

# Matemática Discreta I

## Tema 2. Aritmética entera

Jesús Martínez Mateo [jmartinez@fi.upm.es](mailto:jmartinez@fi.upm.es)

Departamento de Matemática Aplicada a las TIC  
E.T.S. Ingenieros Informáticos  
Universidad Politécnica de Madrid

Grado en Ingeniería Informática  
Curso 2020/21

# Contenidos

## 1 Conjunto de los números enteros

- Axioma de buena ordenación

## 2 Inducción matemática

## 3 Divisibilidad

- Sistemas de numeración
- Máximo común divisor
- Algoritmo de Euclides
  - Identidad de Bezout. Algoritmo extendido de Euclides
- Ecuaciones diofánticas

## 4 Números primos

- Teorema fundamental de la aritmética

# Conjunto de los números enteros $\mathbb{Z}$

Llamamos conjunto de los números enteros al conjunto

$$\mathbb{Z} = \{\dots, -3, -2, -1, 0, 1, 2, 3, \dots\}$$

que junto con las operaciones suma y producto  $(\mathbb{Z}, +, \cdot)$  verifica las siguientes propiedades:

- La suma y el producto son leyes de composición internas:  
 $\forall a, b \in \mathbb{Z}, a + b \in \mathbb{Z}, ab \in \mathbb{Z}.$
- Asociativa:  $\forall a, b, c \in \mathbb{Z}, a + (b + c) = (a + b) + c, a(bc) = (ab)c.$
- Conmutativa:  $\forall a, b \in \mathbb{Z}, a + b = b + a, ab = ba.$
- Existencia de elemento neutro:  $\forall a \in \mathbb{Z}, \exists 0 \in \mathbb{Z} \mid a + 0 = a,$   
 $\exists 1 \in \mathbb{Z} \mid a1 = a.$
- Existencia de elemento opuesto:  $\forall a \in \mathbb{Z}, \exists -a \in \mathbb{Z} \mid a + (-a) = 0.$
- Distributiva:  $\forall a, b, c \in \mathbb{Z}, a(b + c) = ab + ac.$

## Relación de orden en $\mathbb{Z}$

El conjunto de los números enteros  $\mathbb{Z}$  con la relación **menor o igual**  $(\mathbb{Z}, \leq)$  verifica la siguientes propiedades:

- Reflexiva:  $\forall a \in \mathbb{Z}, a \leq a$ .
- Antisimétrica:  $\forall a, b \in \mathbb{Z}$ , si  $a \leq b, b \leq a$  entonces  $a = b$ .
- Transitiva:  $\forall a, b, c \in \mathbb{Z}$ , si  $a \leq b, b \leq c$  entonces  $a \leq c$ .

La relación  $\leq$  es por lo tanto una relación de orden en  $\mathbb{Z}$ , y el par  $(\mathbb{Z}, \leq)$  es un conjunto totalmente ordenado:  $\forall a, b \in \mathbb{Z}, a \leq b$  o  $b \leq a$ .

Otra propiedad del conjunto  $\mathbb{Z}$  es que la relación menor o igual en  $\mathbb{Z}$  es compatible con las operaciones suma y producto:

- $\forall a, b, c \in \mathbb{Z}$ , si  $a \leq b$  entonces  $a + c \leq b + c$ , y si  $a \leq b, c > 0$  entonces  $ac \leq bc$ .

# Axioma de buena ordenación

## Definición

Sea  $S \subseteq \mathbb{Z}$ . Decimos que  $c \in \mathbb{Z}$  es una **cota inferior** del conjunto  $S$  si  $\forall a \in S, c \leq a$ . Si además  $c \in S$  decimos entonces que  $c$  es el **primer elemento** (o elemento mínimo) de  $S$ . Análogamente, decimos que  $d \in \mathbb{Z}$  es una **cota superior** de  $S$  si  $\forall a \in S, a \leq d$ , y decimos que  $d$  es el **último elemento** (o elemento máximo) de  $S$  si  $d \in S$ .

Concluimos con una propiedad más del conjunto  $\mathbb{Z}$ , el **axioma de buena ordenación**:

- Todo subconjunto  $S$  de  $\mathbb{Z}$ , no vacío, y acotado inferiormente (ie. existe una cota inferior de  $S$  en  $\mathbb{Z}$ ) posee un primer elemento. Análogamente, todo subconjunto de  $\mathbb{Z}$ , no vacío, y acotado superiormente posee un último elemento.

