

# Matemática Discreta I

## Clase 10 - Divisibilidad

FAMAF / UNC

25 de abril de 2023

## Definición

Dados dos enteros  $x$  e  $y$  decimos que  $y$  *divide a*  $x$ , y escribimos  $y|x$ , si

$$x = yq \quad \text{para algún } q \in \mathbb{Z}.$$

También decimos que  $y$  es un *factor* de  $x$ , que  $y$  es un *divisor* de  $x$ , que  $x$  es *divisible* por  $y$ , y que  $x$  es *múltiplo* de  $y$ .

## Definición

Dados dos enteros  $x$  e  $y$  decimos que  $y$  *divide a*  $x$ , y escribimos  $y|x$ , si

$$x = yq \quad \text{para algún } q \in \mathbb{Z}.$$

También decimos que  $y$  es un *factor* de  $x$ , que  $y$  es un *divisor* de  $x$ , que  $x$  es *divisible* por  $y$ , y que  $x$  es *múltiplo* de  $y$ .

## Observación.

1. Si  $y|x$ , es decir si  $y$  es divisor de  $x$ , existe  $q$  tal que  $x = yq$ . Luego  $q$  es también un divisor de  $x$ .

## Definición

Dados dos enteros  $x$  e  $y$  decimos que  $y$  *divide a*  $x$ , y escribimos  $y|x$ , si

$$x = yq \quad \text{para algún } q \in \mathbb{Z}.$$

También decimos que  $y$  es un *factor* de  $x$ , que  $y$  es un *divisor* de  $x$ , que  $x$  es *divisible* por  $y$ , y que  $x$  es *múltiplo* de  $y$ .

## Observación.

1. Si  $y|x$ , es decir si  $y$  es divisor de  $x$ , existe  $q$  tal que  $x = yq$ . Luego  $q$  es también un divisor de  $x$ .
2. Si  $y|x$  e  $y \neq 0$ , denotamos  $\frac{x}{y}$  al cociente de  $x$  dividido  $y$ , es decir

$$x = \frac{x}{y} \cdot y$$

Notación.

Si  $y$  no divide a  $x$  escribimos  $y \nmid x$ .

## Notación.

Si  $y$  no divide a  $x$  escribimos  $y \nmid x$ .

## Ejemplos.

(1)  $3 \mid 12$ , pues  $12 = 3 \cdot 4$ . Es decir, 3 es divisor de 12 y luego 4 es otro divisor de 12.

## Notación.

Si  $y$  no divide a  $x$  escribimos  $y \nmid x$ .

## Ejemplos.

(1)  $3 \mid 12$ , pues  $12 = 3 \cdot 4$ . Es decir, 3 es divisor de 12 y luego 4 es otro divisor de 12.

(2)  $12 \nmid 3$ , pues no existe ningún entero  $q$  tal que  $3 = q \cdot 12$ .

## Notación.

Si  $y$  no divide a  $x$  escribimos  $y \nmid x$ .

## Ejemplos.

(1)  $3 \mid 12$ , pues  $12 = 3 \cdot 4$ . Es decir, 3 es divisor de 12 y luego 4 es otro divisor de 12.

(2)  $12 \nmid 3$ , pues no existe ningún entero  $q$  tal que  $3 = q \cdot 12$ .

(3)  $6 \mid 18$ , pues  $18 = 6 \cdot 3$ . Luego también vale que  $18 = (-6) \cdot (-3)$  y que  $-18 = (-6) \cdot 3$  y  $-18 = 6 \cdot (-3)$ . De esto se sigue que

$$\begin{array}{cccc} 6 \mid 18, & -6 \mid 18, & -6 \mid -18, & 6 \mid -18, \\ 3 \mid 18, & -3 \mid 18, & 3 \mid -18, & -3 \mid -18. \end{array}$$



# Propiedades básicas 1

Veamos ahora algunas propiedades básicas de la relación “divide a”.

# Propiedades básicas 1

Veamos ahora algunas propiedades básicas de la relación “divide a”.

Sean  $a, b, c$  enteros, entonces

# Propiedades básicas 1

Veamos ahora algunas propiedades básicas de la relación “divide a”.

Sean  $a, b, c$  enteros, entonces

1.  $1|a \quad a|\pm a;$

# Propiedades básicas 1

Veamos ahora algunas propiedades básicas de la relación “divide a”.

