

Matemática Discreta II

Mauro Polenta Mora

Ejercicio 2

Consigna

Sean $a, b \in \mathbb{Z}$.

1. Probar que si $d \mid a$ y $d \mid b$, entonces $d \mid (ax + by)$, para todo $x, y \in \mathbb{Z}$.
2. Probar que $\text{mcd}(a, b) = \text{mcd}(b, a - bq)$, para todo $q \in \mathbb{Z}$.
3. Describir el Algoritmo de Euclides para calcular el $\text{mcd}(a, b)$.
4. Usar el Algoritmo de Euclides para calcular el $\text{mcd}(a, b)$ en los siguientes casos:
 1. $a = 63, b = 15$
 2. $a = 455, b = 1235$
 3. $a = 2366, b = 273$

Resolución

Parte 1

- Probar que si $d \mid a$ y $d \mid b$, entonces $d \mid (ax + by)$, para todo $x, y \in \mathbb{Z}$.

Como $d \mid a$ y $d \mid b$, tenemos que:

- $a = dq_1$ con $q_1 \in \mathbb{Z}$
- $b = dq_2$ con $q_2 \in \mathbb{Z}$

Entonces tenemos que:

- $ax + by = dq_1x + dq_2y$, y sacando factor común d :
- $ax + by = d(q_1x + q_2y)$ con $q_1x + q_2y \in \mathbb{Z}$

Por lo tanto tenemos que $d \mid (ax + by)$

Parte 2

- Probar que $\text{mcd}(a, b) = \text{mcd}(b, a - bq)$, para todo $q \in \mathbb{Z}$.

Llamamos:

- $d = \text{mcd}(a, b)$, y
- $d' = \text{mcd}(b, a - bq)$

La estrategia para probar esta parte es mostrar que $d \leq d'$ y $d' \leq d$.

$$d \leq d'$$

$$\begin{aligned} & \begin{cases} d \mid a \\ d \mid b \end{cases} \\ & \Rightarrow (\text{por propiedades de divisibilidad (1.1.5)}) \\ & \begin{cases} d \mid a - bx \\ d \mid b \end{cases} \end{aligned}$$

Entonces tenemos que $d \in \text{Div}(a - bx) \cup \text{Div}(b)$, por lo tanto $d \leq \text{mcd}(b, a - bx) = d'$.

$$d' \leq d$$

$$\begin{aligned} & \begin{cases} d \mid b \\ d \mid a - bx \end{cases} \\ & \Rightarrow (\text{por propiedades de divisibilidad (1.1.5)}) \\ & \begin{cases} d \mid b \\ d \mid 1(a - bx) + bx \end{cases} \\ & \Rightarrow (\text{por propiedades de divisibilidad (1.1.5)}) \\ & \begin{cases} d \mid b \\ d \mid a \end{cases} \end{aligned}$$

Entonces tenemos que $d' \in \text{Div}(a) \cup \text{Div}(b)$, por lo tanto $d' \leq \text{mcd}(a, b) = d$.

Conclusión

Juntando las dos partes, tenemos que:

- $d \leq d'$, y
- $d' \leq d$

Entonces, podemos concluir que:

- $d = d'$

Que es lo que queríamos probar. \square

Parte 3

Está hecho en la clase 2 del teórico.

Parte 4

1. $a = 63, b = 15$
2. $a = 455, b = 1235$
3. $a = 2366, b = 273$

Subparte 1

- $a = 63, b = 15$

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

Subparte 2

- $a = 455, b = 1235$

$$\begin{aligned} & \text{mcd}(455, 1235) \\ &= \\ & \text{mcd}(1235, 455) \\ &= \\ & \text{mcd}(455, 325) \\ &= \\ & \text{mcd}(325, 130) \\ &= \\ & \text{mcd}(130, 65) \\ &= \\ & \text{mcd}(65, 0) \\ &= \\ & 65 \end{aligned}$$

Subparte 3

- $a = 2366, b = 273$

$$\begin{aligned}
& mcd(2366, 273) \\
& = \\
& mcd(273, 182) \\
& = \\
& mcd(182, 91) \\
& = \\
& mcd(91, 0) \\
& = \\
& 91
\end{aligned}$$