Universidad Industrial de Santander

School of Mathematics

Constructive method for linear Diophantine equations in three variables

(Based on Bézout's lemma)

Abstract

This work presents an explicit and constructive procedure to describe all integer solutions of the linear Diophantine equation $ax + by + cz = d$. The approach relies on Bézout's lemma and on the interpretation of $ax + by + cz$ as a homomorphism $\varphi_n : \mathbb{Z}^3 \to \mathbb{Z}$ with kernel of rank 2, so each solution set is a coset $x_0 + L$. The main result is stated as a theorem and is translated into a two-step algorithm: fix one variable and solve the two-variable equation by means of Bézout, obtaining the complete parametrization in terms of two integers. The geometric reading (parallel integral planes) and the primitive case $\gcd(a, b, c) = 1$, where the recipe simplifies, are included. As an outlook, the extension of the scheme to n variables is sketched for future development.

Framework

The starting point of this work is the relationship between the greatest common divisor (gcd) and the least common multiple (lcm), both supported by the algebraic structure of *integer linear combinations*. Bézout's lemma states that for every pair of integers a, b there exists a combination $ax_0 + by_0 = \gcd(a, b)$, which shows that the set of all common multiples and divisors of a and b is organized by means of a simple linear equation in $\mathbb{Z}^2$. In this way, the notion of divisibility is translated into the existence of integer solutions of a linear identity, establishing the algebraic foundation of every linear Diophantine equation.

When passing to three variables, the interest no longer lies only in checking the existence of solutions, but in *describing them completely*. The problem becomes one of *parametrization*: how to express all possible solutions by means of a minimal number of integer parameters, so that each particular solution can be obtained by substituting suitable values. In this context, "to parametrize well" means to preserve the underlying algebraic structure—the subgroup of homogeneous solutions—and at the same time to keep the method constructive.

This work does not introduce new theory in the strict sense; it relies entirely on already established tools, but organizes them in such a way that they produce an *explicit and direct* description of the general solution of the linear Diophantine equation in three variables. The proposed approach combines Bézout's lemma, the notion of the kernel of a homomorphism, and the free structure of subgroups of $\mathbb{Z}^n$. In this way one obtains an operative method that allows us to pass from abstract theory to an effective construction of all solutions.

From a geometric point of view, the equation

$$ax + by + cz = d$$

defines a family of parallel integral planes in $\mathbb{Z}^3$. Each plane corresponds to a coset $x_0 + L$, where L is the homogeneous subgroup of solutions of $ax + by + cz = 0$. This geometric reading motivates the interpretation of the main result as a complete characterization of that family of planes and of the integral lattice that generates them.

Remark 0.1 (Relationship between Bézout and Diophantine equations). Bézout's lemma may be interpreted as the fundamental case of a linear Diophantine equation in two variables. Every linear equation $a_1x_1 + \cdots + a_nx_n = d$ can be solved recursively by reducing it to an equation in two variables of the form $ax + by = d'$, which is precisely Bézout's form (an elementary exposition of this case may be found in [2]). Thus, the general method does not introduce new ideas, but rather amplifies the original principle of the lemma.

Origin and personal motivation

This work arises from a sustained interest in Bézout's lemma and in the structural role it plays in arithmetic. Although it is usually presented as an elementary result, its reach is much greater: it connects the arithmetic notion of greatest common divisor with an algebraic structure of linear combinations and, at the same time, with a geometric reading in terms of integral lines and planes.

Since my studies on the associativity of the least common multiple, I have worked systematically with Bézout's lemma, finding in it a unifying principle between the arithmetic, the algebraic, and the geometric. This fascination is what drives the present work: to show that, starting from this fundamental identity, one can construct explicit and beautifully simple methods to describe general solutions of Diophantine equations, without resorting to new theory, but by reorganizing the essential elements that Bézout himself leaves us.

