Title: New simple formula to solve diophantic linear equations.
Author: Zeolla, Gabriel Martín
Comments: 12 pages
gabrielzvirgo@hotmail.com

Keywords: Linear diophantic equations

Abstract: This document writes a new, very simple algorithm to solve linear diophantic equations in their particular solution, without having to solve them with the Euclid algorithm and the Bezout identity among others.
The algorithm is very simple, fast and practical, we can choose any method to find the GCD and then replace it in the formula. This algorithm helps us to predict whether the result belongs to integers numbers or natural numbers.

Introducción

The Diophantine equations, which, as their name indicates, are due to Diophantus, an ancient Greek mathematician whose work had great importance and influence on later generations. The problems dealt with by Diophantus dealt with merely numerical aspects in which the properties of integers intervene.

There are several methods for solving linear Diophantian equations, from the method of Diophantus, Euler and others.

Linear Diophantine equations are the expressions $ax + by = c$, where a, b, c are given integers, so x, y are the integer variables to be found. The so-called "Bézout Lemma" states that the system has a solution if and only if $d = mcd(a, b)$ divides c. In that case the equation has infinite solutions.

Theorem: Let $a, b, c \in \mathbb{Z}$. The Diophantine equation $ax + by = c$ has an integer solution if, and only if the greatest common divisor of a and b divides c.

Demonstration:
Suppose that the integers x_0 and y_0 are a solution to the equation $ax + by = c$
with this we have that $ax_0 + by_0 = c$. Then if $d = mcd\ (a, b)$, then
$d = mcd\ (a, b) \rightarrow d \mid a$ and $d \mid b \rightarrow d \mid (ax0 + by0) \rightarrow d \mid c$

Greatest Common Divisor

Definition: Given the integers $a;\ b > 0$, we define greatest common divisor of a and b, as the largest number that divides both a and b. It is denoted in two ways: $(a;\ b) = c\ or\ gcd(a;\ b) = c$. We will use $(a;\ b)$ to denote the greatest common divisor.

Example. Let's find GCD of 20 and 25. The divisors are of 20:$\pm1; \pm2; \pm4; \pm5, \pm10, \pm20$, the divisors of 25 are: $\pm1; \pm5, \pm25$ and the common divisors of 20 and 25 are; $\pm1; \pm5$, and the greatest common divisor is 5, so the GCD of 20 and 25 is 5 and by notation (20; 25) = 5.

Definition: If the greatest common divisor of $(a;\ b)\ =\ 1$, we say that the integers are relatively prime, or coprime.

Example

$$ax + by = c$$

$$\boldsymbol{7x + 3y = 100}$$
$$d = MCD(7,3) = 1$$
$$\therefore\ has\ a\ solution\ since\ \ 1|100$$

A) Particular solution of the equation: **Using Euclid's algorithm and Bezout's lemma**

$$\boldsymbol{7x_0 + 3y_0 = 1}$$
$$x_0 = 1$$
$$y_0 = -2$$

$$\therefore 7 * 1 + 3 * (-2) = 1$$

B) Particular Final Solution

Then $7\text{x} + 3\text{y} = 100$

I multiply by 100 on both sides of the previous result (A)

$$7 * (1 * 100) + 3 * (-2 * 100) = 1 * 100$$
$$\boldsymbol{7 * 100 + 3 * (-200) = 100}$$

C) General Solution

$$\begin{cases} x = x_0 * C - \dfrac{b}{d} * k \\ y = y_0 * C + \dfrac{a}{d} * k \end{cases}$$

$$C = c/d$$
$$C = 100/1$$

$K \in \mathbb{Z}$

$$x = 1 * 100 - \frac{3}{1} * k \qquad \boldsymbol{x = 100 - 3k}$$
$$y = -2 * 100 + \frac{7}{1} * k \qquad \boldsymbol{y = -200 + 7k}$$

Replacing x, y in the initial equation:

$$7\text{x} + 3\text{y} = 100$$
$$\therefore\quad \boldsymbol{7(100 - 3k) + 3(-200 + 7k) = 100}$$

