La Ecuación $xa + yb = c$

Alan Reyes-Figueroa
Teoría de Números

(Aula 06) 21.julio.2025

La ecuación $xa + yb = c$

Recordemos:

Teorema (Teorema de Bézout)

Para todo $a, b \in \mathbb{Z}$*, existen* $M, N \in \mathbb{Z}$ *tales que* $Ma + Nb = d$*,* $d = (a, b)$*.*

Propiedad

La ecuación diofantina $xa + yb = c$ *admite solución en* $\mathbb{Z}$ *si, y sólo si,* $d \mid c$*, donde* $d = (a, b)$*.*

Si (x_0, y_0) *es una solución particular de la ecuación, entonces todas las otras soluciones son de la forma*

$$x = x_0 + \tfrac{b}{d}t, \qquad y = y_0 - \tfrac{a}{d}t, \qquad t \in \mathbb{Z}.$$

<u>Prueba</u>: ($\Rightarrow$) Como $d = (a, b)$ existen enteros $r, s \in \mathbb{Z}$ con $a = dr$, $b = ds$.

La ecuación $xa + yb = c$

Si existe una solución $(x_0, y_0) \in \mathbb{Z}^2$, entonces

$$c = x_0 a + y_0 b = x_0(dr) + y_0(ds) = d(x_0 r + y_0 s) \quad \Rightarrow \quad d \mid c.$$

$(\Leftarrow)$ Sea $d \mid c$. Entonces $c = dq$, para algún $q \in \mathbb{Z}$. Por el Teorema de Bézout, existen enteros $M, N \in \mathbb{Z}$ tales que $d = Ma + Nb$. Entonces

$$(Mq)a + (Nq)b = (Ma + Nb)q = dq = c,$$

y $(Mq, Nq) \in \mathbb{Z}^2$ es una solución de $xa + yb = c$.

Para la segunda afirmación del teorema, supongamos que se conoce una solución $(x_0, y_0) \in \mathbb{Z}^2$ de la ecuación dada. Si $(x', y') \in \mathbb{Z}^2$ es cualquier otra solución, entonces $ax_0 + by_0 = c = ax' + by'$. Lo anterior es equivalente a $a(x' - x_0) = b(y_0 - y')$.

La ecuación $xa + yb = c$

Tenemos $a(x' - x_0) = b(y_0 - y')$.
De nuevo, como $d = (a, b)$, existen enteros primos relativos r y s, tales que $a = dr$, $b = ds$. Sustituyendo estos valores en la ecuación anterior y cancelando el factor común d, entonces

$$r(x' - x_0) = s(y_0 - y').$$

La situación es ahora la siguiente: $r \mid s(y_0 - y')$, con $(r, s) = 1$. Del lema de Euclides, $r \mid y_0 - y'$; ó, en otras palabras, $y_0 - y' = rt$ para algún número entero $t \in \mathbb{Z}$.
Sustituyendo, obtenemos

$$x' - x_0 = st.$$

Esto lleva a las fórmulas

$$x' = x_0 + st = x_0 + \tfrac{b}{d}t, \qquad y' = y_0 - rt = y_0 - \tfrac{a}{d}t.$$

Sin importar el valor de $t \in \mathbb{Z}$, estos valores satisfacen la ecuación diofantina, pues

$$\begin{aligned} ax' + by' &= a\left(x_0 + \tfrac{b}{d}t\right) + b\left(y_0 - \tfrac{a}{d}t\right) = (ax_0 + by_0) + \underbrace{\left(\tfrac{ab}{d} - \tfrac{ab}{d}\right)}_{=0}t \\ &= c \end{aligned}$$

Entonces, existen infinitas soluciones a la ecuación, una para cada $t \in \mathbb{Z}$, en la forma requerida. $\square$

Corolario

Si $(a, b) = 1$ y si $(x_0, y_0) \in \mathbb{Z}^2$ es una solución particular de la ecuación diofantina $xa + yb = c$, entonces todas las soluciones son de la forma

$$x = x_0 + bt, \qquad y = y_0 - at, \qquad t \in \mathbb{Z}.$$

Ejemplos

Discutir la solución general para las siguientes ecuaciones diofantinas:

i) $6x + 51y = 22$

ii) $14x + 35y = 93$

iii) $33x + 14y = 115$.

Ejemplos

Solución: Las primeras dos ecuaciones no poseen solución, pues $3 \nmid 22$ y $7 \nmid 93$.

La tercera ecuación, $33x + 14y = 115$, $d = (33, 14) = 1$ y $1|115$. Entonces esta ecuación lineal sí posee soluciones enteras.
Para encontrarlas, resolvemos la ecuación homogénea $33x + 14y = 1$, mediante el algoritmo de Euclides. Tenemos:

$$\begin{aligned} 33 &= 2(14) + 5 \\ 14 &= 2(5) + 4 \\ 5 &= 1(4) + 1. \end{aligned}$$

Así que $1 = 5 - 4 = 5 - (14 - 2 \cdot 5) = 3(5) - 14 = 3(33 - 2 \cdot 14) - 14 = 3(33) - 6(14)$.
Multiplicando esta última ecuación por 115, obtenemos $345(33) - 805(14) = 115$, lo que produce la solución base $x_0 = 345$, $y_0 = -805$.

