La Ecuación $xa + yb = c$

Alan Reyes-Figueroa
Teoría de Números

(Aula 06) 19.julio.2024

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 $a(x' - x_0) = b(y_0 - y')$.

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

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

La ecuación $xa + yb = c$

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) $33x + 14y = 115.$