Contextualization and comparison of methods

During the development of this topic in class, a method proposed by another student was presented to deal with linear Diophantine equations in three variables, and the rest were invited to reflect on its validity. At that moment I presented the procedure that is developed here, based on Bézout's lemma, and was told that it was not correct. However, the subsequent analysis revealed that the method put forward in this work is not only valid, but actually constitutes a general formulation, whereas the one proposed on that occasion corresponded to a particular case.

The technique of *grouping terms* into a single intermediate variable—for example, substituting $w = 4x + 7y$ in the equation $8x + 14y + 5z = 11$ to reduce it to $2w + 5z = 11$—appears occasionally in different sources and classical number-theory handbooks. Nevertheless, in those texts this reduction is usually presented as an operative device without further theoretical development. In general, elementary treatments of linear Diophantine equations tend to focus exclusively on the case of two variables, while the versions for three or more variables are mentioned only marginally, merely stating that the existence criterion associated with the greatest common divisor extends to n variables, but without offering a complete proof.

The present work seeks to fill this conceptual gap: to establish an explicit description of the equation in three variables as a natural step within the same Bézout framework, showing that the jump from two to three variables does not require new theory, but rather a coherent reorganization of already known arithmetic ideas.

1. Main result

Brief context. Based on Bézout's lemma and on the structure of the subgroup of solutions in $\mathbb{Z}^3$, we obtain an explicit (constructive) description of all integer solutions of $ax + by + cz = d$.

Theorem 1.1 (Integer solutions of $ax + by + cz = d$)**.** *Let $a, b, c, d \in \mathbb{Z}$, with $(a, b) \neq (0, 0)$, and let $g = \gcd(a, b)$. If $\gcd(a, b, c) \mid d$, then the equation*

$$ax + by + cz = d$$

has integer solutions, and all of them are given by

$$\begin{cases} x = x_0 \dfrac{d - ct}{g} + \dfrac{b}{g}\, k, \\ y = y_0 \dfrac{d - ct}{g} - \dfrac{a}{g}\, k, \\ z = t, \end{cases} \qquad k \in \mathbb{Z}, \quad t \in t_0 + \frac{g}{h}\mathbb{Z},$$

where (x_0, y_0) is a Bézout solution of $ax + by = g$. Moreover, the set of solutions is a coset $x_0 + L$, where L is a free subgroup of $\mathbb{Z}^3$ of rank 2.

Note. If $(a, b) = (0, 0)$, the equation reduces to $cz = d$. It has an integer solution if and only if $c \mid d$, in which case $z = d/c$ and x, y are free in $\mathbb{Z}$. This is the degenerate case and is treated separately.

Demostración. Let $h = \gcd(a, b, c)$. If $h \nmid d$, there is no solution. Suppose $h \mid d$ and fix $g = \gcd(a, b)$. Choose $(x_0, y_0) \in \mathbb{Z}^2$ such that $ax_0 + by_0 = g$ (Bézout).

(I) Reminder: two variables. For $D \in \mathbb{Z}$, the equation $ax + by = D$ has an integer solution $\iff g \mid D$. If $g \mid D$, write $D = gq$; then $(x_1, y_1) = (qx_0, qy_0)$ is a solution. If (x, y) and (x', y') are solutions, then $a(x - x') + b(y - y') = 0$, whence $(x - x', y - y') = \left(\frac{b}{g}k,\ -\frac{a}{g}k\right)$ for some $k \in \mathbb{Z}$ (because $\gcd(a/g, b/g) = 1$). Thus,

$$\text{all solutions are } (x, y) = \left(x_0\tfrac{D}{g} + \tfrac{b}{g}k,\ \ y_0\tfrac{D}{g} - \tfrac{a}{g}k\right), \quad k \in \mathbb{Z}. \tag{$*$}$$

