CAUCHY – Jurnal Matematika Murni dan Aplikasi
Volume 11 (2) (2026), Pages 1831–1843
p-ISSN: 2086-0382; e-ISSN: 2477-3344

A Generalization Euclidean Algorithm Approach for Solving Multi-Variable Linear Diophantine Equations

Ikhsan Abdul Rouf, Hery Susanto*, and I Made Sulandra

Department of Mathematics, Faculty of Mathematics and Natural Sciences, State University of Malang, Malang, Indonesia.

Abstract

Multi-variable linear Diophantine equations of the form $a_1x_1 + a_2x_2 + \cdots + a_nx_n = b$ where $a_i, b \in \mathbb{Z}$ have some various applications in many fields, such as in cryptography, chemistry, and statistics, can be used to determine public and private keys, balance chemical equations, and model scheduling problems, respectively. The equation has infinitely many integer solutions, if $gcd(a_1, a_2, \ldots, a_n)$ divides b. There are two algorithms to find the solution of the equation, namely Smith normal form and integer lattice methods. This paper shows a different method to find the general solution of the equation. Our method applies the generalized Euclidean algorithm to find the GCD of $a_1, a_2, \ldots, a_n$. Next, we use back-substitution process through the steps of the generalized Euclidean algorithm to express the GCD as a linear combination of $a_1, a_2, \ldots, a_n$. Next, from that linear combination we multiply by $b/gcd(a_1, a_2, \ldots, a_n)$ to obtain a particular solution of the equation. Moreover, from that particular solution we construct the general solution of the equation.

Keywords: Multi-Variable Linear Diophantine Equation, Generalized Euclidean Algorithm.

1. Introduction

Multi-variable linear Diophantine equations are equations of the form

$$a_1x_1 + a_2x_2 + \cdots + a_nx_n = b \tag{1}$$

where $a_i, b \in \mathbb{Z}$ and $n \geq 2$, with solutions restricted to integers. In case $n = 2$, the equation

$$a_1x_1 + a_2x_2 = b$$

has a solution if and only if $gcd(a_1, a_2) \mid b$ [1]. Based on Bézout's Theorem, we can conclude that there are integers x and y such that

$$gcd(a, b) = ax + by.$$

The Euclidean algorithm is one of the algorithms used to determine the greatest common divisor (GCD) of two integers [2]. Since $gcd(a_1, a_2) \mid b$, then $b = k \cdot gcd(a_1, a_2), k \in \mathbb{Z}$. The extended Euclidean algorithm can be applied to find that integers x and y [3].

*Corresponding author. E-mail: hery.susanto.fmipa@um.ac.id

Received: June 06, 2026 Revised: July 28, 2026 Accepted: August 01, 2026
DOI: https://doi.org/10.18860/cauchy.v11i2.43242

Multi-variable linear Diophantine equations have applications in various fields. In cryptography, they are applied in the RSA algorithm to determine public and private keys [4–8]. In chemistry, linear Diophantine equations can be used to balance chemical equations [9]. Furthermore, in statistics, they can be utilized to model scheduling problems in big data systems [10]. These applications demonstrate that Diophantine equations are not only important in number theory but also useful for solving practical problems in various disciplines [11, 12].

A multi-variable linear Diophantine equation of the form (1) has an integer solution if

$$gcd(a_1, a_2, \ldots, a_n) \mid b.$$

In other words, equation (1) can be expressed as [13]

$$a_1x_1 + a_2x_2 + \cdots + a_nx_n = k \cdot gcd(a_1, a_2, \ldots, a_n), \quad k \in \mathbb{Z}.$$

There are two algorithms to find solution of equation (1), that is Smith normal form and integer lattice methods. These two algorithms using matrices to find the solution, Smith normal form need to find a unimodular matrix and integer lattice method need to find a basis lattice integer. For example, to find solution of equation $a_1x_1 + a_2x_2 + a_3x_3 = b$, Smith normal form will find the GCD of a_1, a_2, a_3 using matrix $\begin{bmatrix} a_1 & a_2 & a_3 \end{bmatrix}$ and using row operations and until we get $\begin{bmatrix} d & 0 & 0 \end{bmatrix}$.Thus, we obtain $d = gcd(a_1, a_2, a_3)$. To find the solution of that equation we will find a unimodular matrix V and the solution is

$$\begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix} = V \begin{bmatrix} b/d \\ s \\ t \end{bmatrix}$$

where $s, t \in \mathbb{Z}$ [14]. Whereas, integer lattice method will find a particular solution X_p of equation $a_1x_1 + a_2x_2 + a_3x_3 = b$ and find a basis (V_1, V_2) for the set $\{(x_1, x_2, x_3) \mid a_1x_1 + a_2x_2 + a_3x_3 = 0\}$. Then, the solution is $X_p + sV_1 + tV_2$ where $s, t \in \mathbb{Z}$ [15].

Therefore, this article proposes a different method for finding solution of multi-variable linear Diophantine equations. In this article, the generalized Euclidean algorithm is employed to determine the GCD of $a_1, a_2, \ldots, a_n$, rather than using a matrix-based approach. Next, we use back-substitution process through the steps of the generalized Euclidean algorithm to express GCD as a linear combination of $a_1, a_2, \ldots, a_n$. Next, from the linear combination multiply by $b/gcd(a_1, a_2, \ldots, a_n)$ to obtain a particular solution of the equation. Moreover, from that particular solution we construct the general solution of the equation. For example, to find the general solution of equation $a_1x_1 + a_2x_2 + a_3x_3 = b$, we first find GCD of a_1, a_2, a_3 using the generalized Euclidean algorithm. Next, using back-substitution process we will obtain $gcd(a_1, a_2, a_3) = a_1c_1 + a_2c_2 + a_3c_3$ for some $c_1, c_2, c_3 \in \mathbb{Z}$. The equation $a_1x_1 + a_2x_2 + a_3x_3 = b$ has solution, if $gcd(a_1, a_2, a_3) \mid b$. So, we can express $b = gcd(a_1, a_2, a_3) \cdot k = a_1c_1k + a_2c_2k + a_3c_3k$. Thus we obtain a particular solution that is, $(z_1, z_2, z_3) = (c_1k, c_2k, c_3k)$. From that particular solution we will construct the general solution.