Sean  $a, b, c$  enteros, entonces

1.  $1|a \quad a|\pm a$ ;

Demostración.

# Propiedades básicas 1

Veamos ahora algunas propiedades básicas de la relación “divide a”.

Sean  $a, b, c$  enteros, entonces

1.  $1|a \quad a|\pm a$ ;

Demostración.

- $a = 1 \cdot a$ .
- $a = a \cdot 1$ .
- $-a = a \cdot (-1)$ .

## Propiedades básicas 2

2.  $a|0$  y 0 sólo divide a 0;

## Propiedades básicas 2

2.  $a|0$  y 0 sólo divide a 0;

Demostración.

## Propiedades básicas 2

2.  $a|0$  y 0 sólo divide a 0;

Demostración.

- $0 = a \cdot 0$ .
- Si  $0|a$  entonces existe  $q$  tal que  $a = 0 \cdot q = 0$ .

3. si  $a|b$ , entonces  $a|bc$  para cualquier  $c$ ;



## Propiedades básicas 2

2.  $a|0$  y 0 sólo divide a 0;

Demostración.

- $0 = a \cdot 0$ .
- Si  $0|a$  entonces existe  $q$  tal que  $a = 0 \cdot q = 0$ .

3. si  $a|b$ , entonces  $a|bc$  para cualquier  $c$ ;

Demostración.

## Propiedades básicas 2

2.  $a|0$  y 0 sólo divide a 0;

Demostración.

- $0 = a \cdot 0$ .
- Si  $0|a$  entonces existe  $q$  tal que  $a = 0 \cdot q = 0$ .

3. si  $a|b$ , entonces  $a|bc$  para cualquier  $c$ ;

Demostración.

- $a|b \Rightarrow b = a \cdot q \Rightarrow bc = a \cdot qc \Rightarrow a|bc$ .

## Propiedades básicas 2

4. si  $a|b$  y  $a|c$ , entonces  $a|(b+c)$ ;

## Propiedades básicas 2

4. si  $a|b$  y  $a|c$ , entonces  $a|(b+c)$ ;

Demostración.

## Propiedades básicas 2

4. si  $a|b$  y  $a|c$ , entonces  $a|(b+c)$ ;

Demostración.

- $a|b$  y  $a|c \Rightarrow b = a \cdot q$  y  $c = a \cdot q' \Rightarrow$   
 $b + c = a \cdot q + a \cdot q' = a \cdot (q + q') \Rightarrow a|(b + c).$

5. si  $a|b$  y  $a|c$ , entonces  $a|(rb + sc)$  para cualesquiera  $r, s \in \mathbb{Z}$ .

## Propiedades básicas 2

4. si  $a|b$  y  $a|c$ , entonces  $a|(b+c)$ ;

Demostración.

- $a|b$  y  $a|c \Rightarrow b = a \cdot q$  y  $c = a \cdot q' \Rightarrow$   
 $b + c = a \cdot q + a \cdot q' = a \cdot (q + q') \Rightarrow a|(b + c).$

5. si  $a|b$  y  $a|c$ , entonces  $a|(rb + sc)$  para cualesquiera  $r, s \in \mathbb{Z}$ .

Demostración.

## Propiedades básicas 2

4. si  $a|b$  y  $a|c$ , entonces  $a|(b+c)$ ;

Demostración.

- $a|b$  y  $a|c \Rightarrow b = a \cdot q$  y  $c = a \cdot q' \Rightarrow$   
 $b + c = a \cdot q + a \cdot q' = a \cdot (q + q') \Rightarrow a|(b + c).$

5. si  $a|b$  y  $a|c$ , entonces  $a|(rb + sc)$  para cualesquiera  $r, s \in \mathbb{Z}$ .

Demostración.

- $a|b$  y  $a|c \Rightarrow b = a \cdot q$  y  $c = a \cdot q' \Rightarrow$   
 $rb + sc = a \cdot rq + a \cdot sq' = a \cdot (rq + sq') \Rightarrow a|(rb + sc).$

## Propiedades básicas 3

6. si  $a|b + c$  y  $a|c$ , entonces  $a|b$ ;



## Propiedades básicas 3

6. si  $a|b + c$  y  $a|c$ , entonces  $a|b$ ;

Demostración.

## Propiedades básicas 3

6. si  $a|b + c$  y  $a|c$ , entonces  $a|b$ ;

Demostración.