# Propiedad cancelativa

## Teorema (Propiedad cancelativa del producto)

$\forall a, b, c \in \mathbb{Z}$ , si  $a \neq 0$ ,  $ab = ac$  entonces  $b = c$ .

### Demostración.

Probamos en primer lugar que  $a0 = 0$ . Efectivamente,

$$\begin{aligned} a0 &= a0 + \underbrace{0}_{\text{neutro} +} = a0 + \underbrace{a + (-a)}_{\text{opuesto} +} = a0 + \underbrace{a1}_{\text{neutro} \cdot} - a = \\ &= \underbrace{a(0 + 1)}_{\text{distributiva}} - a = a1 - a = 0. \end{aligned}$$

Probamos ahora que si  $ab = 0$  con  $a \neq 0$  tenemos necesariamente que  $b = 0$ .

# Propiedad cancelativa

## Teorema (Propiedad cancelativa del producto)

$\forall a, b, c \in \mathbb{Z}$ , si  $a \neq 0$ ,  $ab = ac$  entonces  $b = c$ .

### Demostración.

Efectivamente,

$$ab = 0 \Rightarrow ab = a + (-a) \Rightarrow ab + a = a \Rightarrow a(b + 1) = a.$$

Finalmente, podemos reescribir

$$ab = ac \Rightarrow ab + a(-c) = 0 \Rightarrow a(b - c) = 0$$

y por ser  $a \neq 0$  tenemos que  $b - c = 0$ , y por lo tanto  $b = c$ . □

# Inducción matemática

## Definición

Decimos que un conjunto  $S$  es un **conjunto inductivo** si verifica que:

- $1 \in S$ .
- Si  $x \in S$  entonces  $x + 1 \in S$ .

Veamos que  $\mathbb{N}$  es el mejor conjunto inductivo.

## Teorema

Si  $S \subseteq \mathbb{N}$  es un conjunto inductivo, entonces  $S = \mathbb{N}$ .

## Demostración.

Asumimos que  $S \neq \mathbb{N}$  y por lo tanto existe el complementario de  $S$  en  $\mathbb{N}$ ,  $S^c$ , no vacío. Como  $S^c \subseteq \mathbb{N} \subset \mathbb{Z}$  y está acotado inferiormente (ya que  $\mathbb{N}$  lo está), por el axioma de buena ordenación tenemos que  $S^c$  tiene un primer elemento, digamos  $a$ . Luego  $a - 1 \notin S^c$  y por lo tanto  $a - 1 \in S$ , pero por la hipótesis tendríamos que  $(a - 1) + 1 \in S$ , es decir, también tendríamos que  $a \in S$  lo que contradice que  $a$  es el primer elemento de  $S^c$ .





# Inducción matemática

## Teorema (Principio de inducción)

Sea  $P_n$  una proposición matemática. Si se verifican:

- $P_1$  es verdadera.
- Si  $P_k$  es verdadera entonces  $P_{k+1}$  también lo es.

entonces  $P_n$  es verdadera para todo  $n \in \mathbb{N}$ .

## Demostración.

Sea  $S = \{n \in \mathbb{N} \mid P_n \text{ es cierta}\}$ . Por la hipótesis de inducción sabemos que  $1 \in S$  y si  $k \in S$  entonces  $k + 1 \in S$  por lo que  $S$  es un conjunto inductivo y por el teorema anterior sabemos que  $S = \mathbb{N}$ . Luego la propiedad  $P_n$  es cierta  $\forall n \in \mathbb{N}$ . □

# Inducción matemática

## Ejemplo

Demuestra por inducción que  $\sum_{k=1}^n (2k - 1) = n^2$  para todo  $n \in \mathbb{N}$ .

