Matemática Discreta I
Clase 11 - Máximo común divisor (1)

FAMAF / UNC

27 de abril de 2023

Definición de MCD

Definición

Si a y b son enteros algunos de ellos no nulo, decimos que un entero positivo d es un *máximo común divisor*, o *mcd*, de a y b si

a) $d|a$ y $d|b$;

b) si $c|a$ y $c|b$ entonces $c \leq d$.

- La condición (a) nos dice que d es un común divisor de a y b.
- La condición (b) nos dice que cualquier divisor común de a y b es mayor o igual a d.

Ejemplo

¿Cuál es el mcd entre 60 y 84?

Solución

- 6 es un divisor común de 60 y 84, pero no es el mayor divisor común, porque $12|60$ y $12|84$ pero $12 < 6$.
- Los divisores positivos comunes de 60 y 84 son 1, 2, 3, 6 y 12, luego aunque 6 es un divisor común, no satisface (2) de la definición.
- En este caso, 12 claramente es el **máximo común divisor**.

Ejemplo

Hallar $\mathrm{mcd}(174, 72)$.

Solución

Divisores de 174: 1, 2, 3, 6, 29, 58, 87, 174

Divisores de 72: 1, 2, 3, 4, 6, 8, 9, 12, 18, 24, 36, 72

Luego, 6 es divisor común de 174 y 72, y todos los demás divisores comunes (1, 2 y 3) dividen a 6.

Por lo tanto $\mathrm{mcd}(174, 72) = 6$. $\square$

Proposición

Sean a, b enteros con $a \neq 0$, entonces

1. $\text{mcd}(b, a) = \text{mcd}(a, b) = \text{mcd}(\pm a, \pm b)$,
2. *si* $a > 0$, $\text{mcd}(a, 0) = a$ *y* $\text{mcd}(a, a) = a$,
3. $\text{mcd}(1, b) = 1$.

Demostración

Estas propiedades son de demostración casi trivial, por ejemplo para demostrar que $\text{mcd}(1, b) = 1$ comprobamos que 1 cumple con la definición:

(a) $1|1$ y $1|b$;

(b) si $c|1$ y $c|b$ entonces $c|1$,

propiedades que son obviamente verdaderas.
1. y 2. se dejan a cargo del lector. □

La siguiente propiedad no es tan obvia y resulta muy importante.

Propiedad

Si $a \neq 0, b \in \mathbb{Z}$, *entonces* $\operatorname{mcd}(a, b) = \operatorname{mcd}(a, b - a)$.

Demostración

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

(a) $d|a$ y $d|b$ y (b) si $c|a$ y $c|b$ entonces $c|d$.

Debemos probar que

(a') $d|a$ y $d|b - a$ y (b') si $c|a$ y $c|b - a$ entonces $c|d$.

Por (a), $d|a$ y $d|b \Rightarrow d|b - a \Rightarrow$ (a').

Si $c|a$ y $c|b - a \Rightarrow c|a + (b - a) = b \overset{(b)}{\Rightarrow} c|d \Rightarrow$ (b'). $\square$

Ejemplo

Encontrar el mcd entre 174 y 72.

Solución:

$$\begin{aligned}
(174, 72) &= (72, 174) = (72, 174 - 72) = (72, 102)\\
&= (72, 102 - 72) = (72, 30)\\
&= (30, 72) = (30, 72 - 30) = (42, 30)\\
&= (30, 42) = (30, 42 - 30) = (30, 12)\\
&= (12, 30) = (12, 30 - 12)\\
&= (12, 18) = (12, 18 - 12) = (12, 6)\\
&= (6, 12) = (6, 12 - 6)\\
&= (6, 6) = (6, 6 - 6)\\
&= (6, 0)\\
&= 6. \qquad \square
\end{aligned}$$

• En general no es sencillo encontrar todos los divisores de un número entero grande.

• No es factible calcular el mcd de números grandes revisando todos los divisores comunes.

• El algoritmo anterior nos da un método práctico y relativamente eficiente para calcular el mcd.