2. Methods

This study adopts an analytical mathematical to approach general solution of multi-variable linear Diophantine equations. The research methodology consists of the following steps:

1. Construct the generalized Euclidean algorithm to find GCD of several integers through the generalized division algorithm.
2. Explain the back-substitution process from generalized Euclidean algorithm to express GCD as linear combination.

3. Construct the general solution of multi-variable linear Diophantine equations from a particular solution.

Before presenting the result and discussion of the generalized Euclidean algorithm and multi-variable linear Diophantine equations, we first review some definitions, lemmas, and theorems.

Definition 1. Let $a_1, a_2, a_3, \ldots, a_n$ be integers, not all zero. The greatest common divisor (GCD) of these integers is the largest positive integer that divides all of them [16].

Definition 2. Multi-variable linear Diophantine equations are equations of the form

$$a_1x_1 + a_2x_2 + \cdots + a_nx_n = b$$

where $n \geq 2$ and $a_i, b \in \mathbb{Z}$ for all $i = 1, 2, \ldots, n$ [17].

Theorem 1. *If a and b are integers, then there are integers x and y such that [16]*

$$ax + by = gcd(a, b).$$

Next lemma is associative property of the GCD.

Lemma 1. *If $a_1, a_2, a_3, \ldots, a_n$ are integers, not all zero, then [16]*

$$gcd(a_1, a_2, a_3, \ldots, a_k, a_{k+1}, \ldots, a_{n-1}, a_n) = gcd(a_1, a_2, a_3, \ldots, gcd(a_k, a_{k+1}), \ldots, a_{n-1}, a_n).$$

Theorem 2. *For any integer q, it holds that $gcd(a, b) = gcd(a + bq, b)$ [16].*

Lemma 2. *If $a, b,$ and c are positive integers such that $gcd(a, b) = 1$ and $a \mid bc$, then $a \mid c$ [16].*

3. Results and Discussion

In this section, we will prove the generalized Euclidean algorithm to find the GCD of several integers. Before we prove that algorithm, firstly we will prove two theorems that will be used to prove the generalized Euclidean algorithm.

Theorem 3. *Let $a_1, a_2, a_3 \ldots, a_n$ be a sequence of integers. If $|a_1| \geq |a_2| \geq |a_3| \geq \cdots \geq |a_n| > 0$, then there are integers $q_1, q_2, \ldots, q_{n-1}, r$ such that*

$$a_1 = a_2q_1 + a_3q_2 + \cdots + a_nq_{n-1} + r,$$

where $0 \leq r < |a_n|$.

Proof. Consider the set $S = \{a_1 - a_2q_1 - a_3q_2 - \ldots - a_nq_{n-1} | q_i \in \mathbb{Z}, i = 1, 2, \ldots, n-1\}$. Let T be the set of all non-negative integers in S. Note that T is nonempty, because we can choose $q_i = 0$ for all $i = 1, 2, \ldots, n-2$ and $q_{n-1} < a_1/a_n$. So, $a_1 - a_2q_1 - a_3q_2 - \ldots - a_nq_{n-1}$ is positive.
By the well ordering property of non-negative integers, T must has a smallest element, namely $r = a_1 - a_2p_1 - a_3p_2 - \ldots - a_np_{n-1} \geq 0$, for some $p_i \in \mathbb{Z}, i = 1, 2, \ldots, n-1$

Suppose $r \geq |a_n|$. Then,

$$r \geq r - |a_n| = a_1 - a_2p_1 - a_3p_2 - ... - a_np_{n-1} - |a_n|.$$

If $a_n < 0$, then we have $r - |a_n| = a_1 - a_2p_1 - a_3p_2 - ... - a_n(p_{n-1} - 1)$. If $a_n > 0$, then we have $r - |a_n| = a_1 - a_2p_1 - a_3p_2 - ... - a_n(p_{n-1} + 1)$. Since $r - |a_n| \geq 0$, then $r - |a_n| \in T$. This contradicts that r is a smallest element in T. Thus, $0 \leq r < |a_n|$. □

Theorem 4. *Let $a_1, a_2, a_3, \ldots, a_n$ be a sequence of integers. There are integers $q_1, q_2, ..., q_{n-1}$, such that $gcd(a_1, a_2, a_3, ..., a_n) = gcd(a_1 + a_2q_1 + a_3q_1 + ... + a_nq_{n-1}, a_2, a_3, ..., a_n)$ for any positive integer $n > 1$.*

Proof. We prove by the mathematical induction. Note that for the case $n = 2$, had been already proven by Theorem 2. Assume true for $n = k$, that is $gcd(a_1, a_2, a_3, ..., a_k) = gcd(a_1 + a_2q_1 + a_3q_1 + ... + a_kq_{k-1}, a_2, a_3, ..., a_k)$. Next, we will show for $n = k + 1$. Using Lemma 1, Theorem 2, and the Hypothesis induction we get

$$\begin{aligned}
gcd(a_1, a_2, a_3, ..., a_k, a_{k+1}) &= gcd(gcd(a_1, a_2, a_3, ..., a_k), a_{k+1}) \\
&= gcd(gcd(a_1 + a_2q_1 + a_3q_2 + ... + a_kq_{k-1}, a_2, a_3, ..., a_k), a_{k+1}) \\
&= gcd(a_1 + a_2q_1 + a_3q_2 + ... + a_kq_{k-1}, a_2, a_3, ..., a_k, a_{k+1}) \\
&= gcd(a_2, a_3, \ldots, a_k, a_1 + a_2q_1 + a_3q_2 + ... + a_kq_{k-1}, a_{k+1}) \\
&= gcd(a_2, a_3, \ldots, a_k, gcd(a_1 + a_2q_1 + a_3q_2 + ... + a_kq_{k-1}, a_{k+1})) \\
&= gcd(a_2, a_3, \ldots, gcd(a_k, a_1 + a_2q_1 + ... + a_kq_{k-1} + a_{k+1}q_k, a_{k+1})) \\
&= gcd(a_2, a_3, \ldots, a_k, a_1 + a_2q_1 + a_3q_2 + ... + a_kq_{k-1} + a_{k+1}q_k, a_{k+1}) \\
&= gcd(a_1 + a_2q_1 + a_3q_2 + ... + a_kq_{k-1} + a_{k+1}q_k, a_2, a_3, \ldots, a_k, a_{k+1}).
\end{aligned}$$

Hence, by the mathematical induction the statement holds for any positive integer $n > 1$. □

The following is a corollary of Theorem 4.

