2019-09-23

Identidad de Bézout

"Dados $a, b \in \mathbb{Z}^+$, existen $x, y \in \mathbb{Z}$ tales que:

$$mcd(a,b) = ax + by"$$

Ej: Sabemos $mcd(5,3) = 1$. Por la identidad de Bézout sabemos que existen x, y $\mathbb{Z}$ con:

$$1 = 5x + 3y$$

por ejemplo: $x = -1$; $y = 2$

$1 = 5(-1) + 3(2)$
$1 = 5(-1+3) + 3(2-5)$
$1 = 5(-1) + 5 \cdot 3 + 3 \cdot 2 - 3 \cdot 5$
$1 = 5(-1+6) + 3(2-10)$
$1 = 5 \cdot (1) + \cancel{5 \cdot 6} + 3 \cdot 2 - \cancel{3 \cdot 10}$

$\boxed{!}$
- Bézout dice que existen x, y $\mathbb{Z}$, pero no dice cómo encontrarlos.
- De hecho los numeros x, y $\mathbb{Z}$, no son únicos.

Ej: El algoritmo de euclidés extendido:

$a = 328 \quad b = 500$

Por Bézout, sabemos que existen $x, y \in \mathbb{Z}$ tales que:

- agarramos la última ecuación con residuo

$16 = 12 + 4$
$16 - 12 = 4$

$4 = 500x + 328y$

∴ ¿Cómo encontramos x e y?

$mcd(500, 328)$
$500 = 328 + 172$ (1) (5)
$mcd(328, 172)$
$328 = 172 + 156$ (2) (4)
$mcd(172, 156)$
$172 = 156 + 16$ (3) (3)
$mcd(156, 16)$
$156 = 9 \cdot 16 + 12$ (4) (2)
$mcd(16, 12)$
$16 = 12 + 4$ (5) (1)
$mcd(12, 4)$
$12 = 4 \cdot 3 + 0$
$mcd(4, 0)$

$$\boxed{16 - 1\cdot 12 = 4} \quad (1)$$

master

- De la ecuacion (2) despejo el residuo:

$$156 - 9\cdot 16 = 12 \quad (2)$$

[!] no desarrollar las multiplicaciones

- sustituyo el 12 en (1) y remplazo en la (1)

$$\boxed{16 - (156 - 9\cdot 16) = 4}$$

master

De la ecuación (3) despejamos : $16 = 172 - 156$ sustituimos en master:

$$(3)\ 172 - 156 = 16$$

$$16 - 156 + 9\cdot 16 = 4$$

$$10\cdot 16 - 156 = 4$$

$$\boxed{10\underbrace{(172 - 156)}_{(3)} - 156 = 4}$$

master

$$(4)\ 328 - 1\cdot 172 = 156$$

$$(5)\ 500 - 328 = 172$$

$$10(172 - 156) - 156 = 4$$

$$10\cdot 172 - 10\cdot 156 - 156 = 4$$

$$10\cdot 172 - 11\cdot 156 = 4$$

$$10\cdot 172 - 11\underbrace{(328 - 172)}_{(4)} = 4$$

$$10\cdot 172 - 11\cdot 328 + 11\cdot 172 = 4$$

$$21\cdot 172 - 11\cdot 328 = 4$$

$$21\underbrace{(500 - 328)}_{(5)} - 11\cdot 328 = 4$$

$$21\cdot 500 - 21\cdot 328 - 11\cdot 328 = 4$$

$$21\cdot 500 - 32\cdot 328 = 4$$

$$21\cdot \underbrace{500}_{b} - 32\cdot \underbrace{328}_{a} = 4$$

$x = 21$; $y = 32$

es una de las infinitas soluciones

Encontramos las demás soluciones tienen la forma siguiente:

$$x = 21 + \boxed{k_1}$$
$$y = -32 - \boxed{k_2}$$

Los escogemos de forma inteligente

Recordemos:

$$mcd(a,b) \cdot mcm(a \cdot b) = a \cdot b$$

Si escogemos $K_1 = \dfrac{328}{\underbrace{4}_{mcd}}$ $\quad K_2 = \dfrac{500}{\underbrace{4}_{mcd}}$

master $\left[4 = 500 \cdot \left(21 + \frac{328}{4}\right) + 328\left(-32 - \frac{500}{4}\right) \right.$

$$= 500 \cdot 21 + \cancel{\frac{500 \cdot 328}{\underbrace{4}_{mcm(500,328)}}} + 328(-32) - \cancel{\frac{328 \cdot 500}{4}}$$

$$= 500 \cdot 21 + 328(-32)$$

▲ En general una solución tiene la forma para x:

$$x = 21 + \frac{328}{4} \cdot K \qquad K \in \mathbb{Z}$$
$$y = -32 - \frac{500}{4} K$$

En resumen:

- Bézout: $mcd(a,b) = ax + by$
  - Euclides extendido:

    Encuentre soluciones $x = x_0$ & $y = y_0$

  - La solución general: donde $K \in \mathbb{Z}$

$$\boxed{x = x_0 + \frac{b}{mcd(a,b)} \cdot K} \qquad \boxed{y = y_0 - \frac{a}{mcd(a,b)} \cdot K}$$