(II) Three variables by reduction to two. Given $t \in \mathbb{Z}$, solving $ax + by + cz = d$ with $z = t$ is equivalent to

$$ax + by = d - ct.$$

By $(*)$, this is possible $\iff g \mid (d - ct)$. Since $\gcd(c, g) = \gcd(a, b, c) = h$ and $h \mid d$, there exists $t_0 \in \mathbb{Z}$ satisfying $ct_0 \equiv d \pmod{g}$, and *all* admissible t are

$$t = t_0 + \frac{g}{h}\, s, \qquad s \in \mathbb{Z}.$$

For such t, the quotient $\frac{d-ct}{g}$ is an integer and, by $(*)$, all solutions are given by

$$x = x_0 \frac{d - ct}{g} + \frac{b}{g}\, k, \qquad y = y_0 \frac{d - ct}{g} - \frac{a}{g}\, k, \qquad z = t, \qquad k \in \mathbb{Z}.$$

In other words,

$$\boxed{x = x_0 \frac{d - ct}{g} + \frac{b}{g}\, k, \quad y = y_0 \frac{d - ct}{g} - \frac{a}{g}\, k, \quad z = t, \quad k \in \mathbb{Z}, \ \ t \in t_0 + \tfrac{g}{h}\mathbb{Z}.}$$

(III) Structure. The set of solutions is a coset of $\ker \varphi$, where

$$\varphi : \mathbb{Z}^3 \to \mathbb{Z}, \qquad \varphi(x, y, z) = ax + by + cz.$$

Since $\ker \varphi$ is a free subgroup of $\mathbb{Z}^3$ of rank 2, there exists a particular solution (x_0, y_0, t_0) such that

$$\{(x, y, z) \in \mathbb{Z}^3 : ax + by + cz = d\} = (x_0, y_0, t_0) + \ker \varphi.$$

In other words, the set of solutions is a coset $x_0 + L$, where $L = \ker \varphi$ is a free subgroup of $\mathbb{Z}^3$ of rank 2. □

Corollary 1.2 (Constructive form in two steps)**.** *Let $g = \gcd(a, b)$. Then all integer solutions of $ax + by + cz = d$ are obtained as follows:*

1. *Fix $z = t \in \mathbb{Z}$ such that $g \mid (d - ct)$ and solve $ax + by = d - ct$;*
2. *express the solutions as*

$$x = x_1 + \frac{b}{g}k, \qquad y = y_1 - \frac{a}{g}k, \qquad k \in \mathbb{Z},$$

where (x_1, y_1) is a particular solution of $ax + by = d - ct$, and recover $z = t$.

Example 1.3. For $5x + 4y + 10z = 8$, $g = \gcd(5, 4) = 1$, $(x_0, y_0) = (1, -1)$. Then

$$(x, y, z) = (8 - 10t + 4k,\ -8 + 10t - 5k,\ t), \quad k, t \in \mathbb{Z}.$$

Remark 1.4 (Geometry and limiting cases). Let $g = \gcd(a, b)$ and $h = \gcd(a, b, c)$. The set of solutions is a coset of a free subgroup of $\mathbb{Z}^3$ of rank 2, generated by the direction vectors

$$v_1 = \left(\tfrac{b}{g}, -\tfrac{a}{g}, 0\right) \quad \text{and some} \quad v_2 = (u, v, \tfrac{g}{h}) \in \ker \varphi,$$

where $au + bv = -c\,\frac{g}{h}$. In particular, there exists a v_2 with third component 1 **if and only if** $g \mid c$.

More precisely, if (x_0, y_0, t_0) is a particular solution of $ax + by + cz = d$, then the complete set of solutions is

$$(x, y, z) = (x_0, y_0, t_0) + \langle v_1, v_2 \rangle,$$

which shows that geometrically the solution space is an integral plane in $\mathbb{Z}^3$.

If $c = 0$, one recovers the two-variable case $ax + by = d$; if $g = 1$, the family simplifies.