Corollary 1. *Given integers sequence $a_1, a_2, ..., a_n$. If $a_1 = a_2q_1 + a_3q_2 + ... + a_nq_{n-1} + r$ where $q_1, q_2, ..., q_{n-1}, r$ are integers, then $gcd(a_1, a_2, ..., a_n) = gcd(r, a_2, ..., a_n)$.*

Proof. Using Theorem 4 and choosing $r = a_1 - a_2q_1 - a_3q_2 - ... - a_nq_{n-1}$. □

Theorem 3 can be applied iteratively until the remainder becomes zero, which reduces the number of integers one by one, until we have one integer that is the GCD of $a_1, a_2, \ldots, a_n$. Therefore, Theorem 3 can be used to determine the GCD of n integers. We will prove the generalized Euclidean algorithm for positive integers sequence, because of the fact $gcd(a_1, , a_2, \ldots, a_n) = gcd(|a_1|, |a_2|, \ldots, |a_n|)$.

Theorem 5. ***The Generalized Euclidean Algorithm.*** *Given positive integers sequence $a_1, a_2, \ldots, a_n$ where $a_1 > a_2 > \cdots > a_n$. Let $r_i = a_i$ for all $1 \leq i \leq n$, and apply Theorem 3 multiple times to obtain $r_j = r_{j+1}q_1^{(j)} + r_{j+2}q_2^{(j)} + \cdots + r_{j+n-1}q_{n-1}^{(j)} + r_{j+n}$, where $0 \leq r_{j+n} < r_{j+n-1} < \cdots < r_{j+1} < r_j$, for $j = 1, 2, 3, \ldots, s_1$ and $r_{s_1+n} = 0$. If we repeat the process with $n - 1$ integers and $r_i = r_{s_1+i}$ for all $1 \leq i \leq n - 1$ we will obtain $r_{s_2+n-1} = 0$,*

and so on, until we get one integer $r_{s_{(n-1)}}$, then $gcd(a_1, a_2, ..., a_n) = r_{s_{(n-1)}}$.

Proof. Let $r_i = a_i$ for $i = 1, 2, 3, ..., n$. Applying Theorem 3 multiple times, we obtain

$$\begin{aligned}
r_1 &= r_2 q_1^{(1)} + r_3 q_2^{(1)} + ... + r_n q_{n-1}^{(1)} + r_{n+1} && 0 \le r_{n+1} < r_n \\
r_2 &= r_3 q_1^{(2)} + r_4 q_2^{(2)} + ... + r_{n+1} q_{n-1}^{(2)} + r_{n+2} && 0 \le r_{n+2} < r_{n+1} \\
&\vdots \\
r_j &= r_{j+1} q_1^{(j)} + r_{j+2} q_2^{(j)} + \cdots + r_{j+n-1} q_{n-1}^{(j)} + r_{j+n} && 0 \le r_{j+n} < r_{j+n-1} \\
&\vdots \\
r_{s_1} &= r_{s_1+1} q_1^{(s_1)} + r_{s_1+2} q_2^{(s_1)} + ... + r_{s_1+n-1} q_{n-1}^{(s_1)} + 0.
\end{aligned}$$

Because the remainders are integer and the sequence of remainders $r_1 > r_2 > \cdots > r_{s_1+n} \ge 0$ cannot contain more than r_1 terms, consequently a zero remainder must eventually occur. This process will decrease the number of integers by one. We repeat this process with $n-1$ integers and we obtain $r_{s_2+n-1} = 0$. We continue this process until the number of integers is one. That is,

$$\begin{aligned}
r_{s_1+1} &= r_{s_1+2} q_1^{(s_1+1)} + r_{s_1+3} q_2^{(s_1+1)} + ... + r_{s_1+n-1} q_{n-2}^{(s_1+1)} + r_{s_1+n} && 0 \le r_{s_1+n} < r_{s_1+n-1} \\
r_{s_1+2} &= r_{s_1+3} q_1^{(s_1+2)} + r_{s_1+4} q_2^{(s_1+2)} + ... + r_{s_1+n} q_{n-2}^{(s_1+2)} + r_{s_1+n+1} && 0 \le r_{s_1+n+1} < r_{s_1+n} \\
&\vdots \\
r_{s_2} &= r_{s_2+1} q_1^{(s_2)} + r_{s_2+2} q_2^{(s_2)} + ... + r_{s_2+n-2} q_{n-2}^{(s_2)} + 0 \\
&\vdots \\
r_{s_{(n-1)}-2} &= r_{s_{(n-1)}-1} q_1^{(s_{(n-1)}-2)} + r_{s_{(n-1)}} && 0 \le r_{s_{(n-1)}} < r_{s_{(n-1)}-1} \\
r_{s_{(n-1)}-1} &= r_{s_{(n-1)}} q_1^{(s_{(n-1)}-1)} + 0.
\end{aligned}$$

