

# Matemática Discreta II

Mauro Polenta Mora

## CLASE 1 - 30/7/2025

### Divisibilidad

#### Introducción

Veamos algo de notación para los conjuntos que estaremos usando de ahora en adelante:

- $\mathbb{Z}$  es el conjunto de números enteros, es decir:
  - $\mathbb{Z} = \{0, \pm 1, \pm 2, \pm 3, \dots\}$
- $\mathbb{Z}^+$  es el conjunto de números enteros POSITIVOS, sin incluir el 0:
  - $\mathbb{Z}^+ = \{n \in \mathbb{Z} : n > 0\} = \{1, 2, 3, \dots\}$
- $\mathbb{N}$  es el conjunto de números naturales:
  - $\mathbb{N} = \{0, 1, 2, 3, \dots\}$

#### Teorema 1.1.1 (Teorema de la división entera)

Dados  $a, b \in \mathbb{Z}$ , con  $b \neq 0$ , existen únicos  $q, r \in \mathbb{Z}$  con:

- $0 \leq r < |b|$  y,
- $a = bq + r$

Veamos algunas observaciones antes de pasar a la demostración:

1. A  $q$  se le llama el cociente y a  $r$  el resto de dividir  $a$  entre  $b$ .
2. Basta con suponer que  $b > 0$ , ya que si  $a = bq + r$  entonces  $a = (-b)(-q) + r$
3. Basta con suponer que  $a \geq 0$ , ya que si  $a = bq + r$  (con  $b > 0$  y  $0 \leq r \leq b$ ) entonces:
  - $-a = -bq - r$

Pero aquí tenemos el problema de que si  $r \neq 0$  entonces no obtuvimos un resto positivo. Entonces observemos que si sumamos y restamos  $b$ , tenemos que:

- $-a = -bq - b + b - r$ , reagrupando:
- $-a = b(-q - 1) + b - r$

Y ahora si  $r \neq 0$ , al tener que  $0 < r < b$ , tenemos que:

- $0 < b - r < b$

Entonces con las últimas dos observaciones nos podemos permitir probar el teorema considerando  $a \geq 0$  y  $b > 0$ .

### **Demostración**

Suponemos que  $a \geq 0$  y  $b > 0$  por lo visto en las observaciones anteriores.

Para probar la existencia, consideremos el conjunto:

- $S = \{s \in \mathbb{N} : s = a - bx \text{ para algún } x \in \mathbb{Z}\}$

Entonces, al ser  $a \geq 0$ , tomando  $x = 0$ , tenemos que  $a \in S$ , por lo que  $S \neq \emptyset$ . Usando que todo conjunto de números naturales no vacío tiene mínimo, llamamos  $r = \min(S)$ . Por definición de  $S$  ya tenemos que  $s \geq 0$  y que existe un  $q \in \mathbb{Z}$  tal que:

- $r = a - bq$ , que es equivalente a:
- $a = bq + r$

Ahora nos faltaría probar que  $r < b$ , supongamos por el contrario, que  $r \geq b$ . Entonces tendríamos que para cualquier  $s \in \mathbb{N}$ , se cumple que  $r = b + s$  con  $0 \leq s < r$ , pero en este caso también tendríamos que:

- $s = r - b = a - bq - b = a - b(q + 1)$

Entonces  $s \in S$  y además  $s < r$ . Pero esto es absurdo, pues  $r = \min(S)$ .

Ahora veamos la unicidad: supongamos que  $a = bq_1 + r_1$  y  $a = bq_2 + r_2$  con  $0 \leq r_1, r_2 < b$ . Por lo tanto tenemos que  $bq_1 + r_1 = bq_2 + r_2$ , o escrito de otra forma:

- $r_2 = b(q_1 - q_2) + r_1 \quad (*_1)$

Observemos que:

- Si  $q_1 - q_2 \geq 1$ , entonces tendríamos que  $r_2 \geq b$ , que es absurdo.
- Si  $q_1 - q_2 \leq -1$ , entonces tendríamos que  $r_2 < 0$  (pues  $r_1 < b$ ), que también es absurdo.

Entonces necesariamente  $q_1 - q_2 = 0$ , por lo que  $q_1 = q_2$ . Sustituyendo ahora en  $(*_1)$ , obtenemos que  $r_1 = r_2$

### **Proposición 1.1.2 (aplicación del Teorema de la división entera)**

Sean  $b \in \mathbb{N}$ , con  $b \geq 2$  y  $x \in \mathbb{N}$ , entonces existen  $a_0, a_1, \dots, a_n$  enteros tales que podemos escribir a  $x$  en base  $b$  como:

$$x = b^n a_n + b^{n-1} a_{n-1} + \dots + b^1 a_1 + b^0 a_0 = \sum_{i=0}^n b^i a_i$$

Con  $0 \leq a_i < b$  y  $a_n \neq 0$

## Demostración

Lo probaremos por inducción en  $x \in \mathbb{N}$ . Si  $x = 0$  la demostración es directa pues  $x = b^0 \cdot 0$ . Si  $x > 0$ , entonces por el teorema de la división entera tenemos que existen  $q$  y  $r$  tales que  $x = bq + r$  con  $0 \leq r < b$ . Como  $q < x$ , entonces aplicamos la hipótesis inductiva sobre él, obteniendo que:

$$\bullet \quad q = \sum_{i=0}^n b^i a'_i \text{ con } 0 \leq a_i < b.$$

Entonces:

$$\begin{aligned} x & \\ &= (\text{sustituyendo por } q) \\ &b \left( \sum_{i=0}^n b^i a'_i \right) + r \\ &= (\text{operatoria}) \\ &\left( \sum_{i=0}^n b^{i+1} a'_i \right) + r \\ &= (\text{operatoria}) \\ &\sum_{i=0}^{n+1} b^i a'_i \quad \text{con } a_0 = r \text{ y } a_{i+1} = a'_i \end{aligned}$$

Lo que demuestra la propiedad. Observemos que los enteros son únicos, y denotamos la descomposición de  $x$  en base  $b$  como  $x = (a_n a_{n-1} \dots a_1 a_0)_b$

## Ejemplos 1.1.3

### Ejemplo 1

Veamos como escribir  $n = 233$  en base 4:

$$\begin{aligned} 233 &= 4 \cdot 58 + 1 \\ &= 4 \cdot (4 \cdot 14 + 2) + 1 \\ &= 4 \cdot (4 \cdot (4 \cdot 3 + 2) + 2) + 1 \\ &= 4^3 \cdot 3 + 4^2 \cdot 2 + 4^1 \cdot 2 + 4^0 \cdot 1 \end{aligned}$$

Entonces  $233 = (3221)_4$

### Ejemplo 2

Si queremos hallar la descomposición de  $n = 233$  en base 2, podemos usar la descomposición en base 4:

$$\begin{aligned} 233 &= 4^3 \cdot 3 + 4^2 \cdot 2 + 4^1 \cdot 2 + 4^0 \cdot 1 \\ &= 2^6 \cdot (2^1 \cdot 1 + 1) + 2^4 \cdot 2 + 2^2 \cdot 2 + 2^0 \cdot 1 \\ &= 2^7 + 2^6 + 2^5 + 2^3 + 2^0 \end{aligned}$$

Entonces  $233 = (11101001)_2$