Ejercicio 5. [Cofactores.] Sean $a, b \in \mathbb{Z}$ no nulos.

a. Probar que $d = \text{mcd}(a, b)$, si y sólo si, existen $a^*, b^* \in \mathbb{Z}$, coprimos, tales que: $a = da^*$ y $b = db^*$. Los enteros a^* y b^* se denominan cofactores de a y b. Sugerencia: usar Bezout.

b. Hallar los cofactores de $a = 63$ y $b = 15$.

c. Probar que si a es par y b impar entonces: $\text{mcd}(a, b) = \text{mcd}(a/2, b)$. Sugerencia: usar cofactores.

a) $d = \text{mcd}(a,b) \iff$ existen $\underbrace{a^* \text{ y } b^*}_{\text{cofactores de } a \text{ y } b}$ coprimos tales que $a = da^*$ y $b = db^*$

($\Rightarrow$) $d = \text{mcd}(a,b) \Rightarrow \begin{cases} d \mid a \\ d \mid b \end{cases}$

entonces existen a^* y b^* tales que $a = da^*$ y $b = db^*$ $(a^*, b^* \in \mathbb{Z})$

nos falta ver que a^* y b^* son coprimos

por la igualdad de Bezout, como $d = \text{mcd}(a,b)$ tenemos

$$d = ax + by \quad \text{para algunos } x, y \in \mathbb{Z}$$

$$d = da^*x + db^*y$$

$$d = d(a^*x + b^*y)$$

$$1 = a^*x + b^*y$$

entonces $\text{mcd}(a^*, b^*) = 1$, es decir a^* y b^* son coprimos

teorema de Bézout:

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

$d = \text{mcd}(a,b)$

$$a = da^* \quad \text{y} \quad b = db^*$$

suponemos que $a^* = qn$ y $b^* = q'n$

$\Rightarrow a = da^* = \underline{dn}q$ y $b = db^* = \underline{dn}q'$

$dn \mid a$ y $dn \mid b$

esto contradice que $d = \text{mcd}(a,b)$

($\Leftarrow$) tenemos que $a = da^*$ y $b = db^*$ donde $\underbrace{a^* \text{ y } b^* \text{ son coprimos}}_{\text{mcd}(a^*, b^*) = 1}$

queremos probar que $\text{mcd}(a,b) = d$

$$\operatorname{mcd}(a,b) = \operatorname{mcd}(da^*, db^*) = d\,\underbrace{\operatorname{mcd}(a^*, b^*)}_{=1} = d$$

$$\operatorname{mcd}(dc, de) = d\operatorname{mcd}(c,e)$$

b. Hallar los cofactores de $a = 63$ y $b = 15$.

c. Probar que si a es par y b impar entonces: $\operatorname{mcd}(a,b) = \operatorname{mcd}(a/2, b)$. Sugerencia: usar cofactores.

b) cofactores de $a = 63$ y $b = 15$

$\operatorname{mcd}(63, 15) = ?$

$63 = 15 \cdot 4 + 3 \longrightarrow \operatorname{mcd}(63,15) = \operatorname{mcd}(15,3)$

$15 = 3 \cdot 5 + 0 \longrightarrow \operatorname{mcd}(15,3) = \operatorname{mcd}(3,0) = 3$

entonces $\operatorname{mcd}(63,15) = 3$

$\underset{a}{\underset{\uparrow}{63}} = \underset{\operatorname{mcd}(a,b)}{\underset{\uparrow}{3}} \cdot 21 \longrightarrow a^* = 21$

$\underset{b}{\underset{\uparrow}{15}} = \underset{\operatorname{mcd}(a,b)}{\underset{\uparrow}{3}} \cdot 5 \longrightarrow b^* = 5$

c) Queremos probar que

si a es par y b es impar $\Rightarrow \operatorname{mcd}(a,b) = \operatorname{mcd}(a/2, b)$

Sea $d = \operatorname{mcd}(a,b)$

[queremos probar que $d = \operatorname{mcd}(a/2, b)$

buscamos

$a/2 = dq$ y $b = dq'$

con q y q' coprimos]

Como $d = \operatorname{mcd}(a,b)$ existen a^* y b^* coprimos tales que $\begin{cases} a = da^* \\ b = db^* \end{cases}$

b es impar $\Rightarrow$ d es impar y b^* es impar

$$\left.\begin{array}{l} d \text{ impar} \\ a = da^* \\ a \text{ par} \end{array}\right\} \Rightarrow a^* \text{ es par} \Rightarrow \frac{a^*}{2} \in \mathbb{Z}$$

$$\left.\begin{array}{l} a = da^* \\ a \text{ par} \\ a^* \text{ par} \end{array}\right\} \Rightarrow \frac{a}{2} = d\,\frac{a^*}{2}$$