- 1 Comprobamos que efectivamente se cumple para  $n = 1$ , es decir,  $\sum_{k=1}^1 (2k - 1) = 2 \cdot 1 - 1 = 1^2$ .
- 2 Asumimos que se cumple para  $n$ , es decir, que  $\sum_{k=1}^n (2k - 1) = n^2$ , y demostramos que también se cumple para  $n + 1$ . Efectivamente,

$$\sum_{k=1}^n (2k - 1) = n^2 \Rightarrow$$

$$\Rightarrow \left( \sum_{k=1}^n (2k - 1) \right) + 2(n + 1) - 1 = n^2 + 2(n + 1) - 1 \Rightarrow$$

$$\Rightarrow \sum_{k=1}^{n+1} (2k - 1) = n^2 + 2n + 1 = (n + 1)^2. \quad \square$$

# Divisibilidad

## Definición

Sean  $a, b \in \mathbb{Z}$  con  $b \neq 0$ . Decimos que  $b$  **divide a**  $a$  (o que  $b$  es un divisor o factor de  $a$ ), y lo denotamos por  $b \mid a$ , si y sólo si existe  $q \in \mathbb{Z}$  tal que  $a = qb$ . También decimos que  $a$  es un múltiplo de  $b$ .

**Propiedades.** Sean  $a, b, c, d \in \mathbb{Z}$ .

- $1 \mid a$ .
- $a \mid 0$ .
- Si  $a \mid b$  y  $b \mid c$  entonces  $a \mid c$ .
- Si  $a \mid b$  y  $c \mid d$  entonces  $ac \mid bd$ .
- Si  $c \mid a$  y  $c \mid b$  entonces  $c \mid (ax + by) \quad \forall x, y \in \mathbb{Z}$ .
- Si  $a \mid b$  y  $b \mid a$  entonces  $a = b$  o  $a = -b$ .

# Divisibilidad

## Teorema (Teorema de la división)

Sean  $a, b \in \mathbb{Z}$  con  $b > 0$ . Existe un único par de enteros  $q$  y  $r$  tales que

$$a = qb + r, \quad 0 \leq r < b.$$

## Definición

Sean  $a, b \in \mathbb{Z}$  con  $b > 0$ , y  $q, r \in \mathbb{Z}$  tales que  $a = qb + r$  con  $0 \leq r < b$ . Llamamos **dividendo** al entero  $a$ , **divisor** al entero  $b$ , y a los enteros  $q$  y  $r$  los llamamos **cociente** y **resto**, respectivamente.

## Corolario

Sean  $a, b \in \mathbb{Z}$  con  $b \neq 0$ . Existe un único par de enteros  $q$  y  $r$  tales que

$$a = qb + r, \quad 0 \leq r < |b|.$$

# Divisibilidad

## Demostración.

- **Existencia.** Sea  $S = \{a - qb \mid q \in \mathbb{Z}\}$ . El conjunto  $S \cap \mathbb{N}$  es un subconjunto no vacío de  $\mathbb{N}$ , y por lo tanto de  $\mathbb{Z}$ . El principio de buena ordenación nos asegura la existencia de un primer elemento de la forma  $r = a - qb \geq 0$ , es decir,  $a = qb + r$  con  $r \geq 0$ . Se tiene también necesariamente que  $r < b$ . De lo contrario, si  $r \geq b$  existe el entero  $r - b = a - (q + 1)b \geq 0$  por lo que  $r$  no sería el primer elemento de  $S$ .
- **Unicidad.** Suponemos que existen  $q, q', r, r' \in \mathbb{Z}$  tales que  $a = qb + r = q'b + r'$  con  $0 \leq r < b$  y  $0 \leq r' < b$ . Tenemos entonces que  $r - r' = (q' - q)b$ . Si  $q \neq q'$  tenemos que  $|q' - q| \geq 1$  y por lo tanto  $|r - r'| \geq b$  lo que contradice que  $0 \leq r < b$  y  $0 \leq r' < b$ .



# Sistemas de numeración

## Definición

Decimos que  $n \in \mathbb{N}$  **está expresado en base  $b$** , y lo denotamos por  $n = (r_k r_{k-1} \dots r_1 r_0)_b$ , si

$$n = r_k b^k + r_{k-1} b^{k-1} + \dots + r_1 b + r_0 = \sum_{j=0}^k r_j b^j$$

con  $0 \leq r_i < b$  para todo  $i \in \{0, 1, \dots, k\}$ , y  $r_k \neq 0$ .

