Matemática Discreta I
Clase 12 - Máximo común divisor (1)

FAMAF / UNC

3 de mayo de 2022

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 $c|d$.

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 $c|d$.

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

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 $c|d$.

- 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 también divisor de d.

Ejemplo

¿Cuál es el mcd entre 60 y 84?

Ejemplo

¿Cuál es el mcd entre 60 y 84?

Solución

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 $12 \not| 6$.
- 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**.

Preguntas

Preguntas

- Dados $a, b \in \mathbb{Z}$ arbitrarios, alguno de ellos no nulo ¿existe el máximo común divisor?

Preguntas

- Dados $a, b \in \mathbb{Z}$ arbitrarios, alguno de ellos no nulo ¿existe el máximo común divisor?
  Rta: Sí.

Preguntas

- Dados $a, b \in \mathbb{Z}$ arbitrarios, alguno de ellos no nulo ¿existe el máximo común divisor?
  Rta: Sí.

- Si existe, ¿hay una forma eficiente de calcularlo?

Preguntas

- Dados $a, b \in \mathbb{Z}$ arbitrarios, alguno de ellos no nulo ¿existe el máximo común divisor?
  Rta: Sí.

- Si existe, ¿hay una forma eficiente de calcularlo?
  Rta: Sí.

Preguntas

- Dados $a, b \in \mathbb{Z}$ arbitrarios, alguno de ellos no nulo ¿existe el máximo común divisor?
  Rta: Sí.

- Si existe, ¿hay una forma eficiente de calcularlo?
  Rta: Sí.

- ¿Cuántos máximos común divisores puede tener un par de enteros?

Preguntas

- Dados $a, b \in \mathbb{Z}$ arbitrarios, alguno de ellos no nulo ¿existe el máximo común divisor?
  Rta: Sí.

- Si existe, ¿hay una forma eficiente de calcularlo?
  Rta: Sí.

- ¿Cuántos máximos común divisores puede tener un par de enteros?
  Rta: 1.

La primera y tercera pregunta son respondidas por el siguiente:

Teorema

Dados $a, b \in \mathbb{Z}$, alguno de ellos no nulo, existe un único $d \in \mathbb{Z}$ que es el máximo común divisor.

La primera y tercera pregunta son respondidas por el siguiente:

Teorema

Dados $a, b \in \mathbb{Z}$, alguno de ellos no nulo, existe un único $d \in \mathbb{Z}$ que es el máximo común divisor.

Idea de la demostración

La primera y tercera pregunta son respondidas por el siguiente:

Teorema

Dados $a, b \in \mathbb{Z}$, alguno de ellos no nulo, existe un único $d \in \mathbb{Z}$ que es el máximo común divisor.

Idea de la demostración

$$S = \{ma + nb : m, n \in \mathbb{Z}, ma + nb > 0\} \subset \mathbb{N}.$$

El mínimo de S es el mcd. $\square$

La primera y tercera pregunta son respondidas por el siguiente:

Teorema

Dados $a, b \in \mathbb{Z}$, alguno de ellos no nulo, existe un único $d \in \mathbb{Z}$ que es el máximo común divisor.

Idea de la demostración

$$S = \{ma + nb : m, n \in \mathbb{Z}, ma + nb > 0\} \subset \mathbb{N}.$$

El mínimo de S es el mcd. $\square$

Notación

Sean $a, b \in \mathbb{Z}$, alguno de ellos no nulo, denotamos $\mathrm{mcd}(a, b)$ o (a, b) al máximo común divisor entre a y b.

Ejemplo

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

Ejemplo

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

Solución

Ejemplo

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

Solución

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

Ejemplo

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

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

Ejemplo

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

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 $\text{mcd}(174, 72) = 6$. $\square$

Proposición

Sean $a, b \in \mathbb{Z}$, *alguno de ellos no nulo. Entonces existen* $s, t \in \mathbb{Z}$ *tal que*

$$(a, b) = sa + tb.$$

Demostración

Es consecuencia inmediata de la demostración del teorema de la p. 5. □

Proposición

Sean $a, b \in \mathbb{Z}$, *alguno de ellos no nulo. Entonces existen* $s, t \in \mathbb{Z}$ *tal que*

$$(a, b) = sa + tb.$$

Demostración

Es consecuencia inmediata de la demostración del teorema de la p. 5. $\square$

Corolario

Sean a *y* b *enteros,* b *no nulo, entonces*

$$(a, b) = 1 \Leftrightarrow \text{existen } s, t \in \mathbb{Z} \text{ tales que } 1 = sa + tb.$$

Proposición

Sean $a, b \in \mathbb{Z}$, *alguno de ellos no nulo. Entonces existen* $s, t \in \mathbb{Z}$ *tal que*

$$(a, b) = sa + tb.$$

Demostración

Es consecuencia inmediata de la demostración del teorema de la p. 5. $\square$

Corolario

Sean a *y* b *enteros,* b *no nulo, entonces*

$$(a, b) = 1 \Leftrightarrow \text{existen } s, t \in \mathbb{Z} \text{ tales que } 1 = sa + tb.$$

Definición

Si $(a, b) = 1$ entonces decimos que a y b son *coprimos*.

Observación

Por el corolario de la página anterior

$$a, b \text{ coprimos} \quad \Leftrightarrow \quad \text{existen } s, t \in \mathbb{Z} \text{ tales que } 1 = sa + tb.$$

Observación

NO es cierto que si existen $s, t \in \mathbb{Z}$ tales que $d = sa + tb \Rightarrow d = (a, b)$.

Por ejemplo, $4 = 2 \cdot 6 + (-2) \cdot 4$ y $(6, 4) = 2$.

Proposición

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

1. $\mathrm{mcd}(b, a) = \mathrm{mcd}(a, b) = \mathrm{mcd}(\pm a, \pm b)$,

Proposición

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

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

Proposición

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

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

Proposición

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

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

Demostración

Estas propiedades son de demostración casi trivial, por ejemplo para demostrar que $\mathrm{mcd}(1, b) = 1$ 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. $\square$

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

Propiedad

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

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 $c|d$.

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

Propiedad

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

Demostración

Sea $d = \mathrm{mcd}(a, b)$, 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 $c|d$.

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

Propiedad

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

Demostración

Sea $d = \text{mcd}(a, b)$, 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').

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 72 y 174.

Ejemplo

Encontrar el mcd entre 72 y 174.

Solución:

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

- 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.

- 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.

• 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

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

Ejemplo

Encuentre el mcd de 174 y 72.

Ejemplo

Encuentre el mcd de 174 y 72.

Solución

Ejemplo

Encuentre el mcd de 174 y 72.

Solución

Con el uso repetido de la proposición anterior, obtenemos

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

Por lo tanto $(174, 72) = 6$. □