Remark 1.5 (Parallel family and image of φ_n). Let $n = (a, b, c)$ and $h = \gcd(a, b, c)$. Consider the homomorphism

$$\varphi_n : \mathbb{Z}^3 \to \mathbb{Z}, \qquad \varphi_n(x, y, z) = n \cdot (x, y, z) = ax + by + cz.$$

This map has image $h\mathbb{Z}$ and kernel $L = \ker \varphi_n$ of rank 2. For each $d \in h\mathbb{Z}$, the set of solutions of $n \cdot x = d$ is a *coset* $x_0 + L$, that is, an integral plane "filled" by the lattice L.

If $\gcd(a, b, c) = 1$, then $\mathrm{im}(\varphi_n) = \mathbb{Z}$ and all parallel hyperplanes $n \cdot x = d$ that contain integer points appear (one for each d). If $h > 1$, only those parallels with $d \in h\mathbb{Z}$ exist, spaced by steps of h along the normal.

In particular, dividing the whole equation by h yields the primitive form without changing the solution set, whereas scaling only the coefficients by a factor $s \in \mathbb{Z}$ restricts the possible values of d to $s\,h\mathbb{Z}$.

Application and connection with exploratory problem 5.5 of *Problemas de Teoría de Números* by professor Arnoldo Teherán

Problem. Similarly to the case of linear equations in linear algebra, one can consider systems of linear Diophantine equations. For simplicity, the following system in three variables is proposed:

$$\begin{cases} a_{11}x_1 + a_{12}x_2 + a_{13}x_3 = b_1, \\ a_{21}x_1 + a_{22}x_2 + a_{23}x_3 = b_2, \end{cases} \qquad a_{ij}, b_j \in \mathbb{Z},$$

and one is asked to determine a criterion for this system to have a solution in $\mathbb{Z}$, finding necessary and sufficient conditions to be able to eliminate one variable and obtain a Diophantine equation in two variables that has a solution.

This formulation is solved directly from the theoretical framework built in this work. The *elimination of a variable* corresponds precisely to fixing one variable in the general equation

$$ax + by + cz = d,$$

reducing it to the two-variable case $ax + by = d - ct$. The proposed method shows that this reduction is possible whenever $\gcd(a, b, c) \mid d$, and that the existence of solutions in $\mathbb{Z}$ is equivalent to the divisibility

$$\gcd(a, b) \mid (d - ct),$$

a condition that determines the admissible values of t. Therefore, the "elimination criterion" requested in the problem is expressed in terms of Bézout's lemma: the variable $z = t$ can be fixed freely in an arithmetic progression $t \in t_0 + \frac{g}{h}\mathbb{Z}$ (where $g = \gcd(a, b)$ and $h = \gcd(a, b, c)$), and the remaining variables are determined constructively via Bézout's linear combinations.

Moreover, the same principle extends without conceptual modification to the case of m linear Diophantine equations in three variables, and similarly can be formulated for a general system of m equations in n variables. Each equation

$$a_{i1}x_1 + a_{i2}x_2 + \cdots + a_{in}x_n = b_i, \quad i = 1, \ldots, m,$$

can be interpreted as a homomorphism $\varphi_i : \mathbb{Z}^n \to \mathbb{Z}$, and the complete system as the intersection of m affine preimages

$$\varphi_1^{-1}(b_1) \cap \cdots \cap \varphi_m^{-1}(b_m).$$

In arithmetic terms, each elimination step must preserve the structure of $\mathbb{Z}^n$. This is achieved by $\mathbb{Z}$-linear combinations (unimodular transformations) that allow one to reduce the system without leaving the integer context; equivalently, this procedure corresponds to applying the Smith normal form to the linear map associated with the system [4].

Consequently, the constructive method developed here describes not only the equation in three variables, but also the general mechanism that allows one to address *any finite linear Diophantine system*, repeating the reduction process until reaching an equation in two variables.