We can assume that we eventually obtain a zero remainders, because the sequence of remainders is strictly decreasing and it non-negative integers sequence. Thus, by Corollary 1 we obtain

$$\begin{aligned}
(a_1, a_2, \ldots, a_n) = (r_1, r_2, \ldots, r_n) &= (r_2, r_3, \ldots, r_n, r_{n+1}) \\
&= (r_3, \ldots, r_{n+1}, r_{n+2}) \\
&\vdots \\
&= (r_{s_1+1}, \ldots, r_{s_1+n-1}, 0) \\
&= (r_{s_1+1}, \ldots, r_{s_1+n-1}) \\
&\vdots \\
&= (r_{s_2+1}, \ldots, r_{s_2+n-2}, 0) \\
&= (r_{s_2+1}, \ldots, r_{s_2+n-2}) \\
&\vdots \\
&= (r_{s_{(n-1)}-1}, r_{s_{(n-1)}}) \\
&= (r_{s_{(n-1)}}, 0)
\end{aligned}$$

$$= r_{s_{(n-1)}}.$$

Thus, $(a_1, a_2, ..., a_n) = r_{s_{(n-1)}}$. □

We see that the quotients selection in Theorem 3 not unique, but for convenience we choose the quotients as follows. First, rearrange the numbers so we get decreasing sequence of positive integer. Next, we will divide a_1 with a_2 to obtain q_1 and a remainder r_1. Then, we divide r_1 with a_3 to obtain q_2 and a remainder r_2, and so on until we obtain the last remainder r. Next, several illustrative examples related to the generalized Euclidean algorithm.

Example 1. The GCD of $105, 70, 42$, and 30 is 1.
By the generalized Euclidean algorithm, we have

$$\begin{aligned}
105 &= 70 \cdot 1 + 42 \cdot 0 + 30 \cdot 1 + 5 && 5 = 105 \cdot (1) + 70 \cdot (-1) + 30 \cdot (-1)\\
70 &= 42 \cdot 1 + 30 \cdot 0 + 5 \cdot 5 + 3 && 3 = 70 \cdot (1) + 42 \cdot (-1) + 5 \cdot (-5)\\
42 &= 30 \cdot 1 + 5 \cdot 2 + 3 \cdot 0 + 2 && 2 = 42 \cdot (1) + 30 \cdot (-1) + 5 \cdot (-2)\\
\boxed{30 &= 5 \cdot 6 + 3 \cdot 0 + 2 \cdot 0 + 0}\\
\boxed{5 &= 3 \cdot 1 + 2 \cdot 1 + 0}\\
3 &= 2 \cdot 1 + 1 && 1 = 3 \cdot (1) + 2 \cdot (-1)\\
\boxed{2 &= 1 \cdot 2 + 0}.
\end{aligned}$$

From Example 1 we can express the GCD of 105, 70, 42, and 30 as a linear combination of 105, 70, 42, and 30. That is,

$$\begin{aligned}
1 &= 3 \cdot 1 + 2 \cdot (-1)\\
&= 3 \cdot 1 + (42 \cdot 1 + 30 \cdot (-1) + 5 \cdot (-2)) \cdot (-1)\\
&= 3 \cdot 1 + 42 \cdot (-1) + 30 \cdot 1 + 5 \cdot 2\\
&= (70 \cdot 1 + 42 \cdot (-1) + 5 \cdot (-5)) \cdot 1 + 42 \cdot (-1) + 30 \cdot 1 + 5 \cdot 2\\
&= 70 \cdot 1 + 42 \cdot (-2) + 30 \cdot 1 + 5 \cdot (-3)\\
&= 70 \cdot 1 + 42 \cdot (-2) + 30 \cdot 1 + (105 \cdot 1 + 70 \cdot (-1) + 30 \cdot (-1)) \cdot (-3)\\
&= 105 \cdot (-3) + 70 \cdot 4 + 42 \cdot (-2) + 30 \cdot 4.
\end{aligned}$$

Example 2. The GCD of $56, 78, -42$, and 16 is 2.
First, we rearrange and find the positive of each integer. So, we work with positive integer sequence $78, 56, 42, 16$. By the generalized Euclidean algorithm, we have

$$\begin{aligned}
78 &= 56 \cdot 1 + 42 \cdot 0 + 16 \cdot 1 + 6 && 6 = 78 \cdot (1) + 56 \cdot (-1) + 16 \cdot (-1)\\
56 &= 42 \cdot 1 + 16 \cdot 0 + 6 \cdot 2 + 2 && 2 = 56 \cdot (1) + 42 \cdot (-1) + 6 \cdot (-2)\\
\boxed{42 &= 16 \cdot 2 + 6 \cdot 1 + 2 \cdot 0 + 0}\\
\boxed{16 &= 6 \cdot 2 + 2 \cdot 2 + 0}\\
\boxed{6 &= 2 \cdot 3 + 0}.
\end{aligned}$$

From Example 2 we can express the GCD of $78, 56, 42$, and 16 as a linear combination of $78, 56, 42$, and 16. That is,

$$\begin{aligned}2 &= 56 \cdot (1) + 42 \cdot (-1) + 6 \cdot (-2)\\ &= 56 \cdot (1) + 42 \cdot (-1) + (78 \cdot (1) + 56 \cdot (-1) + 16 \cdot (-1)) \cdot (-2)\\ &= 78 \cdot (-2) + 56 \cdot (3) + 42 \cdot (-1) + 16 \cdot (2)\\ &= 78 \cdot (-2) + 56 \cdot (3) + 42 \cdot (-1) + 16 \cdot (2).\end{aligned}$$

Example 3. The GCD of $48, 56, 16$, and 16 is 8.
First, we rearrange and choose one of each integer. So, we work with positive integer sequence $56, 48, 16$. By the generalized Euclidean algorithm, we have

$$\begin{aligned}56 &= 48 \cdot 1 + 16 \cdot 0 + 8 \qquad & 8 &= 56 \cdot (1) + 48 \cdot (-1)\\ \boxed{48 &= 16 \cdot 3 + 8 \cdot 0 + 0}\\ \boxed{16 &= 8 \cdot 2 + 0}.\end{aligned}$$

From Example 3 we can express the GCD of $56, 48$, and 16 as a linear combination of $56, 48$, and 16. That is,

$$8 = 56 \cdot (1) + 48 \cdot (-1).$$

Now, we can set the coefficient of all other numbers is zero. So, we obtain the linear combination is

$$8 = 56 \cdot (1) + 48 \cdot (-1) + 16 \cdot 0.$$

From explanation above, we have conclusion that $gcd(a_1, a_2, \ldots, a_n) = a_1x_1 + a_2x_2 + \cdots + a_nx_n, x_i \in \mathbb{Z}$ for all $i = 1, 2, \ldots, n$.