New simple formula to solve diophantic linear equations

$$\forall\, |\boldsymbol{a}| < |\boldsymbol{b}| \quad a, b, c, d, x, y, z \in \boldsymbol{Z}$$

$$\boldsymbol{ax \pm by = c}$$

$$\left(\pm\frac{\boldsymbol{z} * |\boldsymbol{b}| \pm \boldsymbol{d}}{\boldsymbol{k}}, \pm\frac{\boldsymbol{z} * |\boldsymbol{a}| \pm \boldsymbol{d}}{\boldsymbol{k}}\right)$$

The algorithm presents 2 variables for its positive form and 2 variables for its negative form, when $|\boldsymbol{a}| < |\boldsymbol{b}|$

$z\ is\ the\ difference\ between\ |\boldsymbol{x_0}|, |\boldsymbol{y_0}|$

$K\ is\ the\ difference\ between\ |a - b|$

$d = GCD$

In the next examples it will be clearer how to obtain (z).

****

Chapter I

New positive algorithm

$$ax + by = c$$

$$ax_0 + by_0 = GCD(a, b)$$

The result of this can have two variables, one when $\boldsymbol{x_0}$ is positive and $\in \mathbb{N}$ and another when $-\boldsymbol{x_0}$ is negative and $\in \mathbb{Z}$. The same thing happens in the opposite way for the $\boldsymbol{y_0}$.

Variable I: (positive) x

$$(x_0, -y_0)$$

$$\left(\frac{\boldsymbol{z} * |\boldsymbol{b}| - \boldsymbol{d}}{\boldsymbol{k}}, -\frac{\boldsymbol{z} * |\boldsymbol{a}| - \boldsymbol{d}}{\boldsymbol{k}}\right)$$

Variable II: (negative)

$$(-\boldsymbol{x_0}, \boldsymbol{y_0})$$

When x is negative we add the minus before the parentheses to the previous formula

$$-\left(\frac{z * |b| - d}{k}, -\frac{z * |a| - d}{k}\right)$$

$$= \left(-\frac{\boldsymbol{z} * |\boldsymbol{b}| + \boldsymbol{d}}{\boldsymbol{k}}, \frac{\boldsymbol{z} * |\boldsymbol{a}| + \boldsymbol{d}}{\boldsymbol{k}}\right)$$

What variable do we use then?

The algorithm to find the particular solution A and B then has two possibilities from which we must choose one.

$$(x_0, -y_0) \; or \; (-x_0, y_0)$$

$$\left(\frac{z * |b| - d}{k}, -\frac{z * |a| - d}{k}\right) \; or \; \left(-\frac{z * |b| + d}{k}, \frac{z * |a| + d}{k}\right)$$

To know which of the two variables we should use, we only have to take into account the following:

$$x_0 = K|\, z * b - d \quad or \quad x_0 = K|\, z * b + d$$

If K divides and works with the first we use the left formula, otherwise we use the right formula. It could also be checked using y_0 but using one of the two is enough to know which variable to use.

New positive algorithm

$$\forall\, |a| < |b| \;\; a, b, c, d, x, y, z \in \mathbb{Z}$$

$$ax + by = c$$
$$it\ has\ a\ solution\ S \leftrightarrow GCD(a, b)\ |c$$

$$ax_0 + by_0 = d$$
$$d = GCD(a, b)$$
$$k = |a - b|$$

$$|a| \,\Lambda\, |b| \equiv r(mod\ K)$$

$When\ d \neq r$

$$Z = \left|\frac{k * n \pm d}{r}\right|$$

$When\ d = |r|$ or $r = 0$

$$Z = 1$$

$Z, n \in \mathbf{N} \neq 0$

$$Z = \; is\ the\ difference\ between\ |x_0|, |y_0|$$

Particular solution, Variable I:

$$(x_0, -y_0)$$

$$\left(\frac{z * |b| - d}{k}, -\frac{z * |a| - d}{k}\right)$$

Particular solution, Variable II:

