

Divisibilidad - Algoritmo de Euclides

Algoritmo de Euclides

Como corolario de las propiedades anteriores tenemos que:

$$\forall a \in \mathbb{N}, \forall b \in \mathbb{N}^* : x \mid a \wedge x \mid b \Leftrightarrow x \mid b \wedge x \mid (a \bmod b)$$

Por lo tanto, *los divisores comunes entre el dividendo y el divisor son los mismos que entre el divisor y el resto*, esto es:

$$D(a) \cap D(b) = D(b) \cap D(a \bmod b).$$

El *Algoritmo de Euclides* consiste en aplicar la propiedad anterior a divisiones sucesivas hasta obtener resto 0, y el último resto no nulo será el Máximo Común Divisor.

Ejemplo:

Aplicando el Algoritmo de Euclides, calcular $\text{MCD}(756, 525)$:

Algoritmo

entrada (a,b)

funcion $\text{MCD}(a,b)$:

 mientras b sea diferente de 0:

 asignar al par (a,b) el par (b,a mod b)

salida a

Algoritmo recursivo

entrada (a,b)

funcion $\text{MCD}(a,b)$:

 Si (b=0) salida a

 sino salida $\text{MCD}(b,a \bmod b)$