Lemma 3. *Let $a_1, a_2, \ldots, a_n$ be integers. Then, there are integers $c_1, c_2, \ldots, c_n$ such that*

$$gcd(a_1, a_2, \ldots, a_n) = a_1c_1 + a_2c_2 + \cdots + a_nc_n.$$

Proof. We will prove by the mathematical induction. For case $n = 2$, based on Theorem 1, there are integers y_1 and y_2 such that

$$gcd(a_1, a_2) = a_1y_1 + a_2y_2.$$

Assume, for the case $k = n$, that there are integers $y_1, y_2, \ldots, y_k$ such that

$$gcd(a_1, a_2, \ldots, a_k) = a_1y_1 + a_2y_2 + \cdots + a_ky_k.$$

Then, by Lemma 1 and the Hypothesis induction, we obtain

$$\begin{aligned}gcd(a_1, a_2, \ldots, a_k, a_{k+1}) &= gcd(gcd(a_1, a_2, \ldots, a_k), a_{k+1})\\ &= gcd(a_1b_1 + a_2b_2 + \cdots + a_kb_k, a_{k+1}).\end{aligned}$$

From the last form, applying Theorem 1, there are integers d and e such that

$$\begin{aligned}gcd(a_1, a_2, \ldots, a_k, a_{k+1}) &= gcd(a_1b_1 + a_2b_2 + \cdots + a_kb_k, a_{k+1})\\ &= (a_1y_1 + a_2y_2 + \cdots + a_ky_k)d + a_{k+1}e\end{aligned}$$

$$= a_1(y_1 d) + a_2(y_2 d) + \cdots + a_k(y_k d) + a_{k+1} e.$$

Thus, it is proven that there are integers $c_1, c_2, \ldots, c_n$ such that

$$gcd(a_1, a_2, \ldots, a_n) = a_1 c_1 + a_2 c_2 + \cdots + a_n c_n. \qquad \square$$

Lemma 4. *Let $a_1, a_2, \ldots, a_n$ be integers. If $gcd(a_1, a_2, \ldots, a_n) = d$, then $gcd(\frac{a_1}{d}, \frac{a_2}{d}, \ldots, \frac{a_n}{d}) = 1$.*

Proof. Let $a_1, a_2, \ldots, a_n$ be integers with $gcd(a_1, a_2, \ldots, a_n) = d$. We will show that $\frac{a_1}{d}, \frac{a_2}{d}, \ldots, \frac{a_n}{d}$ have no common divisors other than 1. Assume that e be a positive integer such that $e \mid \frac{a_i}{d}$ for all $1 \leq i \leq n$. Then, there is an integer k_i such that $\frac{a_i}{d} = ek_i$. So, we obtain that $a_i = dek_i$. Hence, de is a common divisor of a_i. Since, d is the GCD of $a_1, a_2, \ldots, a_n$ we have $de \leq d$. So, e must be 1. Consequently, $gcd(\frac{a_1}{d}, \frac{a_2}{d}, \ldots, \frac{a_n}{d}) = 1$. $\square$

Next, we will presenting the general solution of a multi-variable linear Diophantine equation. In general, a multi-variable linear Diophantine equation has two possibilities: it either has no solution if $gcd(a_1, a_2, a_3, \ldots, a_n) \nmid b$, or has infinitely many solutions if $gcd(a_1, a_2, a_3, \ldots, a_n) \mid b$.

Theorem 6. *Let $a_1, a_2, \ldots, a_n$ be a sequence of integers with $|a_1| \geq |a_2| \geq |a_3| \geq \cdots \geq |a_n| > 0$ and $d = gcd(a_1, a_2, \ldots, a_n)$. A multi-variable linear Diophantine equation*

$$a_1 x_1 + a_2 x_2 + \cdots + a_n x_n = b.$$

has infinitely many integer solutions if and only if $d \mid b$.

Proof. Let $(y_1, y_2, \ldots, y_n)$ be a solution of equation (1) and let $d = gcd(a_1, a_2, \ldots, a_n)$. So, $d \mid a_i$ for all $1 \leq i \leq n$ and $a_1 y_1 + a_2 y_2 + \cdots + a_n y_n = b$. Thus, we get $d \mid (a_1 y_1 + a_2 y_2 + \cdots + a_n y_n)$ and it follows that $d \mid b$.
Conversely if $d \mid b$, based on Lemma 3, there are integers $c_1, c_2, \ldots, c_n$ such that

$$d = a_1 c_1 + a_2 c_2 + \cdots + a_n c_n.$$

Since $d \mid b$, there is an integer e such that $b = de$. Consequently,

$$b = de = (a_1 c_1 + a_2 c_2 + \cdots + a_n c_n)e = a_1(c_1 e) + a_2(c_2 e) + \cdots + a_n(c_n e).$$

Thus, $(z_1, z_2, \ldots, z_n)$ where $z_i = c_i e$ for all $1 \leq i \leq n$ is a particular solution of the equation. Next, we will show that there are infinitely many solutions by constructing the solution set of equation (1). Let $(y_1, y_2, y_3, \ldots, y_n)$ be a solution of equation (1) and the particular solution $(z_1, z_2, \ldots, z_n)$. So, we obtain

$$a_1 y_1 + a_2 y_2 + \cdots + a_n y_n = b$$

$$a_1 z_1 + a_2 z_2 + \cdots + a_n z_n = b.$$

Subtracting these two equations yields

$$a_1(y_1 - z_1) + a_2(y_2 - z_2) + \cdots + a_n(y_n - z_n) = 0 \qquad (2)$$

$$a_i(y_i - z_i) = -(a_1(y_1 - z_1) + \cdots + a_{i-1}(y_{i-1} - z_{i-1}) + a_{i+1}(y_{i+1} - z_{i+1}) + \cdots + a_n(y_n - z_n)).$$