entonces tenemos $\frac{a}{2} = d\,\frac{a^*}{2}$ y $b = db^*$

vamos a ver que $mcd\left(\frac{a^*}{2}, b^*\right) = 1$

$$\left.\begin{array}{l} Div_+(a^*) \cap Div_+(b^*) = \{1\} \\ \{1\} \subset Div_+\left(\frac{a^*}{2}\right) \subseteq Div_+(a^*) \end{array}\right] \; Div_+\left(\frac{a^*}{2}\right) \cap Div_+(b^*) = \{1\}$$

otra forma de ver que $mcd\left(\frac{a^*}{2}, b^*\right) = 1$

$$mcd(a^*, b^*) = 1 \Rightarrow 1 = a^*x + b^*y \text{ con } x, y \in \mathbb{Z}$$

$$\Rightarrow 1 = \frac{a^*}{2} 2x + b^*y \text{ con } x, y \in \mathbb{Z}$$

$$\Rightarrow mcd\left(\frac{a^*}{2}, b\right) = 1$$

En conclusión tenemos:

$$\left.\begin{array}{l} \frac{a}{2} = d\,\frac{a^*}{2} \\ b = db^* \\ \frac{a^*}{2} \text{ y } b^* \text{ son coprimos} \end{array}\right] \Rightarrow d = mcd\left(\frac{a}{2}, b\right)$$

Ejercicio 6. En cada caso, hallar $a, b \in \mathbb{N}$ que verifiquen las condiciones dadas.

a. $ab = 22275$ y $\mathrm{mcd}(a,b) = 15$. Sugerencia: usar cofactores y factorizar en producto de primos.

b. $ab = 1008$ y $\mathrm{mcm}(a,b) = 168$. Recordar que: $\mathrm{mcm}(a,b) \cdot \mathrm{mcd}(a,b) = |a||b|$, $\forall\, a, b \in \mathbb{Z}$.

c. $a + b = 1271$ y $\mathrm{mcm}(a,b) = 330 \cdot \mathrm{mcd}(a,b)$.

d. $a + b = 122$ y $\mathrm{mcd}(a,b) + \mathrm{mcm}(a,b) = 1802$.

a) buscamos $a, b \in \mathbb{N}$ tales que $\begin{cases} ab = 22275 \\ \mathrm{mcd}(a,b) = 15 \end{cases}$

como $\mathrm{mcd}(a,b) = 15$ existen a^* y b^* coprimos tales que

$$\begin{cases} a = 15a^* \\ b = 15b^* \end{cases}$$

$22275 = ab = 15a^* \, 15b^* = 15^2 a^* b^*$

entonces $a^* b^* = 99$

Divisores de 99: $99 \cdot 1 = 99$

$33 \cdot 3 = 99 \leftarrow$ no sirve porque 33 y 3 no son coprimos

$11 \cdot 9 = 99$

(1) $a^* = 99$ y $b^* = 1$

$\Rightarrow \begin{cases} a = 15a^* = 1485 \\ b = 15b^* = 15 \end{cases}$

(2) $a^* = 1$ y $b^* = 99$

$\Rightarrow \begin{cases} a = 15 \\ b = 1485 \end{cases}$

(3) $a^* = 11$ y $b^* = 9$

$\Rightarrow \begin{cases} a = 15 \cdot 11 = 165 \\ b = 15 \cdot 9 = 135 \end{cases}$

(4) $b^* = 11$ y $a^* = 9$

$\Rightarrow \begin{cases} a = 135 \\ b = 165 \end{cases}$

b) buscamos $a, b \in \mathbb{N}$ tq $\begin{cases} ab = 1008 \\ \mathrm{mcm}(a,b) = 168 \end{cases}$

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

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

$$168 = \frac{1008}{mcd(a,b)} \Rightarrow mcd(a,b) = \frac{1008}{168} = 6$$

$d = mcd(a,b) = 6$

entonces existe a^* y b^* coprimos tales que

$$a = 6a^* \quad y \quad b = 6b^*$$

$1008 = ab = 6a^* 6b^* = 6^2 a^* b^*$

$\Rightarrow a^* b^* = 28$

Divisores de 28: $28 \cdot 1 = 28$

$14 \cdot 2 = 28$ $\qquad 28 = \underbrace{2 \cdot 2}\cdot\underbrace{7}$

$7 \cdot 4 = 28$

este no sirve porque no son coprimos.

(1) $a^* = 7$ y $b^* = 4$

$$\Rightarrow \begin{cases} a = 6 \cdot 7 = 42 \\ b = 6 \cdot 4 = 24 \end{cases}$$

(2) $a^* = 4$ y $b^* = 7$

$$\Rightarrow \begin{cases} a = 24 \\ b = 42 \end{cases}$$

(3) $a^* = 28$ y $b^* = 1$

$$\Rightarrow \begin{cases} a = 6 \cdot 28 = 168 \\ b = 6 \end{cases}$$

(4) $a^* = 1$ y $b^* = 28$

$$\Rightarrow \begin{cases} a = 6 \\ b = 168 \end{cases}$$