Parametric Solutions of System of Linear Diophantine Equations by Crushing Method

P. Anuradha Kameswari* and Aweke Belay

1Department of Mathematics, Andhra University, Visakhapatnam - 530003, Andhra Pradesh, India.

Authors’ contributions
This work was carried out in collaboration between both authors. Both authors read and approved the final manuscript.

Article Information
DOI: 10.9734/ARJOM/2021/v17i930330

Received: 22 August 2021
Accepted: 27 October 2021

Abstract
There are studies on parametric solutions of system of Linear Diophantine equations based on uni-modular reductions of the coefficient matrix. In this paper we generate parametric solutions, with uni-modular row reductions on the coefficient matrix, based on the steps used in obtaining gcd of the coefficients in a row by crushing method. This application of gcd by crushing specifies an order for the row reductions and enables to give algorithm for the computations.

Keywords: Diophantine equations; parametric solutions.

2010 Mathematics Subject Classification: 94A60, 11T71.

1 Introduction
A general system of Linear Diophantine equations is written as \( AX = B \). A Linear Diophantine equation given as \( a_1x_1 + a_2x_2 + \cdots + a_nx_n = b \) may also be represented as \( AX = b \) for \( A = (a_1, a_2, \ldots, a_n) \) and \( X = (x_1, x_2, \ldots, x_n) \). The study of solutions of Linear Diophantine equations

*Corresponding author: E-mail: panuradhakameswari@yahoo.in;
with two variables is extended to $n$ variables for $n > 2$ in [1], [2], [3]. The existence of solutions is based on a relation between greatest common divisor of all the coefficients and the constant coefficient of the given Linear Diophantine equation. There are several studies on solutions of Systems of Linear Diophantine equations given in [4],[5],[6],[7],[8]. In [9],[10], parametric solutions of system of Linear Diophantine equations generated using uni-modular row reductions on the coefficient matrix, are discussed. In this paper, we generate parametric solutions of system of Linear Diophantine equations with uni-modular row reductions on the coefficient matrix, based on the steps used in obtaining gcd of coefficients by crushing method. In this context the theorems in [1] on existence of solutions and the conditions for existence of infinitely many solutions for linear Diophantine equations are mentioned in the following. In section 2 parametric solutions of system of Linear Diophantine Equations are generated with row reductions by crushing method and algorithm for the computations are also given.

**Definition 1.1.** A Linear Diophantine equation in $n$ variables is an equation of the form $a_1x_1 + a_2x_2 + \cdots + a_nx_n = b$, where $b, a_i$, are all integers for all $i = 1, 2, \ldots, n$ and $x_1, x_2, \ldots, x_n$ are unknowns in integers.

**Theorem 1.2.** The equation $a_1x_1 + a_2x_2 + \cdots + a_nx_n = b$ has infinitely many integer solutions if and only if $gcd(a_1, a_2, \ldots, a_n)$ divides $b$

**Proof.** Follows from [2],[1] □

**Note 1.3.** The gcd of the coefficients may be computed using the formula $gcd(a_1, a_2, \ldots, a_n) = gcd(a_1, a_2, \ldots, gcd(a_{n-1}, a_n))$. In this formula the computation of $gcd$ of $n$ terms is reduced to computation of $gcd$ of $n-1$ terms.

**Definition 1.4.** The gcd of $n$ integers $a_1, a_2, \ldots, a_n$ computed using the formula $gcd(a_1, a_2, \ldots, a_n) = gcd(a_1, a_2, \ldots, gcd(a_{n-1}, a_n))$ is called gcd by crushing.

**Definition 1.5.** A matrix $A$ is said to be in row echelon form if

(i) All the zero rows are at the bottom of the matrix.

(ii) The leading entry(i.e. the first nonzero entry) in each non zero row is to the right of all the leading entries in the rows above it [9].

Any matrix $A$ over integers can be converted into a row reduced echelon form with integer entries by modular row reductions defined in the following.