$$(-x_0, y_0)$$

$$\left(-\frac{z * |b| + d}{k}, \frac{z * |a| + d}{k}\right)$$

$$\boldsymbol{ax + by = c}$$
$$\boldsymbol{When\ |a| > |b|}$$

Starting from variable I

For | a | > | b | they change positions

$$(-\boldsymbol{x_0}, \boldsymbol{y_0})$$

$$\left(-\frac{z * |a| - d}{k}, \frac{z * |b| - d}{k}\right) = Variable\ III$$

Starting from variable II

For | a |> |b |they change positions

$$(\boldsymbol{x_0}, -\boldsymbol{y_0})$$

$$\left(\frac{z * |a| + d}{k} - \frac{z * |b| + d}{k}\right) = Variable\ IV$$

Example 1: Solve the Diophantine Sum Equation

$$\boldsymbol{25x + 36y = 10}$$
$$it\ has\ a\ solution\ \ \boldsymbol{S} \leftrightarrow GCD(25,36)|10 \qquad S = 10$$

$$\boldsymbol{25x_0 + 36y_0 = 1}$$
$$k = |25 - 36| = 11$$

$$25\ \Lambda\ 36 \equiv 3(mod\ 11)$$
$$When\ GCD \neq r$$
$$Z = \left|\frac{11 + 1}{3}\right| = 4, is\ the\ difference\ between\ |\boldsymbol{x_0}|, |\boldsymbol{y_0}|$$

Particular solution A

$$\left(\frac{4 * 36 - 1}{11}, -\frac{4 * 25 - 1}{11}\right) = (13, -9)$$

Solution A: $\boldsymbol{x_0 = 13} \quad \boldsymbol{y_0 = -9}$

Particular solution B

$$\boldsymbol{S * x_0\ \Lambda\ S * y_0}$$
$$\boldsymbol{x = 130, y = -90}$$

Replacing in the initial equation

$$\boldsymbol{\therefore 25 * 130 + 36 * (-90) = 10}$$

Example 2: Solve the Diophantine Sum Equation

$$\mathbf{35x + 55y = 100}$$

$$it\ has\ a\ solution\ \boldsymbol{S} \leftrightarrow GCD(35,55)|100 \qquad S = 20$$

$$\mathbf{35x_0 + 55y_0 = 5}$$

$$k = |35 - 55| = 20$$

$$35\ \Lambda\ 55 \equiv -5(mod\ 20)$$

$$When\ GCD = |r|$$

$$Z = 1, is\ the\ difference\ between\ |x_0|, |y_0|$$

Particular solution A

$$\boldsymbol{s}(-\boldsymbol{x_0}, \boldsymbol{y_0})$$

$$\left(-\frac{1 * 55 + 5}{20}, \frac{1 * 35 + 5}{20}\right) = (-3, 2)$$

Solution A: $\boldsymbol{x_0 = -3} \quad \boldsymbol{y_0 = 2}$

Particular solution B

$$\boldsymbol{S * x_0\ \Lambda\ S * y_0}$$

$$\boldsymbol{x = -60}\ , \quad \boldsymbol{y = 40}$$

Replacing in the initial equation

$$\boldsymbol{\therefore 35 * (-60) + 55 * 40 = 100}$$

Chapter II

New negative algorithm

$$ax - by = c$$

$$ax_0 - by_0 = GCD(a, b)$$

The result of this can have two variables, one when $\boldsymbol{x_0}$, $\boldsymbol{y_0}$ are positive and $\in \mathbb{N}$.
Another when $-\boldsymbol{x_0}$, $-\boldsymbol{y_0}$ are negative $\in \mathbb{Z}$.