## Teorema

*Sea  $b \in \mathbb{N}$  con  $b \geq 2$ . Cualquier número  $n \in \mathbb{N}$  puede expresarse de forma única en base  $b$ .*

# Sistemas de numeración

## Demostración.

Por el teorema de la división entera tenemos que

$$n = q_0b + r_0 \quad 0 \leq r_0 < b \quad 0 \leq q_0 < n$$

$$q_0 = q_1b + r_1 \quad 0 \leq r_1 < b \quad 0 \leq q_1 < q_0 < n$$

$$q_1 = q_2b + r_2 \quad 0 \leq r_2 < b \quad 0 \leq q_2 < q_1 < q_0 < n$$

...

$$q_{k-1} = q_kb + r_k \quad 0 \leq r_k < b \quad 0 = q_k < q_{k-1} < \dots < q_0 < n$$

El conjunto de los cociente  $Q = \{q_i \in \mathbb{Z}\}$  está acotado inferiormente por cero, por lo que por el axioma de buena ordenación existe un primer elemento, es decir, existe  $q_k = 0$  para algún  $k$  finito. Tenemos entonces que

$$\begin{aligned} n &= q_0b + r_0 = (q_1b + r_1)b + r_0 = ((q_2b + r_2)b + r_1)b + r_0 = \\ &= \dots = r_k b^k + r_{k-1} b^{k-1} + \dots + r_1 b + r_0 = \sum_{j=0}^k r_j b^j \end{aligned}$$

# Sistemas de numeración

## Ejemplos

- $5413 = 5 \cdot 10^3 + 4 \cdot 10^2 + 1 \cdot 10 + 3 = (5413)_{10}$ .
- Si queremos representar 11 en base 2 (binario) hacemos

$$11 = 5 \cdot 2 + 1$$

$$5 = 2 \cdot 2 + 1$$

$$2 = 1 \cdot 2 + 0$$

$$1 = 0 \cdot 2 + 1$$

y por lo tanto sabemos que  $11 = 1 \cdot 2^3 + 0 \cdot 2^2 + 1 \cdot 2 + 1 = (1011)_2$ .

- El número  $(10110)_2$  podemos pasarlo a base 10 (decimal) como sigue

$$(10110)_2 = 1 \cdot 2^4 + 0 \cdot 2^3 + 1 \cdot 2^2 + 1 \cdot 2 + 0 = 16 + 4 + 2 = 22.$$



# Máximo común divisor

## Definiciones

- Sean  $a, b \in \mathbb{Z}$ . Decimos que  $d \in \mathbb{Z}$  es un **divisor común** (o factor común) de  $a$  y  $b$  si se tiene que  $d \mid a$  y  $d \mid b$ .
- Sean  $a, b \in \mathbb{Z}$ , no ambos nulos. Llamamos **máximo común divisor** de  $a$  y  $b$ , y lo denotamos por  $\text{mcd}(a, b)$ , al mayor de los divisores comunes de  $a$  y  $b$ . Es decir,  $d = \text{mcd}(a, b)$  si y sólo si
  - ▶  $d \mid a$  y  $d \mid b$  (ie.  $d$  es divisor común).
  - ▶  $\forall d' \in \mathbb{Z}$  tal que  $d' \mid a$  y  $d' \mid b$  entonces se tiene que  $d' \leq d$  (ie.  $d$  es el mayor de los divisores comunes).

## Teorema (Máximo común divisor)

*Sean  $a, b \in \mathbb{Z}$ , no ambos nulos. Existe  $d = \text{mcd}(a, b)$  y es único.*

# Máximo común divisor

## Demostración.

- **Existencia.** Sean  $X$  e  $Y$  dos conjuntos formados por los divisores positivos de  $a$  y  $b$ , respectivamente. El conjunto de los divisores comunes de  $a$  y  $b$  es  $X \cap Y \subseteq \mathbb{Z}$  y verifica que:  $X \cap Y \neq \emptyset$  puesto que  $1 \in X$  y  $1 \in Y$ , y además  $X \cap Y$  está acotado superiormente puesto que  $X$  e  $Y$  están ambos acotados superiormente por  $a$  y  $b$ , respectivamente. El axioma de buena ordenación garantiza entonces la existencia de un último elemento que será  $\text{mcd}(a, b)$ .
- **Unicidad.** Suponemos que existen  $d$  y  $d'$  tales que  $d \mid a$ ,  $d \mid b$ ,  $d' \mid a$  y  $d' \mid b$ , es decir,  $d$  y  $d'$  son ambos divisores comunes de  $a$  y  $b$ . Si  $d = \text{mcd}(a, b)$  se tiene entonces que  $d' \leq d$ , y si  $d' = \text{mcd}(a, b)$  se tiene también que  $d \leq d'$ , y por lo tanto  $d = d'$ .



