Ejercicio 4. [Bezout] Sean $a, b, c \in \mathbb{N}$. Probar las siguientes afirmaciones:

a. $\mathrm{mcd}(ca, cb) = c\,\mathrm{mcd}(a, b)$. Sugerencia: usar Bezout y probar la doble desigualdad.

b. Si $c|a$ y $c|b$ entonces: $\mathrm{mcd}(a/c, b/c) = \mathrm{mcd}(a, b)/c$.

c. Si a y b son primos entre sí, entonces: $\mathrm{mcd}(a-b, a+b) = 1$ o 2. Sugerencia: probar primero que $\mathrm{mcd}(a-b, a+b)$ divide a $\mathrm{mcd}(2a, 2b)$.

a) $\mathrm{mcd}(ca, cb) = c\,\mathrm{mcd}(a,b)$

c) a y b coprimos

queremos ver que $\mathrm{mcd}(a-b, a+b) = 1$ o 2

Afirmación: $\mathrm{mcd}(a-b, a+b) \mid \mathrm{mcd}(2a, 2b)$

$d = \mathrm{mcd}(a-b, a+b)$

para ver que $d \mid \mathrm{mcd}(2a, 2b)$ alcanza con probar que $d \mid 2a$ y $d \mid 2b$

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

$$\Rightarrow \begin{cases} d \mid \overbrace{(a-b)+(a+b)}^{2a} \\ d \mid \underbrace{(a+b)-(a-b)}_{2b} \end{cases}$$

$$\Rightarrow \begin{cases} d \mid 2a \\ d \mid 2b \end{cases}$$

$$\Rightarrow d \mid \mathrm{mcd}(2a, 2b)$$

Tenemos $\begin{cases} * \ a \text{ y } b \text{ coprimos} \\ * \ \mathrm{mcd}(a-b, a+b) \mid \mathrm{mcd}(2a, 2b) \end{cases}$

Queremos probar que $\mathrm{mcd}(a-b, a+b) = 1$ o 2

a y b coprimos $\Rightarrow \mathrm{mcd}(a,b) = 1$

entonces $\mathrm{mcd}(2a, 2b) = 2\,\mathrm{mcd}(a,b) = 2$

entonces $\mathrm{mcd}(a-b, a+b) \mid 2$

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

Ejercicio 6. [Cofactores.] Sean $a, b \in \mathbb{Z}$ no nulos.

a. Probar que $d = \mathrm{mcd}(a, b)$, 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: $\mathrm{mcd}(a, b) = \mathrm{mcd}(a/2, b)$. Sugerencia: usar cofactores.

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

$d = \mathrm{mcd}(a,b) \Rightarrow \begin{cases} d \mid a \rightsquigarrow a = da^* \\ d \mid b \rightsquigarrow b = db^* \end{cases}$ con a^* y b^* coprimos

a) $d = \mathrm{mcd}(a,b) \iff$ existen $a^*, b^* \in \mathbb{Z}$ coprimos tales que $a = da^*$ y $b = db^*$

($\Rightarrow$)

$d = \mathrm{mcd}(a,b) \Rightarrow \begin{cases} d \mid a \\ d \mid b \end{cases} \Rightarrow a = dq$ para algún $q \in \mathbb{Z}$

$\Rightarrow \begin{cases} a = da^* \\ b = db^* \end{cases}$ con $a^*, b^* \in \mathbb{Z}$

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

Forma 1:

$d = \mathrm{mcd}(a,b) = \mathrm{mcd}(da^*, db^*) = d\,\mathrm{mcd}(a^*, b^*)$

$\Rightarrow d = d\,\mathrm{mcd}(a^*, b^*) \Rightarrow 1 = \mathrm{mcd}(a^*, b^*)$

Forma 2:

$d = \mathrm{mcd}(a,b) \Rightarrow d = ax + by$ para algunos $x, y \in \mathbb{Z}$

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

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

$\Rightarrow \mathrm{mcd}(a^*, b^*) = 1$

Bezout: $\mathrm{mcd}(a^*, b^*) = \min\{s > 0 : s = a^*u + b^*v \text{ con } u, v \in \mathbb{Z}\}$

$\longrightarrow \mathrm{mcd}(a^*, b^*) = 1$

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

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

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

$\mcd(a,b) = d \iff a = da^*$ y $b = db^*$ con a^* y b^* coprimos

a^* y b^* son los cofactores de a y b

b) Hallar los cofactores de 63 y 15

$\mcd(63,15) = ?$ $\quad a = 63$ $\quad b = 15$

$63 = 15 \cdot 4 + 3$

$15 = 3 \cdot 5 + 0$

$\mcd(63,15) = \mcd(15,3) = \mcd(3,0) = 3$

$a = 63 = 3 \cdot 21 \longrightarrow a^* = 21$

$b = 15 = 3 \cdot 5 \longrightarrow b^* = 5$

c. Probar que si a es par y b impar entonces: $\mcd(a,b) = \mcd(a/2, b)$.