Variable V (positive)

$$(\boldsymbol{x_0}, \boldsymbol{y_0})$$

$$\left(\frac{\boldsymbol{z} * |\boldsymbol{b}| - \boldsymbol{d}}{\boldsymbol{k}}, -\frac{\boldsymbol{z} * |\boldsymbol{a}| - \boldsymbol{d}}{\boldsymbol{k}}\right) \; Initial\ formula, Variable\ I$$

When y is negative we add the minus in the position of the y in the previous formula

$$\left(\frac{z * |b| - d}{k}, -\left(-\frac{z * |a| - d}{k}\right)\right)$$

$$\left(\frac{\boldsymbol{z} * |\boldsymbol{b}| - \boldsymbol{d}}{\boldsymbol{k}}, \frac{\boldsymbol{z} * |\boldsymbol{a}| - \boldsymbol{d}}{\boldsymbol{k}}\right) = \boldsymbol{variable\ V}$$

Variable VI (negative)

$$(-x_0, -y_0)$$

$$\left(-\frac{\boldsymbol{z} * |\boldsymbol{b}| + \boldsymbol{d}}{\boldsymbol{k}}, \frac{\boldsymbol{z} * |\boldsymbol{a}| + \boldsymbol{d}}{\boldsymbol{k}}\right) \; Initial\ formula, Variable\ II$$

When y is negative we add the minus in the position of the y in the previous formula

$$\left(-\frac{z * |b| - d}{k}, -\frac{z * |a| - d}{k}\right)$$

$$\left(-\frac{\boldsymbol{z} * |\boldsymbol{b}| + \boldsymbol{d}}{\boldsymbol{k}}, -\frac{\boldsymbol{z} * |\boldsymbol{a}| + \boldsymbol{d}}{\boldsymbol{k}}\right) = Variable\ VI$$

We choose between variables V and VI, where K divides to obtain a correct solution.

New negative algorithm

$$\forall\, |\boldsymbol{a}| < |\boldsymbol{b}| \quad a,b,c,d\,,x,y,z \in \mathbb{Z}$$
$$\boldsymbol{ax - by = c}$$
$$it\ has\ a\ solution\ \boldsymbol{S} \leftrightarrow GCD(a,b)\ |c$$

$$\boldsymbol{ax_0 - by_0 = d}$$
$$d = GCD(a,b)$$
$$k = |a-b|$$

$$\boldsymbol{|a|\ \Lambda\ |b| \equiv r(mod\ K)}$$

$When\ d \neq r$ $\qquad$ $When\ d = |r|$ or $r = 0$

$$Z = \left|\frac{k * n \pm d}{r}\right| \qquad Z = 1$$

$Z, n \in \mathbb{N}$ ≠0

$$Z = \ is\ the\ difference\ between\ |x_0|, |y_0|$$

Particular solution, Variable V:

$$(\boldsymbol{x_0}\,, \boldsymbol{y_0})$$

$$\left(\frac{\boldsymbol{z} * |\boldsymbol{b}| - \boldsymbol{d}}{\boldsymbol{k}}, \frac{\boldsymbol{z} * |\boldsymbol{a}| - \boldsymbol{d}}{\boldsymbol{k}}\right)$$

Particular solution, Variable VI:

$$(-\boldsymbol{x_0}, -\boldsymbol{y_0})$$

$$\left(-\frac{\boldsymbol{z} * |\boldsymbol{b}| + \boldsymbol{d}}{\boldsymbol{k}}, -\frac{\boldsymbol{z} * |\boldsymbol{a}| + \boldsymbol{d}}{\boldsymbol{k}}\right)$$

$$ax - by = c$$
$$When\ |a| > |b|$$

Starting from variable V

$For\ |\ a\ |> |b\ |\ signs\ and\ positions\ change$

$$(x_0\,, y_0) \rightarrow (-x_0\,, -y_0)$$

$$\left(-\frac{\boldsymbol{z} * |\boldsymbol{a}| - \boldsymbol{d}}{\boldsymbol{k}}, -\frac{\boldsymbol{z} * |\boldsymbol{b}| - \boldsymbol{d}}{\boldsymbol{k}}\right) = \boldsymbol{Variable\ VII}$$

Starting from variable VI

$For\ |\ a\ |> |b\ |\ signs\ and\ positions\ change$

$$(-x_0\,, -y_0) \rightarrow (x_0\,, y_0)$$

$$\left(\frac{\boldsymbol{z} * |\boldsymbol{a}| + \boldsymbol{d}}{\boldsymbol{k}}, \frac{\boldsymbol{z} * |\boldsymbol{b}| + \boldsymbol{d}}{\boldsymbol{k}}\right) = \boldsymbol{Variable\ VIII}$$

