

# Matemática Discreta II

Mauro Polenta Mora

## Ejercicio 6

### Consigna

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

1. Probar que  $d = \text{mcd}(a, b)$  si y sólo si existen  $a^*, b^* \in \mathbb{Z}$ , coprimos, tales que:
  - $a = da^*, \quad b = db^*$
  - Los enteros  $a^*$  y  $b^*$  se denominan **cofactores** de  $a$  y  $b$ . *Sugerencia: usar Bezout.*
2. Hallar los cofactores de  $a = 63$  y  $b = 15$ .
3. Probar que si  $a$  es par y  $b$  impar entonces:
  - $\text{mcd}(a, b) = \text{mcd}(\frac{a}{2}, b)$
  - *Sugerencia: usar cofactores.*

## Resolución

### Parte 1

Veamos el siguiente razonamiento:

$$\begin{aligned} d &= \\ &= \text{mcd}(a, b) \\ &= \\ &= \text{mcd}(da^*, db^*) \\ &= (\text{propiedad del ejercicio 4 parte 1}) \\ &= d \cdot \text{mcd}(a^*, b^*) \end{aligned}$$

Entonces necesariamente  $\text{mcd}(a^*, b^*) = 1$  para mantener la igualdad.

**Observación:** Esta es la prueba vista en las notas, pero no demuestra la existencia de los cofactores. Aunque es relativamente intuitivo, en el sentido de que si no tuvieran algún factor coprimo en su descomposición, entonces serían el mismo número.

## Parte 2

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

Hallemos  $\text{mcd}(63, 15)$ :

$$\begin{aligned}\text{mcd}(63, 15) \\ &= \\ \text{mcd}(15, 3) \\ &= \\ \text{mcd}(3, 0) \\ &= \\ 3\end{aligned}$$

Ahora para los cofactores, observemos que:

- $a = 3 \cdot 21 = 63$
- $b = 3 \cdot 5 = 15$

Entonces:

- $a^* = 21$
- $b^* = 5$

Que son coprimos.

## Parte 3

- Probar que si  $a$  es par y  $b$  impar entonces:

- $\text{mcd}(a, b) = \text{mcd}(\frac{a}{2}, b)$
- *Sugerencia: usar cofactores.*

La estrategia será probar las dos desigualdades, por lo que vamos a empezar con eso. Llamamos  $d = \text{mcd}(a, b)$ .

$$d \leq \text{mcd}(\frac{a}{2}, b)$$

Podemos escribir  $a$  de la siguiente forma:

- $a = 2 \cdot \frac{a}{2}$ , además
- $\text{mcd}(2, b) = 1$  pues  $b$  es impar

Entonces podemos usar el lema de Euclides, para concluir que:

- $d \mid \frac{a}{2}$

Entonces  $d \mid \text{mcd}(\frac{a}{2}, b)$ , por lo tanto  $d \leq \text{mcd}(\frac{a}{2}, b)$

$$\text{mcd}(\frac{a}{2}, b) \leq d$$

Llamemos  $d' = \text{mcd}(\frac{a}{2}, b)$ , entonces sabemos que:

- $d' \mid \frac{a}{2}$
- $d' \mid b$

Entonces por propiedades de divisibilidad:

- $d' \mid 2\frac{a}{2} = a$

Y entonces:

- $d' \mid \text{mcd}(a, b)$ , por consecuencia:
- $d' \leq \text{mcd}(a, b)$

Por lo tanto, juntando las dos partes tenemos lo que queríamos probar:

- $\text{mcd}(a, b) = \text{mcd}(\frac{a}{2}, b)$