- $a|b + c$  y  $a|c \Rightarrow b + c = a \cdot q$  y  $c = a \cdot q' \Rightarrow$   
 $b = (b + c) - c = a \cdot q - a \cdot q' = a \cdot (q - q') \Rightarrow a|b.$

## Propiedades básicas 3

6. si  $a|b + c$  y  $a|c$ , entonces  $a|b$ ;

Demostración.

- $a|b + c$  y  $a|c \Rightarrow b + c = a \cdot q$  y  $c = a \cdot q' \Rightarrow$   
 $b = (b + c) - c = a \cdot q - a \cdot q' = a \cdot (q - q') \Rightarrow a|b.$

7. si  $a|b$ , entonces  $\pm a|\pm b$ ;

## Propiedades básicas 3

6. si  $a|b + c$  y  $a|c$ , entonces  $a|b$ ;

Demostración.

- $a|b + c$  y  $a|c \Rightarrow b + c = a \cdot q$  y  $c = a \cdot q' \Rightarrow$   
 $b = (b + c) - c = a \cdot q - a \cdot q' = a \cdot (q - q') \Rightarrow a|b.$

7. si  $a|b$ , entonces  $\pm a|\pm b$ ;

Demostración.

## Propiedades básicas 3

6. si  $a|b + c$  y  $a|c$ , entonces  $a|b$ ;

Demostración.

- $a|b + c$  y  $a|c \Rightarrow b + c = a \cdot q$  y  $c = a \cdot q' \Rightarrow$   
 $b = (b + c) - c = a \cdot q - a \cdot q' = a \cdot (q - q') \Rightarrow a|b.$

7. si  $a|b$ , entonces  $\pm a|\pm b$ ;

Demostración.

- $a|b \Rightarrow b = a \cdot q \Rightarrow$   
 $-b = a \cdot (-q) \Rightarrow a|-b, \quad b = -a \cdot (-q) \Rightarrow -a|b$   
 $-b = -a \cdot q \Rightarrow -a|-b.$



## Proposición

*Sean  $a, b \in \mathbb{N}$ . Entonces*

$$ab = 1 \Rightarrow a = 1 \wedge b = 1.$$

## Proposición

*Sean  $a, b \in \mathbb{N}$ . Entonces*

$$ab = 1 \Rightarrow a = 1 \wedge b = 1.$$

*Demostración.*

## Proposición

Sean  $a, b \in \mathbb{N}$ . Entonces

$$ab = 1 \Rightarrow a = 1 \wedge b = 1.$$

## Demostración.

Como  $a, b \in \mathbb{N}$ , entonces  $a \geq 1$  y  $b \geq 1$ .

Si  $a = 1$ , como  $ab = 1$ , obtenemos  $1 = ab = 1 \cdot b = b$ .

Si  $a > 1$ , como  $b > 0$  por compatibilidad de  $<$  con el producto tenemos que  $ab > b$ , es decir  $1 > b$ , lo cual no es cierto ( $b \in \mathbb{N}$ ). □

## Observación

A partir de la proposición no es difícil probar que si  $a, b \in \mathbb{Z}$  y  $ab = 1$ , tenemos que  $a = 1$  y  $b = 1$  o  $a = -1$  y  $b = -1$ .



## Proposición

Sean  $a, b, c \in \mathbb{N}$ , entonces

(D1)  $a|a$  (reflexividad);

(D2) si  $a|b$  y  $b|a$ , entonces  $a = b$  (antisimetría);

(D3) si  $a|b$  y  $b|c$ , entonces  $a|c$  (transitividad).

Demostración.

## Proposición

Sean  $a, b, c \in \mathbb{N}$ , entonces

(D1)  $a|a$  (reflexividad);

(D2) si  $a|b$  y  $b|a$ , entonces  $a = b$  (antisimetría);

(D3) si  $a|b$  y  $b|c$ , entonces  $a|c$  (transitividad).

## Demostración.

(D1) Esto ya fue probado antes.

## Proposición

Sean  $a, b, c \in \mathbb{N}$ , entonces

(D1)  $a|a$  (reflexividad);

(D2) si  $a|b$  y  $b|a$ , entonces  $a = b$  (antisimetría);

(D3) si  $a|b$  y  $b|c$ , entonces  $a|c$  (transitividad).

## Demostración.

(D1) Esto ya fue probado antes.

(D2)  $a|b \Rightarrow$  existe  $q \in \mathbb{N}$  tal que  $b = aq$ .