Diophantic equation example with subtraction

Example 3: Solve $7x \equiv 5\ (mod\ 9)$ by using Diophantine equation. To find a solution, we need only obtain a solution of the linear Diophantine equation $7x - 9y = 5$.

$$\boldsymbol{7x - 9y = 5}$$
$$it\ has\ a\ solution\ \boldsymbol{S} \leftrightarrow GCD(7,9)|5$$
$$S = 5$$
$$\boldsymbol{7x_0 - 9y_0 = 1}$$
$$k = |7 - 9| = 2$$

$$7\ \Lambda\ 9 \equiv 1(mod\ 2)$$
$$When\ GCD = r \rightarrow Z = 1, is\ the\ difference\ between\ |x_0|, |y_0|$$

Particular solution A : **I use the variable V**

$$(\boldsymbol{x_0}, \boldsymbol{y_0})$$

$$\left(\frac{1 * 9 - 1}{2}, \frac{1 * 7 - 1}{2}\right) = (4,3)$$

Solution A: $\boldsymbol{x_0 = 4} \quad \boldsymbol{y_0 = 3}$

Particular solution B

$$\boldsymbol{S * x_0\ \Lambda\ S * y_0}$$
$$\boldsymbol{x = 20} \qquad \boldsymbol{y = 15}$$
Replacing in the initial equation
$$\boldsymbol{\therefore 7 * 20 - 9 * 15 = 5}$$

Example 4: Solve the Diophantine Subtraction Equation

$$\boldsymbol{35x - 55y = 100}$$
$$it\ has\ a\ solution\ \boldsymbol{S} \leftrightarrow GCD(35,55)|100$$
$$S = 20$$
$$\boldsymbol{35x - 55y = 5}$$
$$k = |35 - 55| = 20$$

$$35\ \Lambda\ 55 \equiv -5(mod\ 20)$$
$$When\ GCD = |r| \rightarrow Z = 1, is\ the\ difference\ between\ |x_0|, |y_0|$$

Particular solution A

I use the variable VI $(-\boldsymbol{x_0}, -\boldsymbol{y_0})$

$$\left(-\frac{1 * 55 + 5}{20}, -\frac{1 * 35 + 5}{20}\right) = (-3, -2)$$

Solution A: $\boldsymbol{x_0 = -3} \quad \boldsymbol{y_0 = -2}$

Particular solution B

$$\boldsymbol{S * x_0\ \Lambda\ S * y_0}$$
$$\boldsymbol{x = -60} \qquad \boldsymbol{y = -40}$$
Replacing in the initial equation
$$\boldsymbol{\therefore 35 * (-60) - 55 * (-40) = 100}$$

Chapter III

Special K values

Recall that k is the difference between a, b

There are values of K that for all their combinations between $\boldsymbol{a}$ and $\boldsymbol{b}$ always Z = 1

$$When\ K = \{1,2,3,4,6\} \rightarrow Z = 1$$

Since the GCF and the remainder are always the same number.

Example A: k=4	Example B: k=6
$\boldsymbol{25x + 29y = 10}$ $\boldsymbol{GCD = 1}$ $k = \lvert 25 - 29 \rvert = 4$ $25\ \Lambda\ 29 \equiv \boldsymbol{-1}(mod\ 4)$ *GCD*=$\lvert r \rvert$→Z=1	$\boldsymbol{39x + 45y = 12}$ $\boldsymbol{GCD = 3}$ $k = \lvert 39 - 45 \rvert = 6$ $39\ \Lambda\ 45 \equiv \boldsymbol{-3}(mod\ 6)$ *GCD*=$\lvert r \rvert$→Z=1