Dividing both sides by d, we obtain

$$\left(\frac{a_i}{d}\right)(y_i - z_i) = -\left(\left(\frac{a_1}{d}\right)(y_1 - z_1) + \cdots + \left(\frac{a_{i-1}}{d}\right)(y_{i-1} - z_{i-1}) + \left(\frac{a_{i+1}}{d}\right)(y_{i+1} - z_{i+1}) + \cdots + \left(\frac{a_n}{d}\right)(y_n - z_n)\right).$$

Let $d_i = \gcd(\frac{a_1}{d}, \frac{a_2}{d}, \ldots, \frac{a_{i-1}}{d}, \frac{a_{i+1}}{d}, \ldots, \frac{a_n}{d})$ for all $1 \leq i < n$. By Lemma 4, we know that $gcd(\frac{a_1}{d}, \frac{a_2}{d}, \ldots, \frac{a_n}{d}) = 1$. So, $gcd(d_i, \frac{a_i}{d}) = 1$ and $d_i \mid (\frac{a_i}{d})(y_i - z_i)$. By Lemma 2, we have $d_i \mid (y_i - z_i)$. Hence, there is an integer k_i such that $d_i k_i = (y_i - z_i)$, this means that $y_i = z_i + d_i k_i$. Putting this value to equation (2) yields

$$\begin{aligned} a_1(d_1k_1) + a_2(d_2k_2) + \cdots + a_{n-1}(d_{n-1}k_{n-1}) + a_n(y_n - z_n) &= 0 \\ -(a_1d_1k_1 + a_2d_2k_2 + \cdots + a_{n-1}d_{n-1}k_{n-1}) &= a_n(y_n - z_n) \\ -\frac{1}{a_n}(a_1d_1k_1 + a_2d_2k_2 + \cdots + a_{n-1}d_{n-1}k_{n-1}) &= y_n - z_n. \end{aligned}$$

Since $(y_n - z_n) \in \mathbb{Z}$, then $(-\frac{1}{a_n}(a_1d_1k_1 + a_2d_2k_2 + \cdots + a_{n-1}d_{n-1}k_{n-1})) \in \mathbb{Z}$. Solving for y_n gives

$$y_n = z_n - \frac{1}{a_n}(a_1d_1k_1 + a_2d_2k_2 + \cdots + a_{n-1}d_{n-1}k_{n-1}) \in \mathbb{Z}.$$

So, the solution of equation (1) must be in the form

$$y_i = z_i + d_ik_i \quad \text{for all } 1 \leq i < n \quad \text{and} \quad y_n = z_n - \frac{1}{a_n}(a_1d_1k_1 + \cdots + a_{n-1}d_{n-1}k_{n-1}) \in \mathbb{Z}.$$

Next, if $\frac{1}{a_n}(a_1d_1k_1 + \cdots + a_{n-1}d_{n-1}k_{n-1}) \in \mathbb{Z}$, then we have set

$$T = \left\{\left(z_1 + d_1k_1, \ldots, z_{n-1} + d_{n-1}k_{n-1}, z_n - \frac{1}{a_n}(a_1d_1k_1 + \cdots + a_{n-1}d_{n-1}k_{n-1})\right) \mid k_i \in \mathbb{Z}\right\}.$$

We will show that every element in T is solution of equation (1). Observe that for $(x'_1, x'_2, \ldots, x'_n) \in T$, we have

$$x'_i = z_i + d_il_i, \quad l_i \in \mathbb{Z} \quad \text{for all } 1 \leq i < n \quad \text{and} \quad x'_n = z_n - \frac{1}{a_n}(a_1d_1l_1 + \cdots + a_{n-1}d_{n-1}l_{n-1}).$$

So, we have

$$a_ix'_i = a_iz_i + a_id_il_i, \quad \text{and} \quad a_nx'_n = a_nz_n - (a_1d_1l_1 + \cdots + a_{n-1}d_{n-1}l_{n-1}).$$

Consider the summation $a_1x'_1 + a_2x'_2 + \ldots + a_nx'_n$, the terms involving $a_id_il_i$ cancel out, leaving only a_iz_i for all $1 \leq i \leq n$. Consequently, we obtain

$$a_1x'_1 + a_2x'_2 + \cdots + a_nx'_n = a_1z_1 + a_2z_2 + \cdots + a_nz_n = b.$$

Therefore, every element in T is the solution of equation (1). Now, since $k_i \in \mathbb{Z}$ and we can choose k_i is multiple of a_n so we have T is infinite set. □

Next, we will explain step-by-step how to find the general solution of equation (1). If there are repeated coefficients, then we only work with one of them and set the other with a parameter. If there are negative coefficients, then we work with its positive and multiply the quotient in

the linear combination with (-1). If there are zero coefficients, then we ignore them. If the coefficients are unordered, then we rearrange them to ordered coefficient such that Theorem 6 can be applied and we rearrange the solution satisfying the original equation.

1. Use the generalized Euclidean algorithm to find $d = gcd(a_1, a_2, \ldots, a_n)$ and for all $1 \leq i < n$ we find $d_i = gcd(\frac{a_1}{d}, \frac{a_2}{d}, \ldots, \frac{a_{i-1}}{d}, \frac{a_{i+1}}{d}, \ldots, \frac{a_n}{d})$.
2. From step 1 and use back-substitution process through the steps of the generalized Euclidean algorithm, we will obtain $d = a_1c_1 + a_2c_2 + \cdots + a_nc_n$. We can find a particular solution of equation (1), that is $z_i = \frac{b}{d}c_i$ for all $1 \leq i \leq n$.
3. Use Theorem 6 to find the general solution.