## Proposición

Sean  $a, b, c \in \mathbb{N}$ , entonces

(D1)  $a|a$  (reflexividad);

(D2) si  $a|b$  y  $b|a$ , entonces  $a = b$  (antisimetría);

(D3) si  $a|b$  y  $b|c$ , entonces  $a|c$  (transitividad).

## Demostración.

(D1) Esto ya fue probado antes.

(D2)  $a|b \Rightarrow$  existe  $q \in \mathbb{N}$  tal que  $b = aq$ .

$b|a \Rightarrow$  existe  $q' \in \mathbb{N}$  tal que  $a = bq'$ .

## Proposición

Sean  $a, b, c \in \mathbb{N}$ , entonces

(D1)  $a|a$  (reflexividad);

(D2) si  $a|b$  y  $b|a$ , entonces  $a = b$  (antisimetría);

(D3) si  $a|b$  y  $b|c$ , entonces  $a|c$  (transitividad).

## Demostración.

(D1) Esto ya fue probado antes.

(D2)  $a|b \Rightarrow$  existe  $q \in \mathbb{N}$  tal que  $b = aq$ .

$b|a \Rightarrow$  existe  $q' \in \mathbb{N}$  tal que  $a = bq'$ .

Luego

$$b = aq = (bq')q = b(q'q).$$

## Proposición

Sean  $a, b, c \in \mathbb{N}$ , entonces

(D1)  $a|a$  (reflexividad);

(D2) si  $a|b$  y  $b|a$ , entonces  $a = b$  (antisimetría);

(D3) si  $a|b$  y  $b|c$ , entonces  $a|c$  (transitividad).

## Demostración.

(D1) Esto ya fue probado antes.

(D2)  $a|b \Rightarrow$  existe  $q \in \mathbb{N}$  tal que  $b = aq$ .

$b|a \Rightarrow$  existe  $q' \in \mathbb{N}$  tal que  $a = bq'$ .

Luego

$$b = aq = (bq')q = b(q'q).$$

Por el axioma de cancelación (cancelando  $b$ ) obtenemos que

$$1 = q'q \Rightarrow q = q' = 1.$$

## Proposición

Sean  $a, b, c \in \mathbb{N}$ , entonces

(D1)  $a|a$  (reflexividad);

(D2) si  $a|b$  y  $b|a$ , entonces  $a = b$  (antisimetría);

(D3) si  $a|b$  y  $b|c$ , entonces  $a|c$  (transitividad).

## Demostración.

(D1) Esto ya fue probado antes.

(D2)  $a|b \Rightarrow$  existe  $q \in \mathbb{N}$  tal que  $b = aq$ .

$b|a \Rightarrow$  existe  $q' \in \mathbb{N}$  tal que  $a = bq'$ .

Luego

$$b = aq = (bq')q = b(q'q).$$

Por el axioma de cancelación (cancelando  $b$ ) obtenemos que

$1 = q'q \Rightarrow q = q' = 1$ . Luego  $a = b$ .

(D3)  $a|b \Rightarrow$  existe  $q \in \mathbb{N}$  tal que  $b = aq$ .



(D3)  $a|b \Rightarrow$  existe  $q \in \mathbb{N}$  tal que  $b = aq$ .

$b|c \Rightarrow$  existe  $q' \in \mathbb{N}$  tal que  $c = bq'$ .

(D3)  $a|b \Rightarrow$  existe  $q \in \mathbb{N}$  tal que  $b = aq$ .

$b|c \Rightarrow$  existe  $q' \in \mathbb{N}$  tal que  $c = bq'$ .

Luego

$$c = bq' = aqq' = a(qq').$$

(D3)  $a|b \Rightarrow$  existe  $q \in \mathbb{N}$  tal que  $b = aq$ .

$b|c \Rightarrow$  existe  $q' \in \mathbb{N}$  tal que  $c = bq'$ .

Luego

$$c = bq' = aqq' = a(qq').$$

Luego  $a|c$ . □

(D3)  $a|b \Rightarrow$  existe  $q \in \mathbb{N}$  tal que  $b = aq$ .

$b|c \Rightarrow$  existe  $q' \in \mathbb{N}$  tal que  $c = bq'$ .

Luego

$$c = bq' = aqq' = a(qq').$$

Luego  $a|c$ . □

### Observación.

Las propiedades (D1), (D2) y (D3) nos dicen que “divide a” es una *relación de orden*.