Demonstration

$\boldsymbol{ax + by = GCD(a,b)}$ $k = \lvert a - b \rvert$ $a\ \Lambda\ b \equiv \boldsymbol{r}(mod\ k)$ $When\ GCD = r \rightarrow \boldsymbol{Z = 1}$ $Z = \left\lvert \frac{kx \pm GCD}{r} \right\rvert$ $If\ x = 0, then\ Z = 1$	applying modular arithmetic we prove the result of Z = 1 $\boldsymbol{kx \equiv GCD(mod\ r)}$ $K(x) - r(y) = GCD$ $So\ if\ x = 0, y = 1$ $\therefore\ r = GCD\ and\ Z = y = 1$

When K ≠{1,2,3,4,6} they also have combinations where z = 1 but not for all cases.

Example k=12, form a pattern of 12 remains

$$\boldsymbol{ax + by = GCD(a,b)}$$
$$a \Lambda b \equiv \boldsymbol{r}(mod\ k)$$

a	b	GCD	residue +	residue -	result
1	13	**1**	1	11	Z=1
2	14	**2**	2	10	Z=1
3	15	**3**	3	9	Z=1
4	16	**4**	4	8	Z=1
5	17	**1**	5	7	Z≠1
6	18	**6**	6	6	Z=1
7	19	**1**	7	5	Z≠1
8	20	**4**	8	4	Z=1
9	21	**3**	9	3	Z=1
10	22	**2**	10	2	Z=1
11	23	**1**	11	1	Z=1
12	24	**12**	0	12	Z=1

In the cases where z = 1 it is precisely where the GCF = |r|, for which |r| is a divisor of K.
Then for the cases where |r| does not divide K, z ≠1

Where K is a prime number greater than 2 this only has 3 combinations where z = 1

$$a \Lambda b \equiv \mathbf{1}(mod\ P) \rightarrow z = 1$$
$$a \Lambda b \equiv \mathbf{-1}(mod\ P) \rightarrow z = 1$$
$$a \Lambda b \equiv \mathbf{0}\ (mod\ P) \rightarrow z = 1$$

We can previously know which algorithm variable to use?

Yes, for the cases where $r\ is\ 1\ or\ -1$ it is possible to know the variable and to know if the result has a solution for the integers numbers or for the natural numbers.

$$When\ r = 1\ use\ the\ positive\ algorithm.$$
$$When\ r = -1\ use\ the\ negative\ algorithm.$$

$$When\ k = a \Lambda r = 0\ use\ the\ positive\ algorithm$$
$$When\ k \neq a \Lambda r = 0\ use\ the\ negative\ algorithm$$

****

Conclution

The algorithm works correctly and it is a great novelty since this method is totally unknown.
There are many ways to solve a diophantic equation, this is another different way that comes to contribute and provides a greater understanding of the subject.
Without a doubt, it is very easy to solve equations using this algorithm.
Solving diophantic equations for the special cases of K is just a matter of replacing numbers, to find the result.
This algorithm allows to anticipate if the result belongs to the integers numbers or to the natural numbers.
I think it is a practical and interesting method for the student.

Professor Zeolla Gabriel Martín
11/11/2021

References

[1] J.Knig, Einleitung, Algebraischen Grszen Leipzig, 1903, 347-460
[2] Th.Schnemann, Jour fr.Math 19, 1839, 292
[3] M.Fekete, Math_es Phys.Lapok, Budapest, 17, 1908, 328-49
[4] Leonard Eugene Dickson,History Of The Theory Of Numbers, Chelsea Publishing Company, New York, 1992
[5] Gareth A.Jones and J.Mary Jones, Elemantary Number Theory, Springer-Verlag London Limited, Great Britain, 1998
[6] Joseph H.Silverman, A Friendly Introduction To Number Theory, Precentice-Hall,Inc., New Jersey, 2001
[7] H.E.Rose, A Course In Number Theory,Clarendon Press, New York, 1994
[8] William Judson Leveque, Topics In Number Theory, Addison-Wesley Publishing Company, USA, 1958
[9] Ivan Niven, Herbert S.Zuckerman, An Introduction To The Theory Of Numbers, John Wiley Sons,Inc., USA, 1967