08-03

Práctico 2: Máximo Común Divisor y Mínimo Común Múltiplo.

$mcd(a,b) = max\{x \in \mathbb{Z}^+ : x|a \text{ y } x|b\}$ $\quad mcd(0,0)=0$

Ppdes: $mcd(1,a) = 1$

$mcd(0,b) = b$

$mcd(a,b) = mcd(|a|,|b|)$

Ppd: $mcd(a,b) = mcd(b, a-bx)$

$\Rightarrow mcd(a,b) = mcd(b, a-bq) = mcd(b,r) \ldots$

Fundamental!!

$\boxed{\text{Id. Bezout: } mcd(a,b) = min\{ax+by \quad x,y \in \mathbb{Z}\}}$

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

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

Ejercicio 1. Sean $a, b, c \in \mathbb{N}$. Probar las siguientes afirmaciones

a. $mcd(ca, cb) = c\, mcd(a, b)$.

b. Si $c|a$ y $c|b$ entonces

$$mcd(a/c, b/c) = mcd(a, b)/c.$$

c. $mcd(b, a + bc) = mcd(a, b)$.

d. Si a es par y b impar entonces

$$mcd(a, b) = mcd(a/2, b).$$

e. $mcd(a, b) = mcd(a - b, b)$

f. Si a, b son primos entre sí entonces

$$mcd(a - b, a + b) = 1 \text{ o } 2.$$

(a) $d = mcd(ca, cb)$ $\quad$ Tenemos que ver que $cd' = d$

$d' = mcd(a, b)$

$cd' \leq d$

$d'|a \rightarrow c \cdot d' | ca \Rightarrow c \cdot d' \in \{x \in \mathbb{Z}^+ : x|ca, x|cb\}$

$d'|b \qquad cd' | cb \qquad \Rightarrow cd' \leq mcd(ca, cb) = d$

$d \leq cd'$: Bezout: $mcd(a,b) = inf\{s>0 : s = ax+by, \ x,y \in \mathbb{Z}\}$

$mcd(ca,cb) = inf\{s>0 : s = c \cdot ax + cby, \ x,y \in \mathbb{Z}\}$

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

$c \cdot mcd(a,b) = c \cdot ax + c \cdot by \in \{s>0 : s = cax + cby\}$

$\geq inf\{cax + cby\} = mcd(ca, cb)$

(b) Si $c|a$ y $c|b \Rightarrow mcd\left(\frac{a}{c}, \frac{b}{c}\right) = \frac{mcd(a,b)}{c}$

$\frac{a}{c}, \frac{b}{c} \in \mathbb{Z}$, por la parte anterior: $mcd\left(\frac{a}{c}, \frac{b}{c}\right) = d$

$mcd\left(c \cdot \frac{a}{c}, c \cdot \frac{b}{c}\right) = c \cdot d$

Observar que no podemos usar directamente el ejercicio previo pues $\frac{1}{c} \notin \mathbb{Z}$. Es necesario que $c|a$ y $c|b$.

$mcd(a,b) = c \cdot d$

$\Rightarrow \frac{mcd(a,b)}{c} = \frac{cd}{c} = d.$

(c) $mcd(b, a+bc) = mcd(a,b) \quad \forall c \in \mathbb{Z}^+$

$d = mcd(a,b)$ Queremos ver que $d = d'$.

$d' = mcd(b, a+bc)$

$\begin{cases} d|a \\ d|b \end{cases} \Rightarrow \begin{cases} d|ax \\ d|by \end{cases} \Rightarrow d|ax+by \quad \forall x,y$

En particular podemos tomar $\Rightarrow x=1, y=c$, luego $\begin{cases} d|a+bc \\ d|b \end{cases}$

Entonces $d \leq máx\{D: D|a+bc \text{ y } D|b\} = mcd(b, a+bc) = d'$

$\begin{cases} d'|b \\ d'|a+bc \end{cases} \Rightarrow \begin{cases} d'|bc \\ d'|a+bc \end{cases} \Rightarrow \begin{cases} d'|a+c-bc = a \\ d'|b \end{cases}$

Como antes $d' \leq mcd(a,b) = d$

Ejercicio 2. Sean $a, b, c \in \mathbb{N}$ tales que a y b son primos entre sí. Probar o dar contraejemplos que

a. Si $a|(bc)$ entonces $a|c$.

b. Si $a|c$ y $b|c$ entonces $ab|c$.

c. ¿Valen las partes anteriores si $\mathrm{mcd}(a,b) \neq 1$?

(a) Id Bezout: $\mathrm{mcd}(a,b) = \min\{s>0 : s = ax+by\}$)

$\mathrm{mcd}(a,b)=1 \Rightarrow \exists\, x,y \in \mathbb{Z} \quad 1 = ax+by$

Sabemos que $a|bc$, queremos ver que $a|c$

Ejemplo:

$\mathrm{mcd}(2,5)=1$

$2 | 5\cdot 4 = 20 \Rightarrow 2|4$

Multiplicando por c en la Id. Bezout tenemos que

$c = a\cdot cx + bcy$ como $a|bc$

$c = a\left(cx + \frac{bc}{a}y\right)$ donde $cx + \underbrace{\frac{bc}{a}}_{\in\mathbb{Z}} \cdot y \in \mathbb{Z}$

$c = a\cdot q$ con $q \in \mathbb{Z}$, es decir $a|c$

(b) $\mathrm{mcd}(a,b)=1$ y $a|c$, $b|c \rightarrow ab|c$

$\exists x,y,\ 1 = ax+b$, multiplicando por c: $\boxed{c = acx + bcy}$,

Queremos $c = ab\cdot q$

Obs: $a|c \Rightarrow \boxed{c=am}$

$b|c \Rightarrow \boxed{c=bn}$

Sustituimos c: $c = abnx + bamy$

$= ab(nx+my)$

$\Rightarrow ab|c$.

(c) $3|18$ $\quad 3\cdot 9 \nmid 18$

$9|18$

$2|12$ pero $8 \nmid 12$

$4|12$