**Definition 1.6.** Modular row reductions are simple matrix row operations as follows:

(i) Exchange of two rows i.e. $R_i \rightarrow R_j$

(ii) Multiply a row by -1 i.e. $R_i \rightarrow -1R_i$

(iii) Replace a row $R_i$ by $R_i + kR_j$ for $j \neq i$ and $k \in \mathbb{Z}$ [9],[7],[11],[12]

In the following section, theorems on generating parametric solutions for system of Linear Diophantine equations in $n$ variables with infinitely many integer solutions are proved.

## 2 Parametric Solution of a System of Linear Diophantine Equations with Row Reduction by Crushing

In this section parametric solutions of system of Linear Diophantine Equations are generated by applying crushing method and algorithm for the computations are also given. We first prove the theorem on row reduction by crushing in the following.
Theorem 2.1. Let $a_1, a_2, \ldots, a_n$ be $n$ integers and if $d = \gcd(a_1, a_2, \ldots, a_n)$ then the column matrix
\[
\begin{pmatrix}
  a_1 \\
  a_2 \\
  \vdots \\
  a_n
\end{pmatrix}
\]
can be reduced to
\[
\begin{pmatrix}
  d \\
  0 \\
  \vdots \\
  0
\end{pmatrix}
\]
by uni modular reductions using $\text{gcd}$ by crushing.

Proof. Let $d = \gcd(a_1, a_2, \ldots, a_n)$ then if we consider $\text{gcd}$ by crushing we have
\[
d = \gcd(a_1, a_2, \ldots, a_n) \\
= \gcd(a_1, a_2, \ldots, \gcd(a_{n-1}, a_n)) \\
= \gcd(a_1, a_2, \ldots, a_{n-2}, d_{n-1})
\]
for $\gcd(a_{n-1}, a_n) = d_{n-1}$

Now to reduce
\[
\begin{pmatrix}
  a_1 \\
  a_2 \\
  \vdots \\
  a_n
\end{pmatrix}
\]
to
\[
\begin{pmatrix}
  d \\
  0 \\
  \vdots \\
  0
\end{pmatrix},
\]
where $d = \gcd(a_1, a_2, \ldots, a_n)$. Start the transformation with row reduction of the last two rows based on the extended euclidean algorithm for $\gcd(a_n, a_{n-1})$ as follows:

