MCD y MCM

Maximo Comun Divisor

- Notación
  - mcd(a, b)
  - (a, b)
- Definicion
  - Un entero positivo d es mcd(a,b) si
    - $d|a \wedge d|b$ — d es un común divisor de a y b
    - $c|a \wedge c|b \Rightarrow c|d$ — Cualquier divisor comun de a y b tambien es divisor de d
- Propiedades
  - Solo puede existir un mcd para cada par de enteros
  - $(a,b) = sa + tb$ — $s, t \in \mathbb{Z}$
  - $(a,b) = 1 \;\Rightarrow\;$ a y b son coprimos
  - a, b coprimos $\;\Leftrightarrow\; 1 = sa + tb$
  - $a, b \in \mathbb{Z} \wedge a \neq 0$
    - $mcd(a,b) = mcd(b,a) = mcd(\pm a, \pm b)$
    - $a > 0$
      - $mcd(a,0) = a$
      - $mcd(a,a) = a$
    - $mcd(1,b) = 1$
  - $a \neq 0 \wedge b \in \mathbb{Z}$ — $mcd(a,b) = mcd(a, b-a)$
  - $a = bq + r \;\Rightarrow\; mcd(a,b) = mcd(b,r)$

$174 = 72 \cdot 2 + 30,$	entonces	$(174, 72) = (72, 30)$
$72 = 30 \cdot 2 + 12,$	entonces	$(72, 30) = (30, 12)$
$30 = 12 \cdot 2 + 6,$	entonces	$(30, 12) = (12, 6)$
$12 = 6 \cdot 2 + 0,$	entonces	$(12, 6) = (6, 0) = 6.$

- Algoritmo de Euclides
  - Definimos
    - $r_0 = a,\; r_1 = b$
    - $(e_i)\;\; r_{i-1} = r_i q_i + r_{i+1}$
    - $(e_k)\;\; r_{k-1} = r_k q_k + 0$
    - $r_k = mcd(a,b)$
    - El proceso de detiene en el primer — $r_i = 0$

Minimo Comun Multiplo

- Definicion
  - Un entero positivo d es mcm(a,b) si
    - $a|m \wedge b|m$ — m es multiplo comun de a y b
    - $a|n \wedge b|n \Rightarrow m|n$ — Cualquier otro multiplo de a y b también debe ser multiplo de m
- Propiedades
  - $mcm(a,b) = \dfrac{ab}{mcd(a,b)}$
  - a,b coprimos $\;\Rightarrow\; mcm(a,b) = ab$