# Máximo común divisor

**Propiedades.** Sean  $a, b \in \mathbb{Z}$ , se verifica que:

- $\text{mcd}(a, b) = \text{mcd}(b, a) = \text{mcd}(-a, b) = \text{mcd}(a, -b) = \text{mcd}(-a, -b)$ .
- $\text{mcd}(a, a) = \text{mcd}(a, 0) = a$ .

Sean  $a_1, a_2, \dots, a_k \in \mathbb{Z}$ , se verifica que:

- $\text{mcd}(a_1, a_2, \dots, a_k) = \text{mcd}(\text{mcd}(a_1, a_2), a_3, \dots, a_k)$ .

## Observación.

Como veremos más adelante, fundamentado en la primera de las propiedades, calcularemos siempre el  $\text{mcd}(a, b)$  asumiendo que  $a > b > 0$ .

# Algoritmo de Euclides

## Teorema

Sean  $a, b \in \mathbb{Z}$ , no ambos nulos, tales que  $a = qb + r$ , entonces

$$\text{mcd}(a, b) = \text{mcd}(b, r)$$

cualesquiera que sean los enteros  $q, r \in \mathbb{Z}$ .

## Demostración.

Sean  $a, b, q, r \in \mathbb{Z}$  tales que  $a = qb + r$ , y sea  $d = \text{mcd}(a, b)$ . Tenemos entonces que  $d \mid a$  y  $d \mid b$ , y por lo tanto  $d \mid (a - qb) = r$ , es decir,  $d \mid r$ . Por otro lado, si existe  $c \in \mathbb{Z}$  con  $c > 0$  tal que  $c \mid b$  y  $c \mid r$ , tenemos también que  $c \mid (qb + r) = a$ , es decir,  $c \mid a$  y por lo tanto, por ser  $c$  divisor común de  $a$  y  $b$ , necesariamente  $c \mid d$ . Luego  $d = \text{mcd}(b, r)$ .  $\square$

## Algoritmo de Euclides

Sean  $a, b \in \mathbb{Z}$ , no ambos nulos, con  $a > b > 0$ . Podemos encontrar el  $\text{mcd}(a, b)$  utilizando el algoritmo de la divisibilidad como sigue.

- Dividimos  $a$  entre  $b$  y encontramos  $q_1$  y  $r_1$  tales que

$$a = q_1 b + r_1 \quad \text{con} \quad 0 \leq r_1 < b$$

y se cumple entonces que  $\text{mcd}(a, b) = \text{mcd}(b, r_1)$ .

- Dividimos ahora  $b$  entre  $r_1$  y encontramos  $q_2$  y  $r_2$  tales que

$$b = q_2 r_1 + r_2 \quad \text{con} \quad 0 \leq r_2 < r_1.$$

y se cumple ahora que  $\text{mcd}(b, r_1) = \text{mcd}(r_1, r_2)$ .

- Repitiendo el proceso obtenemos un conjunto de restos  $r_1, r_2, \dots, r_k$  con  $b > r_1 > r_2 > \dots > r_k \geq 0$ , es decir, una sucesión estrictamente decreciente de enteros positivos de forma que en algún momento  $r_n = 0$ , y tenemos entonces que

$$\text{mcd}(a, b) = \text{mcd}(b, r_1) = \dots = \text{mcd}(r_{n-1}, 0) = r_{n-1}.$$

# Algoritmo de Euclides

## Ejemplo

Calculamos mediante el algoritmo de Euclides el  $\text{mcd}(194, 70)$ .

$$\begin{aligned}\text{mcd}(194, 70) &= & 194 &= 2 \cdot 70 + 54 \\ &= \text{mcd}(70, 54) & 70 &= 1 \cdot 54 + 16 \\ &= \text{mcd}(54, 16) & 54 &= 3 \cdot 16 + 6 \\ &= \text{mcd}(16, 6) & 16 &= 2 \cdot 6 + 4 \\ &= \text{mcd}(6, 4) & 6 &= 1 \cdot 4 + 2 \\ &= \text{mcd}(4, 2) & 4 &= 2 \cdot 2 + 0 \\ &= \text{mcd}(2, 0) = 2\end{aligned}$$