Let $d_{n-1} = \gcd(a_n, a_{n-1})$, consider the row reductions
\[
R_n \rightarrow -R_n \text{ if } a_{1n} < 0 \\
R_{n-1} \rightarrow -R_{n-1} \text{ if } a_{1n-1} < 0 \\
R_n \rightarrow R_{n-1} \text{ if } a_{1n} > a_{1n-1}
\]
i.e. WLOG we assume $a_{n-1} > a_n > 0$, then for $a_{n-1} > a_n$ by division algorithm we have $a_{n-1} = a_n k_1 + r_1$, as $k_1$ is an integer for the uni modular row reduction
\[
R_{n-1} \rightarrow R_{n-1} - k_1 R_n
\]
we have \( \begin{pmatrix} a_{n-1} \\ a_n \end{pmatrix} \) transformed to \( \begin{pmatrix} r_1 \\ a_n \end{pmatrix} \), now repeat the above procedure for \( \begin{pmatrix} r_1 \\ a_n \end{pmatrix} \), consider row reduction $R_n \rightarrow R_{n-1}$, and by division algorithm, $a_n = r_1 k_2 + r_2$ for the uni modular row reduction $R_{n-1} \rightarrow R_{n-1} - k_2 R_n$. Note \( \begin{pmatrix} r_1 \\ a_n \end{pmatrix} \) is transformed to \( \begin{pmatrix} r_2 \\ r_1 \end{pmatrix} \), continuing so on, we have uni modular reductions at each step of division algorithm in extended euclidean algorithm for $d_{n-1} = \gcd(a_n, a_{n-1})$ and the transformation for uni modular reduction at last division algorithm is
\[
\begin{pmatrix}
  a_1 \\
  a_2 \\
  \vdots \\
  a_{n-2} \\
  d_{n-1} \\
  0
\end{pmatrix}
\]
therefore the column matrix
\[
\begin{pmatrix}
  a_1 \\
  a_2 \\
  \vdots \\
  a_{n-1} \\
  a_n
\end{pmatrix}
\]
is transformed to
\[
\begin{pmatrix}
  a_1 \\
  a_2 \\
  \vdots \\
  a_{n-2} \\
  d_{n-1} \\
  0
\end{pmatrix}
\]
Now continue the transformation, by considering row reductions as above for the last two nonzero rows, i.e for $d_{n-2} = \gcd(a_{n-2}, d_{n-1})$
\[
\begin{pmatrix}
  a_1 \\
  a_2 \\
  \vdots \\
  a_{n-2} \\
  d_{n-1} \\
  0
\end{pmatrix}
\]
is transformed as
\[
\begin{pmatrix}
  a_1 \\
  a_2 \\
  \vdots \\
  a_{n-3} \\
  d_{n-2} \\
  0
\end{pmatrix},
\]
therefore continuing so on, with transformation considered
each time for last two non zero terms, we reach to
\[
\begin{pmatrix}
a_1 \\
d_2 \\
\vdots \\
0 \\
0 \\
\end{pmatrix}
\text{transformed to}
\begin{pmatrix}
d_1 \\
0 \\
\vdots \\
0 \\
0 \\
\end{pmatrix}
\]
for \(d_1 = \gcd(a_1, d_2)\)
\[
\begin{pmatrix}
a_1 \\
a_2 \\
\vdots \\
a_{n-1} \\
a_n \\
\end{pmatrix}
\text{is transformed to}
\begin{pmatrix}
d_1 \\
0 \\
\vdots \\
0 \\
0 \\
\end{pmatrix}
\]
where note the gcd \(d_1\) is the gcd \(d\) by crushing as
\[
d = \gcd(a_1, a_2, \ldots, a_{n-2}, a_{n-1}, a_n) \\
= \gcd(a_1, a_2, \ldots, a_{n-2}, \gcd(a_{n-1}, a_n)) \\
= \gcd(a_1, a_2, \ldots, a_{n-2}, d_{n-1}) \quad \text{for } d_{n-1} = \gcd(a_{n-1}, a_n) \\
= \gcd(a_1, a_2, \ldots, a_{n-3}, \gcd(a_{n-2}, d_{n-1})) \\
\vdots \\
= \gcd(a_1, a_2, \gcd(a_3, d_4)) \\
= \gcd(a_1, \gcd(a_2, d_3)) \\
= \gcd(a_1, d_2) \\
= d_1
\]
Therefore, the column matrix \(\begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{pmatrix}\) is transformed to \(\begin{pmatrix} d \\ 0 \\ \vdots \\ 0 \end{pmatrix}\) by unimodular reductions for \(d = \gcd(a_1, a_2, \ldots, a_n)\) is obtained with gcd by crushing.

A general system of \(m\) Linear Diophantine equations in \(n\) variables is written as \(AX = B\) is given as
\[
a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n = b_1 \\
a_{21}x_1 + a_{22}x_2 + \cdots + a_{2n}x_n = b_2 \\
\vdots \\
\vdots \\
a_{m1}x_1 + a_{m2}x_2 + \cdots + a_{mn}x_n = b_m
\]
for \(A = \begin{bmatrix}
a_{11} & a_{12} & \cdots & a_{1n-1} & a_{1n} \\
\vdots & \vdots & \ddots & \vdots & \vdots \\
a_{(m-1)1} & \cdots & a_{(m-1)n-1} & a_{(m-1)n} \\
a_{m1} & \cdots & a_{mn-1} & a_{mn} \\
\end{bmatrix}\)
and $B = \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_i \\ \vdots \\ b_m \end{pmatrix}$ and $X^t = (x_1, x_2, \ldots, x_n)$. In [9], parametric solutions of a general system Linear Diophantine equations generated using unimodular row reductions, are discussed in the following theorem:

**Theorem 2.2.** The system $AX = B$ has integer solutions if and only if the system $R^tK = B$ has integer solutions for $K$, where $R$ is a row echelon form obtained from unimodular row reductions of $[A^t|I]$ to $[R|T]$ and all the solutions of $AX = B$ are of the form $X = T^tK$.