Example 1.6 (Arithmetic elimination and structure of the system)**.** To illustrate this principle in action, consider the linear Diophantine system

$$\begin{cases} 4x_1 + 6x_2 + 9x_3 = 7, \\ 3x_1 - 5x_2 + 6x_3 = 4, \end{cases} \qquad x_1, x_2, x_3 \in \mathbb{Z}.$$

We apply a $\mathbb{Z}$-linear combination of the equations by means of the unimodular matrix

$$U = \begin{pmatrix} 2 & -3 \\ 1 & -1 \end{pmatrix} \in \mathrm{GL}_2(\mathbb{Z}), \qquad \det(U) = 1.$$

Multiplying U by the original system, we obtain

$$\begin{cases} 2(4x_1 + 6x_2 + 9x_3) - 3(3x_1 - 5x_2 + 6x_3) = 2, \\ (4x_1 + 6x_2 + 9x_3) - (3x_1 - 5x_2 + 6x_3) = 3, \end{cases}$$

that is,

$$\boxed{-x_1 + 27x_2 = 2} \qquad \text{and} \qquad \boxed{x_1 + 11x_2 + 3x_3 = 3}.$$

The first equation allows us to eliminate x_1, giving $x_1 = 27x_2 - 2$. Substituting into the second,

$$(27x_2 - 2) + 11x_2 + 3x_3 = 3 \implies 38x_2 + 3x_3 = 5.$$

Fixing $x_3 = t \in \mathbb{Z}$, the equation is reduced to the two-variable case:

$$38x_2 = 5 - 3t.$$

Therefore, there is a solution if and only if $\gcd(38, 3) \mid (5 - 3t)$, which is equivalent to the congruence

$$3t \equiv 5 \pmod{38}.$$

Since $3^{-1} \equiv 13 \pmod{38}$, we obtain $t \equiv 27 \pmod{38}$, that is,

$$t = 27 + 38k, \qquad k \in \mathbb{Z}.$$

For such values of t, we have $x_2 = \dfrac{5 - 3t}{38} = -2 - 3k$ and finally

$$x_1 = 27x_2 - 2 = -56 - 81k.$$

We conclude that the complete set of integer solutions of the system is

$$(x_1, x_2, x_3) = (-56, -2, 27) + k\,(-81, -3, 38), \qquad k \in \mathbb{Z}.$$

This result confirms the theoretical structure established earlier: the system has a solution if and only if the divisibility condition imposed by Bézout is satisfied, and the solution set forms a coset of a free subgroup of $\mathbb{Z}^3$ of rank 1, generated by a direction vector belonging to the kernel of the associated linear map.

To verify this, it suffices to substitute the general solution into the original system:

$$\begin{aligned} 4x_1 + 6x_2 + 9x_3 &= 4(-56 - 81k) + 6(-2 - 3k) + 9(27 + 38k) \\ &= -224 - 324k - 12 - 18k + 243 + 342k \\ &= 7, \end{aligned}$$

$$\begin{aligned} 3x_1 - 5x_2 + 6x_3 &= 3(-56 - 81k) - 5(-2 - 3k) + 6(27 + 38k) \\ &= -168 - 243k + 10 + 15k + 162 + 228k \\ &= 4. \end{aligned}$$

Therefore, the family of solutions obtained satisfies both equations for every $k \in \mathbb{Z}$.

2. Primitive case $\gcd(a, b, c) = 1$

According to Remark 1.5, when the greatest common divisor of the coefficients is 1, the image of the homomorphism $\varphi_n(x) = ax + by + cz$ is all of $\mathbb{Z}$. This means that, for any $d \in \mathbb{Z}$, the equation $ax + by + cz = d$ has integer solutions. In this case the equation is already in its *primitive form*. In particular, when moreover $\gcd(a, b) = 1$ (so that there exists (x_0, y_0) with $ax_0 + by_0 = 1$), we have $g = \gcd(a, b) = 1$ and the constraint $g \mid (d - ct)$ disappears: *t is free in $\mathbb{Z}$*. The solution set retains the structure described in the previous remarks: each plane $n \cdot x = d$ is a translate of the subgroup $L = \ker(\varphi_n)$, and successive planes appear one for each integer d.

