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

Ideas: - Bézout
- usar directamente la definición.

Teo. de Bézout

dados $a, b \in \mathbb{Z}$, $\exists\, x, y \in \mathbb{Z}$ tales que

$\circledast$ $mcd(a,b) = x \cdot a + y \cdot b$

Por otra parte: $a + bc = 1 \cdot a + c \cdot b$

El teo. de Bézout es "una especie de recíproco" de lo siguiente

$\forall\, x, y \in \mathbb{Z} \quad mcd(a,b) \mid (x \cdot a + y \cdot b)$

$\mathrm{mcd}(a,b) \mid a \quad , \quad \mathrm{mcd}(a,b) \mid b$

$\Rightarrow \mathrm{mcd}(a,b) \mid x \cdot a + y \cdot b \quad \forall x, y \in \mathbb{Z}$

o sea cualquier combinación lineal de coefs. enteros

$a+bc$ es una comb. lin. de a y b.

$\Rightarrow \mathrm{mcd}(a,b) \mid a+bc$

Por definición, $\mathrm{mcd}(a,b) \mid b$

$\Rightarrow$ $\mathrm{mcd}(a,b)$ es un divisor común de b y $a+bc$

como $\mathrm{mcd}(b, a+bc)$ es el máximo de los divisores comunes de b y $a+bc$ $\Rightarrow$ $\mathrm{mcd}(a,b) \leq \mathrm{mcd}(b, a+bc)$

Ej: $a = 20$, $b = 12$

(observando el teorema en un ejemplo)

$c = -2$

$$a + bc = 20 + 12(-2) = 20 - 24 = -4$$

$$\operatorname{mcd}(12, -4) = \boxed{4}$$

$\operatorname{mcd}(a,b) \leq \operatorname{mcd}(b, a+bc)$

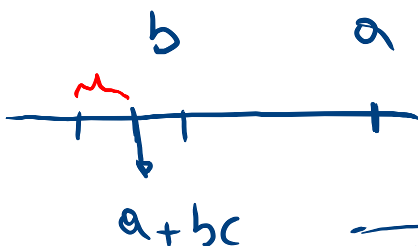
$4 \cdot 5 \quad 4 \cdot 3$

$$\operatorname{mcd}(20, 12) = \boxed{4}$$

(hacer el alg. de Euclides)

. . . .

(paréntesis)



c negativo

a, b

graficar (dibujar en un eje)

$x \cdot a + y \cdot b$

$x, y \in [-10, 10]$

Ya tenemos que $mcd(a,b) \leq mcd(b, a+bc)$

Faltaría probar que $mcd(b, a+bc) \leq mcd(a,b)$

Si tratamos de hacerlo como recién,

podemos probar si $mcd(b, a+bc) \mid b$ (obvio)

si $mcd(b, a+bc) \mid a$

Alcanza con escribir a como combinación lineal de b y $a+bc$

$a = a + bc - bc = (a+bc) + (-c)b$

$\Rightarrow mcd(b, a+bc) \mid a$

Entonces $\text{mcd}(b, a+bc)$ es un divisor común de a y b

$\Rightarrow \underbrace{\text{mcd}(a,b)}_{\text{máximo}} \geq \text{mcd}(b, a+bc)$

Probamos una desigualdad y su opuesta

$\Rightarrow \text{mcd}(a,b) = \text{mcd}(b, a+bc)$

Al final no usamos Bézout, pero usamos el concepto de dividir una comb. lineal, que aparece en el teorema.