. — 22 p.

Поступила 08.07.2009