Identidad de Bézout

Joaquin Nuñez

December 22, 2024

1 Identidad de Bezout

Sean $a, b \in \mathbb{Z}$ no ambos nulos y sea $d = (a : b)$. Entonces, $\exists\ x, y \in \mathbb{Z}$ tal que $d = ax + by$.

2 Demostración

Consideremos el siguiente conjunto S

$$S = \{xa + yb : x, y \in \mathbb{Z},\ xa + by > 0\}$$

Notemos que como alguno de los números $a, -a, b, -b$ es positivo, tenemos que ese número pertenece a S. Pues, por ejemplo, si a es positivo, eligiendo $x = 1$ e $y = 0$, tenemos que $xa + by > 0$ con $x, y \in \mathbb{Z}$. De este modo, S es un conjunto no vacio. Luego, como S es un subconjunto no vacio de $\mathbb{N}$, sabemos que tiene un elemento mínimo. Sea d el elemento mínimo de S. Como $d \in S$, $\exists\ x, y \in \mathbb{Z}$ tales que $d = xa + yb$

Sean ahora q y r el cociente y resto de la división de a por d, es decir, $a = qd + r$ con $0 \leq r < d$. Si $r \neq 0$ tenemos que $r \in S$, pues

$$r = a - qd = a - q(xa + yb) = (1 - qx)a + (-qy)b$$

en donde $1 - qx$ y $-qy$ son números enteros. Pero esto es una contradicción, pues dijimos que d era el mínimo pero $r < d$. Luego $r = 0$, con lo que $d \mid a$

Sean ahora q' y r' el cociente y resto de la división de b por d, es decir, $b = q'd + r'$ con $0 \leq r' < d$. Si $r' \neq 0$ tenemos que $r \in S$, pues

$$r = b - q'd = b - q'(xa + yb) = (-q'x)a + (1 - q'y)b$$

en donde $1 - q'y$ y $-q'x$ son números enteros. Pero esto es una contradicción, pues dijimos que d era el mínimo pero $r' < d$. Luego $r' = 0$, con lo que $d \mid b$

Así, tenemos que d es un divisor común de a y b. Falta ver que es el mayor de entre todos los divisores comunes.

Sea ahora e un divisor común cualquiera de a y b. Entonces, tenemos que

$$\begin{cases} e \mid a \\ e \mid b \end{cases} \Rightarrow \begin{cases} e \mid xa \\ e \mid yb \end{cases} \Rightarrow e \mid xa + yb = d$$

Luego, como $d \neq 0$, tenemos que $e \leq d$. Esto quiere decir que cualquier divisor común de a y b es menor o igual que d, lo cual nos dice que d es el mayor de los divisores comunes, con lo que $d = (a : b)$, con lo que $\exists\ x, y \in \mathbb{Z}$ tal que $d = ax + by$ Así, queda demostrada la identidad de Bezout. $\square$

3 Referencias

1. Mariano Suárez-Álvarez. Notas de Álgebra. 2021.