La próxima proposición nos provee una herramienta aún mejor para calcular el mcd.

Proposición

Sean a, b *enteros no negativos con* $b \neq 0$*, entonces*

$$a = bq + r \quad \Rightarrow \quad \text{mcd}(a, b) = \text{mcd}(b, r). \tag{1}$$

Ejemplo

Encuentre el mcd de 174 y 72.

Solución

Con el uso repetido de la proposición anterior, obtenemos

$$\begin{aligned}
174 &= 72 \cdot 2 + 30, &\quad \text{entonces} \quad (174, 72) &= (72, 30) \\
72 &= 30 \cdot 2 + 12, &\quad \text{entonces} \quad (72, 30) &= (30, 12) \\
30 &= 12 \cdot 2 + 6, &\quad \text{entonces} \quad (30, 12) &= (12, 6) \\
12 &= 6 \cdot 2 + 0, &\quad \text{entonces} \quad (12, 6) &= (6, 0) = 6.
\end{aligned}$$

Por lo tanto $(174, 72) = 6$. $\square$

Algoritmo de Euclides

Para calcular el mcd de enteros a y b, con $b > 0$, definimos q_i y r_i recursivamente de la siguiente manera: $r_0 = a$, $r_1 = b$, y

$$\begin{array}{lcl}
(e_1) & r_0 = r_1 q_1 + r_2 & (0 < r_2 < r_1) \\
(e_2) & r_1 = r_2 q_2 + r_3 & (0 < r_3 < r_2) \\
(e_3) & r_2 = r_3 q_3 + r_4 & (0 < r_4 < r_3) \\
\dots & & \\
(e_i) & r_{i-1} = r_i q_i + r_{i+1} & (0 < r_{i+1} < r_i) \\
\dots & & \\
(e_{k-1}) & r_{k-2} = r_{k-1} q_{k-1} + r_k & (0 < r_k < r_{k-1}) \\
(e_k) & r_{k-1} = r_k q_k + 0, &
\end{array}$$

Entonces $r_k = \mathrm{mcd}(a, b)$.

- El proceso se detiene en el primer resto r_i igual a 0.
- El proceso debe detenerse, porque cada resto no nulo es positivo y estrictamente menor que el anterior.
- Este procedimiento es conocido como el *algoritmo de Euclides*.

Teorema

Sean a y b enteros con $b > 0$, entonces el máximo común divisor es el último resto no nulo obtenido en el algoritmo de Euclides (r_k de la filmina anterior).

Idea de la demostración

$r_{i-1} = r_i q_i + r_{i+1} \Rightarrow \mathrm{mcd}(r_{i-1}, r_i) = \mathrm{mcd}(r_i, r_{i+1})$. Luego,

$$\mathrm{mcd}(a, b) = \mathrm{mcd}(r_0, r_1) = \mathrm{mcd}(r_1, r_2) = \cdots$$
$$\cdots = \mathrm{mcd}(r_{k-1}, r_k) = \mathrm{mcd}(r_k, 0) = r_k. \quad \square$$

Ejemplifiquemos el algoritmo de Euclides.

Ejemplo

Encuentre el mcd de 2406 y 654.

Solución

Tenemos

$$\begin{aligned}
2406 &= 654 \cdot 3 + 444, & \text{entonces} && (2406, 654) &= (654, 444)\\
654 &= 444 \cdot 1 + 210, & \text{entonces} && (654, 444) &= (444, 210)\\
444 &= 210 \cdot 2 + 24, & \text{entonces} && (444, 210) &= (210, 24)\\
210 &= 24 \cdot 8 + 18, & \text{entonces} && (210, 24) &= (24, 18)\\
24 &= 18 \cdot 1 + 6, & \text{entonces} && (24, 18) &= (18, 6)\\
18 &= 6 \cdot 3 + 0 & \text{entonces} && (18, 6) &= (6, 0) = 6
\end{aligned}$$

Por lo tanto $(2406, 654) = 6$.