El resto de soluciones enteras está dada por la parametrización

$$x = 345 + 14t, \qquad y = -805 - 33t, \qquad t \in \mathbb{Z}.$$

Generalizacioness

Hemos visto que el MDC es asociativo, esto es $((a,b),c) = (a,(b,c))$ para $a,b,c \in \mathbb{Z}$. Definimos la notación

$$(a,b,c) = MDC(a,b,c) = ((a,b),c) = (a,(b,c)).$$

En general, para una secuencia finita de enteros $a_1, a_2, \ldots, a_n \in \mathbb{Z}$, definimos

$$(a_1, a_2, \ldots, a_n) = MDC(a_1, a_2, \ldots, a_n).$$

Gracias a la asociatividad, este máximo divisor común generalizado se calcula de forma inductiva

$$(a_1, a_2, \ldots, a_n) = ((a_1, a_2, \ldots, a_{n-1}), a_n).$$

Propiedad (Bézout)

Para cualesquiera $a,b,c \in \mathbb{Z}$, existen $M,N,P \in \mathbb{Z}$ tales que $Ma + Nb + Pc = d$, $d = (a,b,c)$.

Ejemplos

Prueba: Sea $d = (a, b, c)$. Primero calculamos $d_1 = (a, b)$. Por el Teorema de Bézout, existen enteros $M_1, N_1 \in \mathbb{Z}$ tales que

$$M_1 a + N_1 b = d_1.$$

Ahora consideramos $d = (d_1, c)$. De nuevo, por el Teorema de Bézout, existen enteros $Q, P \in \mathbb{Z}$ tales que

$$Qd_1 + Pc = d.$$

Sustituyendo la primera igualdad en la segunda, obtenemos

$$d = Qd_1 + Pc = Q(M_1 a + N_1 b) + Pc = (QM_1)a + (QN_1)b + Pc.$$

Haciendo, $M = QM_1 \in ZZ, N = QN_1 \in \mathbb{Z}, P \in \mathbb{Z}$, resulta

$$Ma + Nb + Pc = d. \quad \square$$

Propiedad (Bézout Generalizado)

Para cualesquiera $a_1, a_2, \ldots, a_n \in \mathbb{Z}$*, existen* $M_1, M_2, \ldots, M_n \in \mathbb{Z}$ *tales que*

$$M_1 a_1 + M_2 a_2 + \ldots + M_n a_n = d, \quad con\ d = (a_1, \ldots, a_n).$$

Prueba: Se resuelve por inducción sobre el Teorema de Bézout. (Ejercicio!).

¿Qué ocurre con la ecuaciones lineales de más de dos variables?
Al igual que en el teorema de Bézout, tenemos la siguiente generalización

Teorema (Soluciones enteras de ecuaciones lineales)

La ecuación diofantina $a_1x_1 + a_2x_2 + \ldots + a_nx_n = k$ admite solución en $\mathbb{Z}$ si, y sólo si, $d \mid k$, donde $d = (a_1, \ldots, a_n)$.

Si $(x_{1,0}, x_{2,0}, \ldots, x_{n,0}) \in \mathbb{Z}^n$ es una solución particular de esta ecuación, entonces todas las otras soluciones son de la forma

$$\begin{aligned} x_1 &= x_{1,0} + c_{1,2}t_2 + \ldots + c_{1,n}t_n, \\ x_2 &= x_{2,0} + c_{2,2}t_2 + \ldots + c_{2,n}t_n, \\ &\vdots \\ x_{n-1} &= x_{n-1,0} + c_{n-1,2}t_2 + \ldots + c_{n-1,n}t_n, \\ x_n &= t_n, \end{aligned}$$

donde las $c_{i,j}$ son constantes enteras, y los $t_2, t_2, \ldots, t_n \in \mathbb{Z}$ corresponden a $n-1$ parámetros enteros.

Ejemplo

Ejemplo: Hallar las soluciones enteras de la ecuación $6x + 9y + 15z = 12$.

Solución: Sea $d = (6, 9, 15) = 3$ y $3 \mid 12 \;\Rightarrow$ hay soluciones enteras. Dividiendo entre d, resolvemos la ecuación fundamental $2x + 3y + 5z = 4$.

Fijamos $z = s \in \mathbb{Z}$. Entonces hacemos $2x + 3y = 4 - 5s = k_s$, y resolvemos la eq. base $2x + 3y = 1$.
$(x_0, y_0) = (-1, 1) \in \mathbb{Z}^2$ es solución. Luego, el resto de soluciones están dadas por

$$x = -1 + 3t, \qquad y = 1 - 2t, \qquad t \in \mathbb{Z}.$$

De ahí que las soluciones de $2x + 3y = k_s$ son de la forma

$$x = -k_s + 3t, \qquad y = k_s - 2t, \qquad t \in \mathbb{Z}.$$

Así,

$$\begin{aligned} x &= -4 + 5s - 3t, \\ y &= 4 - 5s - 2t, \\ z &= s, \qquad\qquad \text{para } s, t \in \mathbb{Z}. \;\square \end{aligned}$$

Ejemplo

Estas son las soluciones de $2x + 3y + 5z = 4$, y también son las soluciones de la ecuación original $6x + 9y + 15z = 12$.

La siguiente tabla muestra algunas de las soluciones obtenidas

s	t	x	y	z	$6x + 9y + 15z$
-1	-1	-12	11	-1	6(-12) + 9(11) + 15(-1) = 12
-1	0	-9	9	-1	6(-9) + 9(9) + 15(-1) = 12
-1	1	-6	7	-1	6(-6) + 9(7) + 15(-1) = 12
0	-1	-7	6	0	6(-7) + 9(6) + 15(0) = 12
0	0	-4	4	0	6(-4) + 9(4) + 15(0) = 12
0	1	-1	2	0	6(-1) + 9(2) + 15(0) = 12
1	-1	-2	1	1	6(-2) + 9(1) + 15(1) = 12
1	0	1	-1	1	6(1) + 9(-1) + 15(1) = 12
1	1	4	-3	1	6(4) + 9(-3) + 15(1) = 12