El algoritmo de Euclides

Sean a y b tales que $a \neq 0$, o bien, $b \neq 0$. El mcd(a,b) se puede calcular:

1. Comience con mcd(a,b) tal que $|a| > |b|$. Si $b = 0$, entonces mcd(a,0) = a.
2. Calculamos el residuo r según el algoritmo de la división de Euclides: $a = q \cdot b + r$, $0 \leq r < b$.
3. Asignamos $a := b$, $b := r$, con esto se sigue cumpliendo que $|a| > |b|$ [recordemos que mcd(a,b)=mcd(b,r)]
4. Repetir los pasos 2 y 3 hasta que $r = 0$.

Entonces el mcd(a,b) será el valor de a al finalizar el algoritmo.

Ejemplo 1. Calcule mcd(24, 54).

Identificamos $a = 54$ & $b = 24$.

Por el algoritmo de la división de Euclides:

$54 = 2 \cdot 24 + 6$ mcd(54, 24) = mcd(24, 6) → $a := 24$ & $b := 6$
$24 = 4 \cdot 6 + 0$ mcd(24,6) = mcd(6,0) = 6

∴ mcd(54, 24) = 6

Ejemplo 2. Calcule mcd(131, 24)

Identificamos $a = 131$ & $b = 24$.

Por el algoritmo de la división de Euclides:

$131 = 5 \cdot 24 + 11$
$24 = 2 \cdot 11 + 2$
$11 = 5 \cdot 2 + 1$
$2 = 2 \cdot 1 + 0$

∴ mcd(131, 24) = 1

⚠️ El hecho que mcd(131,24) = 1 nos indica que ambos números no tienen factores primos en común.

Definición. Sean a y b enteros, tales que mcd(a, b) = 1. Entonces decimos que a y b son **primos relativos** o **coprimos**.

👨‍🏫 Al momento de programar una implementación de este algoritmo se recomienda almacenar todos los valores de q y r que se producen.

La identidad de Bézout (Étienne Bézout, siglo XVIII)

La identidad de Bézout establece que si a y b son enteros diferentes de cero, entonces existen enteros x & y tales que:

$$\text{mcd}(a,b) = ax + by$$

MAC

Ejemplo 3. Encuentre $x,y \in \mathbb{Z}$ tales que $\text{mcd}(131, 24) = 131x + 24y$

Identificamos $a = 131$ & $b = 24$.

Por el algoritmo de la división de Euclides:

$131 = 5\cdot 24 + 11$
$24 = 2\cdot 11 + 2$
$11 = 5\cdot 2 + 1$
$2 = 2\cdot 1 + 0$

$\therefore$ mcd(131, 24) = 1

Para encontrar los valores de x & y realizamos lo siguiente:

Primero, de la penúltima ecuación despejamos el residuo [mcd(131, 24)]:
$11 = 5\cdot 2 + 1 \rightarrow 1 = 11 - 5\cdot 2$

Luego, de la ecuación anterior despejamos el residuo y lo sustituimos:
$24 = 2\cdot 11 + 2 \rightarrow 2 = 24 - 2\cdot 11 \rightarrow 1 = 11 - 5\cdot(24 - 2\cdot 11) = 11 - 5\cdot 24 + 10\cdot 11 \rightarrow 1 = 11\cdot 11 - 5\cdot 24$

$11 + 10\cdot 11 = 11(1 + 10) = 11\cdot 11$

Finalmente, de la primera ecuación despejamos el residuo y lo sustituimos:
$11 = 131 - 5\cdot 24 \rightarrow 1 = 11(131 - 5\cdot 24) - 5\cdot 24 = 11\cdot 131 - 55\cdot 24 - 5\cdot 24 \rightarrow 1 = 131\cdot 11 - 24\cdot 60$

En conclusión los valores $x = 11$ & $y = -60$ satisfacen la ecuación $1 = 131x + 24y$.

Ejercicio 4. Encuentre x & y tales que $52x + 97y = \text{mcd}(97,52)$.

Calculamos el mcd(97,52):

i) $97 = 1\cdot 52 + 45$
ii) $52 = 1\cdot 45 + 7$
iii) $45 = 6\cdot 7 + 3$
iv) $7 = 2\cdot 3 + 1$
v) $3 = 3\cdot 1 + 0$

$\therefore$ mcd(97,52) = 1

Despejamos r de *iv)*:

$1 = 7 - 2\cdot 3$ [$3 = 45 - 6\cdot 7$, despejando r de *iii)*]

$= 7 - 2\cdot(45 - 6\cdot 7) = 13\cdot 7 - 2\cdot 45$ [$7 = 52 - 1\cdot 45$, despejando r de *ii)*]

$= 13\cdot(52 - 1\cdot 45) - 2\cdot 45 = 13\cdot 52 - 15\cdot 45$ [$45 = 97 - 1\cdot 52$, despejando r de *i)*]

$= 13\cdot 52 - 15\cdot(97 - 1\cdot 52) = 28\cdot 52 - 15\cdot 97$

En conclusión, los valores de x & y que satisfacen $52x + 97y = \text{mcd}(97,52)$ son $x = 28$ & $y = -15$.