**Proof.** Follows from [9] □

Now transform $[A^t|I]$ to $[R|T]$ where $I$ is an $n \times n$ identity matrix with unimodular row reductions using gcd by crushing as in theorem 2.1 and obtain an row echelon form $R$. Now as $R$ is row echelon form the matrix equation $R^tK = B$ can be solved for $K$ easily. Therefore by above theorem 2.2 if $R^tK = B$ is solvable in integers then we have integer solutions for $AX = B$ given of the form $X = T^tK$. The process of transformation of $[A^t|I]$ to $[R|T]$ with unimodular row reductions using gcd by crushing is as given in the following.

1. Transform the first column $C_1 = \begin{pmatrix} a_{11} \\ a_{12} \\ \vdots \\ a_{1(n-1)} \\ \vdots \\ a_{1n} \end{pmatrix}$ of $A^t$ by crushing to $\begin{pmatrix} d_1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$, where $d_1 = \gcd(a_{11}, a_{12}, \ldots, a_{1n})$.

\[ \begin{pmatrix} a_{j1} \\ a_{j2} \\ \vdots \\ a_{j(i-1)} \\ \vdots \\ a_{jn} \end{pmatrix} \]

2. All the columns $C_j$ are also transformed by crushing as $\begin{pmatrix} a_{j1} \\ a_{j2} \\ \vdots \\ a_{j(i-1)} \\ d_j \\ 0 \\ \vdots \\ 0 \end{pmatrix}$, where $d_j = \gcd(a_{jj}, a_{jj+1}, \ldots, a_{jn})$ is the $jj^{th}$ entry of reduced matrix.

3. The echelon form $R$ obtained by the uni-modular row reductions with gcd by crushing is of the form as follows
The algorithm to transform $[A'|I]$ as $[R|T]$ with the uni-modular row reductions using gcd by crushing to obtain the echelon form $R$ is given in the following steps for

$$\begin{bmatrix} a_{11} & a_{21} & \cdots & a_{m-1} & a_{m1} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ a_{1n-1} & a_{1n} & \cdots & a_{m-1n} & a_{mn} \end{bmatrix}$$

Algorithm 1 To transform $[A'|I]$ to $[R|T]$ with row reductions by crushing

**step 1:** Transform $[A'|I]$ using the reductions

$$R_n \rightarrow -R_n \text{ if } a_{1n} < 0$$

$$R_{n-1} \rightarrow -R_{n-1} \text{ if } a_{1n-1} < 0$$

$$R_n \rightarrow R_{n-1} \text{ if } a_{1n} > a_{1n-1}$$

**step 2:** Compute the division algorithm $a_{1n-1} = a_{1n}k_1 + r_1$, and then reduce, the transformed form in step 1 by using the uni-modular row reduction

$$R_{n-1} \rightarrow R_{n-1} - k_1 R_n$$

**step 3:** Repeat step 1 and step 2 for $a_{1n}$, and $r_1$, if $r_1 \neq 0$ with division algorithm as $a_{1n} = r_1k_2 + r_2$. Again repeat step 1 and step 2 for $r_1$ and $r_2$ if $r_2 \neq 0$ with division algorithm as $r_1 = r_2k_3 + r_3$ and so on continue repeating step 1 and step 2 for some $t$ times until the remainder $r_t = 0$, giving $r_{t-1} = \gcd(a_{1n}, a_{1(n-1)}) = d_{n-1}$.

After Step 1, step 2, step 3 the transformed matrix $A'$ has $C_1$ with $a_{1n}$ transformed to 0, and $a_{1(n-1)}$ transformed to $d_{n-1}$

**step 4:** Repeat step 3 to $(n-2)^{th}$ entry and $d_{(n-1)}$ in $(n-1)^{th}$ entry for transformed form after step 3 and after obtaining $\gcd(a_{i(n-2)}, d_{(n-1)}) = d_{n-2}$ repeat step 3 for $(n-3)^{th}$ entry and $d_{(n-2)}$ in $(n-2)^{th}$ entry and repeat so on for $i$ times until $n-i = 1$ with $d_1$ in $11^{th}$ entry of the transformed matrix.

In Step 4 the $\gcd d_1$ is the $\gcd$ by crushing of the coefficients in column $C_1$.