Habíamos visto que “ $\leq$ ” también era una relación de orden.

# Ejercicios

## Ejercicio

¿Es cierto que si  $a|bc$ , entonces  $a|b$  ó  $a|c$ ?

# Ejercicios

## Ejercicio

¿Es cierto que si  $a|bc$ , entonces  $a|b$  ó  $a|c$ ?

**Solución.** No necesariamente (es decir la respuesta es NO).

- Es cierto, por ejemplo que  $3|6 \cdot 2$  y que  $3|6$ .
- Pero  $6|4 \cdot 3$  y  $6 \nmid 4$ ,  $6 \nmid 3$ .

## Ejercicio

Determinar todos los divisores de 12.

# Ejercicios

## Ejercicio

¿Es cierto que si  $a|bc$ , entonces  $a|b$  ó  $a|c$ ?

**Solución.** No necesariamente (es decir la respuesta es NO).

- Es cierto, por ejemplo que  $3|6 \cdot 2$  y que  $3|6$ .
- Pero  $6|4 \cdot 3$  y  $6 \nmid 4$ ,  $6 \nmid 3$ .

## Ejercicio

Determinar todos los divisores de 12.

**Solución.**

- $\pm 1, \pm 2, \pm 3, \pm 4, \pm 6, \pm 12$ , (12 divisores).

# Ejercicios

## Ejercicio.

Mostrar que  $4^n - 1$  es divisible por 3 para todo  $n \in \mathbb{N}$ .



# Ejercicios

## Ejercicio.

Mostrar que  $4^n - 1$  es divisible por 3 para todo  $n \in \mathbb{N}$ .

## Solución.

Este ejercicio se puede hacer de dos formas.

**1º demostración.** Por inducción sobre  $n$ .

Caso base  $n = 1$ .  $4^n - 1 = 4^1 - 1 = 4 - 1 = 3$  que obviamente es divisible por 3.

Paso inductivo. Debemos probar que  $3|4^k - 1$  para  $k \geq 1$  (HI) entonces, se deduce que  $3|4^{k+1} - 1$ .

**Opción a)** Ahora bien,

$$4^{k+1} - 1 = 4 \cdot 4^k - 1 = 3 \cdot 4^k + (4^k - 1).$$

Como  $3|3 \cdot 4^k$  y por (HI)  $3|4^k - 1$ , tenemos

$$3|3 \cdot 4^k + 4^k - 1 = 4^{k+1} - 1.$$

**Opción b)** Ahora bien, como por (HI)  $3|4^k - 1$ , existe  $q$  tal que  $4^k - 1 = 3q$ . Entonces,

$$4^{k+1} - 1 = 4 \cdot (4^k - 1) + 3 = 4 \cdot 3q + 3 = 3(4q + 1).$$

Luego

$$3|3(4q + 1) = 4^{k+1} - 1.$$

**2° demostración.** Observemos que  $4 = 3 + 1$ , luego  $4^n - 1 = (3 + 1)^n - 1$ .

$$\begin{aligned} 4^n - 1 &= (3 + 1)^n - 1 = \sum_{i=0}^n \binom{n}{i} 3^i 1^{n-i} - 1 && \text{(binomio de Newton)} \\ &= \sum_{i=0}^n \binom{n}{i} 3^i - 1 \\ &= 1 + \sum_{i=1}^n \binom{n}{i} 3^i - 1 \\ &= 1 + 3 \left( \sum_{i=1}^n \binom{n}{i} 3^{i-1} \right) - 1 \quad (i > 0 \text{ en la sumatoria}) \\ &= 3 \left( \sum_{i=1}^n \binom{n}{i} 3^{i-1} \right) \end{aligned}$$

Luego  $4^n - 1 = 3 \cdot q$ .

Por lo tanto,  $3 \mid 4^n - 1$ .

# Ejercicios

## Ejercicio

¿Cuál es el menor natural que es divisible por 6 y por 15?

# Ejercicios

## Ejercicio

¿Cuál es el menor natural que es divisible por 6 y por 15?

**Solución.** Hagamos una lista de múltiplos de 6 y 15.

- Múltiplos de 6: 6, 12, 18, 24, 30, 36, 42, 48, 54, 60, ...
- Múltiplos de 15: 15, 30, 45, 60, 75, ...
- Luego, el menor natural que es divisible por 6 y por 15 es 30.