Several illustrative examples related to Theorem 6 are provided.

Example 4. Determine all integer solutions of the equation

$$105x_1 + 70x_2 + 42x_3 + 30x_4 = 631.$$

Using the generalized Euclidean algorithm we obtain $d = gcd(105, 70, 42, 30) = 1, d_1 = gcd(70/1, 42/1, 30/1) = 2, d_2 = gcd(105/1, 42/1, 30/1) = 3, d_3 = gcd(105/1, 70/1, 30/1) = 5$. From Example 1 we get,

$$1 = 105 \cdot (-3) + 70 \cdot 4 + 42 \cdot (-2) + 30 \cdot 4.$$

Multiplying both sides by 631, we obtain

$$631 = 105 \cdot (-1893) + 70 \cdot 2524 + 42 \cdot (-1262) + 30 \cdot 2524.$$

So, we get a particular solution is $(-1893, 2524, -1262, 2524)$. Hence, if $\frac{1}{30}(210k_1 + 210k_2 + 210k_3) \in \mathbb{Z}$, then by Theorem 6 we get the solution set of that equation is

$$T = \{(-1893+2k_1, 2524+3k_2, -1262+5k_3, 2524-\frac{1}{30}(210k_1+210k_2+210k_3)) \mid k_1, k_2, k_3 \in \mathbb{Z}\}.$$

Example 5. Determine all integer solutions of the equation

$$56x_1 + 78x_2 - 42x_3 + 16x_4 = 60.$$

First, we rearrange the equation so we have decreasing positive coefficient that is, $78y_1 + 56y_2 + 42y_3 + 16y_4 = 60$ with $y_1 = x_2, y_2 = x_1, y_3 = -x_3$, and $y_4 = x_4$. Using the generalized Euclidean algorithm we obtain $d = gcd(78, 56, 42, 16) = 2, d_1 = gcd(56/2, 42/2, 16/2) = 1, d_2 = gcd(78/2, 42/2, 16/2) = 1, d_3 = gcd(78/2, 56/2, 16/2) = 1$. From Example 2 we get,

$$2 = 78 \cdot (-2) + 56 \cdot (3) + 42 \cdot (-1) + 16 \cdot (2).$$

Multiplying both sides by 30, we obtain

$$60 = 78 \cdot (-60) + 56 \cdot (90) + 42 \cdot (-30) + 16 \cdot (60).$$

So, we get a particular solution is $(-60, 90, -30, 60)$. Hence, if $\frac{1}{16}(78k_1 + 56k_2 + 42k_3) \in \mathbb{Z}$, then by Theorem 6 we get the solution set of that equation is

$$T = \{(-60 + k_1, 90 + k_2, -30 + k_3, 60 - \frac{1}{16}(78k_1 + 56k_2 + 42k_3)) \mid k_1, k_2, k_3 \in \mathbb{Z}\}.$$

Now, since $x_1 = y_2, x_2 = y_1, x_3 = -y_3, x_4 = y_4$ then we have the general solution of equation $56x_1 + 78x_2 - 42x_3 + 16x_4 = 60$ is

$$S = \{(90 + k_2, -60 + k_1, 30 - k_3, 60 - \frac{1}{16}(78k_1 + 56k_2 - 42k_3)) \mid k_1, k_2, k_3 \in \mathbb{Z}\}$$

Example 6. Determine all integer solutions of the equation

$$48x_1 + 56x_2 + 16x_3 + 16x_4 = 24.$$

We see that 16 appears two times, so we can factorize the equation and we obtain $48x_1 + 56x_2 + 16(x_3 + x_4) = 24$. So, we need to solve the equation $56y_1 + 48y_2 + 16y_3 = 24$ with $y_1 = x_2, y_2 = x_1$, and $y_3 = (x_3 + x_4)$. Using the generalized Euclidean algorithm we obtain $d = gcd(56, 48, 16) = 8, d_1 = gcd(48/8, 16/8) = 2, d_2 = gcd(56/8, 16/8) = 1$. From Example 3 we get,

$$8 = 56 \cdot (1) + 48 \cdot (-1) + 16 \cdot 0.$$

Multiplying both sides by 3, we obtain

$$24 = 56 \cdot (3) + 48 \cdot (-3) + 16 \cdot (0).$$

So, we get a particular solution is $(3, -3, 0)$. Hence, if $\frac{1}{16}(112k_1 + 48k_2) \in \mathbb{Z}$, then by Theorem 6 we get the solution set of that equation is

$$T = \{(3 + 2k_1, -3 + k_2, 0 - \frac{1}{16}(112k_1 + 48k_2)) \mid k_1, k_2 \in \mathbb{Z}\}.$$

Now, since $x_1 = y_2, x_2 = y_1, x_3 + x_4 = y_3$ we can set x_3 equal an integer k_3 and we have $x_4 = y_3 - k_3$. So, the general solution of equation $48x_1 + 56x_2 + 16x_3 + 16x_4 = 24$ is

$$S = \{(-3 + k_2, 3 + 2k_1, k_3, 0 - \frac{1}{16}(112k_1 + 48k_2) - k_3) \mid k_1, k_2, k_3 \in \mathbb{Z}\}.$$