**step 5:** Repeat all the above steps for all the columns $C_j$ until $A'$ is transformed to an upper triangular form with $d_j$ in $jj^{th}$ entry for all $j = 1, 2, \ldots, m$.  

$$R = \begin{bmatrix} d_1 & \ast & \cdots & \ast & \cdots & \ast \\ 0 & d_2 & \cdots & \ast & \cdots & \ast \\ \vdots & \vdots & \ddots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & d_j & \cdots & \ast \\ \vdots & \vdots & \ddots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 & \cdots & \ast \end{bmatrix}$$

where $d_j = \gcd(a_{jj}, a_{jj+1}, \ldots, a_{jn})$ for $j = 1, 2, \ldots, m$. 

$$\begin{bmatrix} \ast & \cdots & \ast & \cdots & \ast \\ \ast & \cdots & \ast & \cdots & \ast \\ \vdots & \vdots & \ddots & \vdots & \ddots \\ \ast & \cdots & \ast & \cdots & \ast \\ \ast & \cdots & \ast & \cdots & \ast \end{bmatrix}$$
Example 1. To solve the Linear Diophantine equation

\[ 2x_1 - 3x_2 + 48x_3 - 5x_4 + x_5 = -36 \]

using the above crushing method and given algorithm, first transform \([A']I\) to \([R|T]\) by applying the above algorithm step by step starting from last two rows, then for \(\gcd(2, -3, 48, -5, 1)\) by crushing we have \([A']I\) =

\[
\begin{bmatrix}
2 & 1 & 0 & 0 & 0 & 0 \\
-3 & 0 & 1 & 0 & 0 & 0 \\
48 & 0 & 0 & 1 & 0 & 0 \\
-5 & 0 & 0 & 0 & 1 & 0 \\
1 & 0 & 0 & 0 & 0 & 1 \\
\end{bmatrix}
\]

transformed as

\[
[R|T] =
\begin{bmatrix}
1 & 0 & 0 & 0 & 0 & 1 \\
0 & 1 & 0 & 0 & 0 & -2 \\
0 & 0 & -1 & 0 & 0 & -3 \\
0 & 0 & 0 & 1 & 0 & -48 \\
0 & 0 & 0 & 0 & -1 & -5 \\
\end{bmatrix}
\]

Then to solve \(R'K = b\), where

\[
K = \begin{pmatrix} k_1 \\ k_2 \\ k_3 \\ k_4 \\ k_5 \end{pmatrix}
\]

Note for above \([R|T]\) \(k_1 = -36, k_2, k_3, k_4, K_5 \in \mathbb{Z}\) are arbitrary, we have the required solution \(X\) from \(T\) above as \(T'K = X\), i.e.

\[
\begin{bmatrix}
0 & 1 & 0 & 0 & 0 \\
0 & 0 & -1 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 \\
0 & 0 & 0 & 0 & -1 \\
1 & -2 & -3 & -48 & -5 \\
\end{bmatrix}
\begin{pmatrix}
k_2 \\
k_3 \\
k_4 \\
k_5 \\
\end{pmatrix}
= \begin{pmatrix}
-36 \\
k_2 \\
k_3 \\
k_4 \\
-5 \\
\end{pmatrix}
= \begin{pmatrix}
x_1 \\
x_2 \\
x_3 \\
x_4 \\
x_5 \\
\end{pmatrix}
\]

giving

\[
\begin{aligned}
x_1 &= k_2 \\
x_2 &= -k_3 \\
x_3 &= k_4 \\
x_4 &= -k_5 \\
x_5 &= -36 - 2k_2 - 3k_3 - 48k_4 - 5k_5,
\end{aligned}
\]

is a parametric solution of the given Linear Diophantine equation.

Example 2. To solve the system of Linear Diophantine equations

\[
\begin{aligned}
3x_1 + 4x_2 + 0x_3 + 22x_4 - 8x_5 &= 25 \\
6x_1 + 0x_2 + 0x_3 + 46x_4 - 12x_5 &= 2 \\
0x_1 + 4x_2 + 3x_3 - x_4 + 9x_5 &= 26
\end{aligned}
\]