a es par $\quad a = 6 \rightsquigarrow 3 \text{ y } 2 \quad a/2 = 3 \rightsquigarrow 3$

b es impar $\quad b = 9 \rightsquigarrow 3 \quad b = 9 \rightsquigarrow 3$

$d = \mcd(a,b) \quad \mcd(6,9) = 3 \quad \mcd(3,9) = 3$

queremos ver que $d = \mcd(a/2, b)$

[buscamos $q, q' \in \mathbb{Z}$ coprimos tales que $a/2 = dq$, $b = dq'$]

$d = \mcd(a,b)$

$\Rightarrow$ existen a^* y b^* coprimos tales que $a = da^*$ y $b = db^*$

$a/2 = da^*/2$?

b impar $\Rightarrow$ d impar, $a = da^*$, a es par $\Rightarrow a^*$ es par $\Rightarrow \frac{a^*}{2} \in \mathbb{Z}$

Entonces tenemos $\frac{a}{2} = d\underbrace{\frac{a^*}{2}}_{\in \mathbb{Z}}$ y $b = d\underbrace{b^*}_{\in \mathbb{Z}}$

Falta ver que $\frac{a^*}{2}$ y b^* son coprimos:

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

$\Rightarrow 1 = \frac{a^*}{2} 2x + b^* y$

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

$1 = \frac{a^*}{2} \underbrace{x'}_{\in \mathbb{Z}} + b^* \underbrace{y}_{\in \mathbb{Z}}$

$$\left.\begin{array}{l} \frac{a}{2} = d\frac{a^*}{2} \\ b = db^* \\ \mcd(\frac{a^*}{2}, b^*) = 1 \end{array}\right\} \Rightarrow \mcd(\tfrac{a}{2}, b) = d$$

Ejercicio 7

Buscamos $a, b \in \mathbb{N}$ tales que

a. $ab = 22275$ y $\mcd(a, b) = 15$.

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

Como $\mcd(a,b) = 15$ existen $a^*, b^* \in \mathbb{Z}$ coprimos tales que

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

$ab = 15a^* \cdot 15b^* = 15^2 a^* b^*$

$\Rightarrow 22275 = 15^2 a^* b^*$

$\Rightarrow a^* b^* = \frac{22275}{15^2} = 99$

$\Rightarrow \boxed{a^* b^* = 99}$

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

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

$99 = 11 \cdot 9$

① $a^2 = 99$, $b^2 = 1$

$a = 15 \cdot 99 = 1485$

$b = 15 \cdot 1 = 15$

② $a^2 = 1$, $b^2 = 99$

③ $a^2 = 11$, $b^2 = 9$

$a = 15 \cdot 11 = 165$

$b = 15 \cdot 9 = 135$

④ $a^2 = 9$, $b^2 = 11$

$n(n+1)(n+2)$

Probar que $n(2n+1)(7n+1)$ es divisible entre 6 para todo $n \in \mathbb{N}$.

* $n(2n+1)(7n+1)$ es divisible entre 2

① n es par $\rightsquigarrow n = 2q$

$n(2n+1)(7n+1) = 2q(2 \cdot 2q+1)(7 \cdot 2q+1)$ es divisible entre 2

② n es impar $\rightsquigarrow n = 2q+1$

$7n+1 = 7(2q+1)+1 = 14q+7+1 = 14q+8$

$\Rightarrow 2 \mid 7n+1$

$\Rightarrow 7n+1 = 2Q$

$n(2n+1)(7n+1) = n(2n+1) \cdot 2Q = 2n(2n+1)Q$ ✓

$\Rightarrow 2 \mid n(2n+1)(7n+1)$

* $n(2n+1)(7n+1)$ es divisible entre 3

① $n = 3q$

$n(2n+1)(7n+1) = 3q(2 \cdot 3q+1)(7 \cdot 3q+1)$ ✓

$3 \mid n(2n+1)(7n+1)$

② $n = 3q+1$

$2n+1 = 2(3q+1)+1 = 6q+2+1 = 6q+3 = 3(2q+1)$

$\Rightarrow 3 \mid 2n+1$

$\Rightarrow 3 \mid n(2n+1)(7n+1)$

(3) $n = 3q + 2$

$$7n + 1 = 7(3q+2) + 1 = 3 \cdot 7q + 14 + 1 = 3 \cdot 7q + 15 = 3(7q + 5)$$

$\Rightarrow 3 \mid 7n+1$

$\Rightarrow 3 \mid n(2n+1)(7n+1)$