4. Conclusion

This paper has developed the generalized Euclidean algorithm to find the GCD of $a_1, a_2, \ldots, a_n$. Using back-substitution process from that algorithm to express the GCD as a linear combination of $a_1, a_2, \ldots, a_n$, that is $a_1c_1 + a_2c_2 + \cdots + a_nc_n = gcd(a_1, a_2, \ldots, a_n)$. Next, to find the general solution of multi-variable linear Diophantine equations of the form

$$a_1x_1 + a_2x_2 + \cdots + a_nx_n = b$$

we first find a particular solution that is, $(\frac{b}{d}c_1, \frac{b}{d}c_2, \ldots, \frac{b}{d}c_n)$ where $d = gcd(a_1, a_2, \ldots, a_n)$. If $\frac{1}{a_n}(a_1d_1k_1 + \cdots + a_{n-1}d_{n-1}k_{n-1}) \in \mathbb{Z}, d_i = \gcd(\frac{a_1}{d}, \frac{a_2}{d}, \ldots, \frac{a_{i-1}}{d}, \frac{a_{i+1}}{d}, \ldots, \frac{a_n}{d})$ for all $1 \leq i < n$, and $z_i = \frac{b}{d}c_i$ for all $1 \leq i \leq n$, then the general solution of the equation is

$$T = \left\{ \left(z_1 + d_1k_1, \ldots, z_{n-1} + d_{n-1}k_{n-1}, z_n - \frac{1}{a_n}(a_1d_1k_1 + \cdots + a_{n-1}d_{n-1}k_{n-1}) \right) \mid k_i \in \mathbb{Z} \right\}.$$

For the next researcher, other implementation of generalized Euclidean algorithm can be explored, such as solving system of multi-variable linear Diophantine equations or multi-variable quadratic Diophantine equations.

CRediT Authorship Contribution Statement

Ikhsan Abdul Rouf: Conceptualization, Methodology, Formal analysis, Writing–Original Draft. **Hery Susanto:** Supervision, Validation, Writing–Review & Editing. **I Made Sulandra:** Supervision, Formal analysis, Writing–Review & Editing. All authors have read and approved the final version of the manuscript.

Declaration of Generative AI and AI-assisted technologies

No generative AI and AI-assisted were used during the preparation of this manuscript.

Declaration of Competing Interest

The authors declare no competing interests.

Funding and Acknowledgments

The authors would like to express their sincere thanks to the reviewers for their helpful comments and suggestions. This research was conducted with funding of Desentralisasi FMIPA Universitas Negeri Malang 2025.

References

[1] Mayank Deora and Pinakpani Pal. *Efficient Algorithm for Linear Diophantine Equations in Two Variables*. 2025. DOI: 10.48550/arXiv.2507.23216. arXiv: 2507.23216 [cs.DS].

[2] Amit Prakash. "Solutions of Linear Diophantine Equations Using Elementary Methods". In: *Panamerican Mathematical Journal* 34.3 (2024), pp. 295–314. DOI: 10.52783/pmj.v34.i3.6420.

[3] Johannes A. Buchmann. *Introduction to Cryptography*. Springer, 2000. 285 pp. DOI: 10.1007/978-1-4684-0496-8.

[4] P. Anuradha Kameswari, S. S. Sriniasarao, and Aweke Belay. "An Application of Linear Diophantine Equations to Cryptography". In: *Advances in Mathematics: Scientific Journal* 10.6 (2021). Published online: 10 June 2021, pp. 2799–2806. DOI: 10.37418/amsj.10.6.8.

[5] Tahang Purwandi and Syamsyida Rozi. "Pemanfaatan Persamaan Diophantine Linear dalam Membangkitkan Kunci Privat pada Algoritma RSA". In: *Jurnal Riset Mahasiswa Matematika* 4.6 (2025), pp. 301–309. DOI: 10.18860/jrmm.v4i6.34656.

[6] Noriko Hirata-Kohno and Attila Petho. "A Key Exchange Protocol Based on Diophantine Equations and S-Integers". In: *JSIAM Letters* 6 (2014), pp. 85–88. DOI: 10.14495/jsiaml.6.85.

[7] B. S. S. Srinivasarao. "A Key Exchange with Linear Diophantine Equations". M.Phil. dissertation. Andhra University, 2020.

[8] Yi Zhou. "Role of Linear Diophantine Equations in RSA Encryption". In: *Theoretical and Natural Science* 42.1 (2024), pp. 108–111. DOI: 10.54254/2753-8818/42/20240670.

[9] V. Pandichelvi and S. Saranya. "Application of System Linear Diophantine Equations in Balancing Chemical Equations". In: *International Journal for Research in Applied Science and Engineering Technology* 10.10 (2022), pp. 917–920. DOI: 10.22214/ijraset.2022.47111.

[10] Stavros Souravlas, Sofia Anastasiadou, and Angelo Sifaleras. "Mathematical Modeling for Further Improving Task Scheduling on Big Data Systems". In: *Computational Management Science* 20, 40 (2023). DOI: 10.1007/s10287-023-00474-y.

[11] Shinichi Katayama. "Length of Integer Solutions of Linear Diophantine Equations and Related Problems". In: *Journal of Mathematics, the University of Tokushima* 57 (2023), pp. 19–29. https://www-math.st.tokushima-u.ac.jp/journal/2023/2023-2.pdf.

[12] Thomas Barron. *GPU-Accelerated Factorization Sets in Numerical Semigroups via Parallel Bounded Lexicographic Streams*. 2024. DOI: 10.48550/arXiv.2405.07989. arXiv: 2405.07989 [math.CO].

[13] Rania Amer. "The Mathematical Analysis of Linear Diophantine Equations with Two and Three Variables and Its Applications". In: *The Egyptian International Journal of Engineering Sciences and Technology* 42.1 (2023), pp. 23–28. DOI: 10.21608/eijest.2022.164811.1185.

[14] R. Quinlan, M. Shau, and F. Szechtman. "Linear Diophantine Equations in Several Variables". In: *Linear Algebra and its Applications* 640 (2022), pp. 67–90. DOI: 10.1016/j.laa.2021.12.020.

[15] Kim-Manuel Klein and Janina Reuter. *Simple Lattice Basis Computation – The Generalization of the Euclidean Algorithm*. 2023. DOI: 10.48550/arXiv.2311.15902. arXiv: 2311.15902 [cs.DS].

[16] Kenneth H. Rosen. *Elementary Number Theory*. 6th ed. Addison-Wesley, 2011. 766 pp. https://books.google.com/books?id=JqycRAAACAAJ.

[17] Pio J. Arias. *Elementary Number Theory*. Toronto Academic Press, 2024. 261 pp. https://books.google.com/books?id=WIA7OAEACAAJ.