Corollary 2.1 (Primitive case $\gcd(a, b, c) = 1$ and $\gcd(a, b) = 1$)**.** *If* $\gcd(a, b, c) = 1$ *and* $\gcd(a, b) = 1$*, the equation*

$$ax + by + cz = d$$

has integer solutions for every $d \in \mathbb{Z}$, and the general solution is obtained directly as

$$\begin{cases} x = x_0(d - ct) + bk, \\ y = y_0(d - ct) - ak, \qquad k, t \in \mathbb{Z}, \\ z = t, \end{cases}$$

where (x_0, y_0) is a Bézout solution of $ax + by = 1$; in particular, t is free.

Note. If $\gcd(a, b, c) = 1$ but $\gcd(a, b) = g > 1$, the form of Theorem 1.1 remains valid and t runs through the progression $t \in t_0 + \frac{g}{1}\mathbb{Z} = t_0 + g\mathbb{Z}$, since the condition $g \mid (d - ct)$ is not automatic in that case.

Geometrically, this case corresponds to an infinite family of integral planes parallel to each other, each one "filled" by the rank-2 lattice L. Each value of d produces a distinct coset $x_0 + L$, and all integers are attained as d varies, in contrast with the cases with $\gcd(a, b, c) > 1$, where only multiples of that value appear.

Remark 2.2. In practice, this is the most useful equation: elementary exercises and classic problems treated in the academy are usually adapted precisely to this form. It was from this formulation that the entire work was developed: first I obtained the equation by a direct route, and subsequently I built the theoretical framework needed to justify the neatness and algebraic coherence of its structure.

Conclusion

The expression obtained shows that the structure of the solutions of the equation

$$ax + by + cz = d$$

arises naturally from Bézout's lemma, without the need for additional tools. The procedure exhibits a recursive pattern: each new variable introduces a congruence that preserves the form of the solutions and the free structure of the homogeneous subgroup.

In this sense, the case of three variables is the first visible instance of the general mechanism governing all linear Diophantine equations in $\mathbb{Z}^n$: a chain of unimodular linear combinations that leave the integer arithmetic intact.

This viewpoint suggests that Bézout's lemma is not just an isolated result, but the generating principle of the entire linear Diophantine theory.

Referencias

[1] K. Ireland and M. Rosen, *A Classical Introduction to Modern Number Theory*, 2nd ed., Springer-Verlag, New York, 1990.

[2] I. Niven, H. S. Zuckerman, H. L. Montgomery, *An Introduction to the Theory of Numbers*, 5th ed., John Wiley & Sons, 1991.

[3] T. M. Apostol, *Introduction to Analytic Number Theory*, Springer, 1976.

[4] D. S. Dummit and R. M. Foote, *Abstract Algebra*, 3rd ed., John Wiley & Sons, 2004.

[5] A. Teherán Herrera, *Problemas de Teoría de Números*, Universidad Industrial de Santander, 2025. Available at: `https://drive.google.com/...` (Accessed on 25-Oct-2025).

[6] K. Zelator, *Lattice Points on the Plane $ax + by + cz = d$ and the Diophantine System $ax + by + cz = d$, $ex + fy + gz = h$*, `arXiv:0805.1702` [math.GM], 2008. Available at: https://arxiv.org/abs/0805.1702.

[7] B. Kenaga, *Linear Diophantine Equations*, online Number Theory course, Millersville University. Available at: https://sites.millersville.edu/bikenaga/number-theory/linear-diophantine-equations/linear-diophantine-equations.html (Accessed on 25-Oct-2025).