Teorema: Igualdad de Bezout

Sean $a, b \in \mathbb{Z}$, con $a, b \neq 0$. Entonces:

1) $mcd(a,b) = \min\{s>0 : s = ax+by \text{ par algún } x,y \in \mathbb{Z}\}$

2) En particular $\exists x,y \in \mathbb{Z} : mcd(a,b) = ax+by$

Corolario: Sean $a,b \in \mathbb{Z}$ no nulos

1) Si $k \in \mathbb{Z}$, $k|a$ y $k|b \Rightarrow k \mid mcd(a,b)$

2) Si $n \in \mathbb{Z} \Rightarrow mcd(na,nb) = |n|\, mcd(a,b)$

3) $mcd(a,b) = 1 \leftrightarrow \exists x,y \in \mathbb{Z} : ax+by = 1$

4) Sea $d \in \mathbb{Z}^+ : a = d.a^*$ y $b = d.b^*$ con $a^*, b^* \in \mathbb{Z}$
Entonces $d = mcd(a,b) \leftrightarrow mcd(a^*, b^*) = 1$ *

* A los enteros a^* y b^* con $\begin{cases} a = mcd(a,b).a^* \\ b = mcd(a,b).b^* \end{cases}$

Se les llama cofactores de a y b.

Lema: Sean $a,b,c \in \mathbb{Z}$ con $mcd(a,b) = 1$

Si $a|bc \Rightarrow a|c$

(lema de Euclides)

Propiedades de coprimos

1) Si $k|a$ y $k|b$
$k = mcd(a,b) \leftrightarrow mcd(a/k, b/k)$

2) Sean $a,b,c \in \mathbb{Z} : a|c$ y $b|c$
Si a y b son coprimos
$\Rightarrow ab|c$

3) Si p es primo y $p|ab$
$\Rightarrow p|a$ o $p|b$

Obs: Sea $p \in \mathbb{N}$, $p \neq 1$ que cumple que si $p|bc \Rightarrow p|b$ o $p|c$
Luego p es primo

4) Sea p un entero primo y $a_1, \dots, a_n$ enteros: $p|a_1 \dots a_n \Rightarrow p|a_i$ para algún $i \in \{1 \dots n\}$

Mínimo común múltiplo

Dados $a,b \in \mathbb{Z}$ no nulos, definimos el $mcm(a,b)$ como:

$mcm(a,b) = \min\{x \in \mathbb{Z}^+ : a|x \text{ y } b|x\}$

Proposición: Dados $a,b \in \mathbb{Z}$, no nulos, se cumple

$$mcm(a,b) = \frac{|ab|}{mcd(a,b)}$$

Propiedades:

1) $a \mid mcm(a,b)$ y $b \mid mcm(a,b)$

2) $mcd(a,b) \mid mcm(a,b)$