using the above method and given algorithm, first transform \([A']I\) to \([R|T]\) by applying the above algorithm step by step starting from column one last two rows, by crushing we have \([A']I\) =
Now solving for $K$ from $R^t K = B$ we have for
\[
\begin{pmatrix}
1 & 0 & 0 & 0 & 0 \\
16 & 2 & 0 & 0 & 0 \\
26 & 978 & 1 & 0 & 0
\end{pmatrix}
\begin{pmatrix}
k_1 \\
k_2 \\
k_3 \\
k_4 \\
k_5
\end{pmatrix}
= 
\begin{pmatrix}
25 \\
2 \\
26
\end{pmatrix}
\]

where $k_1 = 25, k_2 = -199, k_3 = 193998, and k_4, k_5 \in \mathbb{Z}$ is arbitrary, then we have the required solution $X$ from $T$ above, as $T^t K = X$, i.e.
\[
\begin{pmatrix}
1 & 2 & 0 & 4 & 0 \\
0 & 50 & 13 & -26493 & -39 \\
0 & 0 & -84 & 171864 & 253 \\
1 & 23 & 6 & -12228 & -18 \\
3 & 89 & 23 & -46872 & -69
\end{pmatrix}
\begin{pmatrix}
x_1 \\
x_2 \\
x_3 \\
x_4 \\
x_5
\end{pmatrix}
= 
\begin{pmatrix}
25 \\
-199 \\
193998 \\
k_4 \\
k_5
\end{pmatrix}
\]

\[
\begin{align*}
x_1 &= -373 + 4k_4 \\
x_2 &= 2512024 - 26493k_4 - 39k_5 \\
x_3 &= -16295832 + 171864k_4 + 253k_5 \\
x_4 &= 1159436 - 12228k_4 - 18k_5 \\
x_5 &= 4444318 - 46872k_4 - 69k_5,
\end{align*}
\]
is a parametric solution of the given system of Linear Diophantine equations.

3 Conclusion

The study on existence of solutions of Linear Diophantine equations is based on a relation between the greatest common divisor of all the coefficients and the constant coefficient of the given Linear Diophantine equation is described in [1]. In this paper, parametric solutions of system of Linear Diophantine equations are generated with uni-modular row reductions on the coefficient matrix, based on the steps used in obtaining $\text{gcd}$ of coefficients by crushing method. The advantage of this application of $\text{gcd}$ by crushing, is the row reductions can be carried out in a specific order and this is used to give algorithm for the computations.

Competing Interests

Authors have declared that no competing interests exist.
References

[1] Srinivasarao BSS. A key exchange with Linear Diophantine equations. M.Phil., Dissertation; 2020.
[2] Deniz Yesilyurt. Solving Linear Diophantine Equations and Linear congruential Equations. Degree Project, Linnaeus University; 2012.
[3] Roy UN, Sah RP, Sah AK, Sourabh SK. Linear Diophantine Equation: Solution and Applications. International Journal of Mathematics Trends and Technology (IJMTT). 2019;65(1).
[4] Sagar Panda. Diophantine equation. National Institute of Technology Rourkela Rourkela, Orissa-769008; 2011.
[5] Felix Lasebnik. On systems of Linear Diophantine equation. 1996;69(4):261-266.
[6] Azam A. Imomov, Yorqin T. Khodjaev. On some methods for solution of Linear Diophantine equation; 2019.
[7] James Mcivor. Lecture notes on Diophantine Equations; 2012.
[8] Vasilious Evangelos Tourloupis. Hermite Normal Forms and its cryptographic applications. University of Wollongong Thesis Collection; 2013.
[9] William J. Gilbert, Anu Pathria. Linear Diophantine equation; 1990.
[10] Florentin Smarandache. Integer algorithms to solve Diophantine linear equations and systems. University of New Mexico, 200 College Road, Gallup, NM 87301, USA.
[11] Tomás Hruž et Dominique Fortin. Parallelism in Hermite and Smith normal forms. Article; 1994.
[12] Arvind V. Linear Diophantine equation. Algebra and Computation Lecture note.

© 2021 Kameswari and Belay; This is an Open Access article distributed under the terms of the Creative Commons Attribution License (http://creativecommons.org/licenses/by/4.0), which permits unrestricted use, distribution and reproduction in any medium, provided the original work is properly cited.

Peer-review history:
The peer review history for this paper can be accessed here (Please copy paste the total link in your browser address bar)
https://www.sdiarticle4.com/review-history/76249