# Identidad de Bezout

## Teorema

Sean  $a, b \in \mathbb{Z}$ , no ambos nulos. Existen enteros  $x$  e  $y$  tales que

$$\text{mcd}(a, b) = ax + by.$$

## Demostración.

Por el algoritmo de Euclides calculamos  $\text{mcd}(a, b)$ . Tenemos entonces que  $\text{mcd}(a, b) = \text{mcd}(b, r_1) = \dots = \text{mcd}(r_{n-1}, 0) = r_{n-1}$ , donde

$$r_{n-1} = r_{n-3} - q_{n-1} \cdot r_{n-2}.$$

Tomando la expresión anterior  $r_{n-2} = r_{n-4} - q_{n-2} \cdot r_{n-3}$  tenemos que

$$r_{n-1} = -q_{n-1}r_{n-4} + (1 + q_{n-1}q_{n-2}) \cdot r_{n-3}.$$

Tomamos entonces  $r_{n-3} = r_{n-5} - q_{n-3} \cdot r_{n-4}$  y así de forma sucesiva hasta llegar a una expresión de la forma  $r_{n-1} = a \cdot x + b \cdot y$ . □

# Algoritmo extendido de Euclides

## Ejemplo

Recordamos los pasos del algo. de Euclides para calcular  $\text{mcd}(194, 70)$ .

$$194 = 2 \cdot 70 + 54 \quad \Rightarrow \quad 54 = 194 - 2 \cdot 70$$

$$70 = 1 \cdot 54 + 16 \quad \Rightarrow \quad 16 = 70 - 1 \cdot 54$$

$$54 = 3 \cdot 16 + 6 \quad \Rightarrow \quad 6 = 54 - 3 \cdot 16$$

$$16 = 2 \cdot 6 + 4 \quad \Rightarrow \quad 4 = 16 - 2 \cdot 6$$

$$6 = 1 \cdot 4 + 2 \quad \Rightarrow \quad 2 = 6 - 1 \cdot 4$$

Encontramos ahora  $x, y \in \mathbb{Z}$  tales que  $\text{mcd}(194, 70) = 194x + 70y$ .

$$\begin{aligned} 2 &= 6 - 1 \cdot 4 \\ &= 6 - 1(16 - 2 \cdot 6) = -1 \cdot 16 + 3 \cdot 6 \\ &= -1 \cdot 16 + 3(54 - 3 \cdot 16) = 3 \cdot 54 - 10 \cdot 16 \\ &= 3 \cdot 54 - 10(70 - 1 \cdot 54) = -10 \cdot 70 + 13 \cdot 54 \\ &= -10 \cdot 70 + 13(194 - 2 \cdot 70) = \underbrace{13}_{x} \cdot 194 - \underbrace{36}_{y} \cdot 70 \end{aligned}$$



# Números coprimos

## Definiciones

- Decimos que dos enteros  $a$  y  $b$  son **coprimos** (primos entre sí o primos relativos) si y sólo si  $\text{mcd}(a, b) = 1$ .
- En el caso de un conjunto de  $k$  enteros,  $a_1, a_2, \dots, a_k \in \mathbb{Z}$ , decimos:
  - ▶  $a_1, a_2, \dots, a_k$  son **coprimos** si y sólo si  $\text{mcd}(a_1, a_2, \dots, a_k) = 1$ .
  - ▶  $a_1, a_2, \dots, a_k$  son **mutuamente coprimos** (o coprimos dos a dos) si y sólo si  $\text{mcd}(a_i, a_j) = 1 \quad \forall i, j \in \{1, 2, \dots, k\}, i \neq j$ .

**Propiedades.** Sean  $a, b, c \in \mathbb{Z}$ . Se verifica que:

- Si  $a$  y  $b$  son coprimos,  $a \mid b$  y  $b \mid c$ , entonces  $(ab) \mid c$ .
- Si  $a$  y  $b$  son coprimos y  $a \mid (bc)$ , entonces  $a \mid c$ .

Sean  $a_1, a_2, \dots, a_k \in \mathbb{Z}$ . Se verifica que:

- Si  $a_1, a_2, \dots, a_k$  son mutuamente coprimos, entonces  $a_1, a_2, \dots, a_k$  son coprimos. El recíproco no siempre es cierto.

# Lema de Euclides

## Teorema

Sean  $a, b, c \in \mathbb{Z}$  tales que  $a \mid (bc)$  y  $\text{mcd}(a, b) = 1$ . Entonces  $a \mid c$ .

## Demostración.

Supongamos que  $\text{mcd}(a, b) = 1$ . Entonces existen  $x, y \in \mathbb{Z}$  tales que

$$ax + by = 1.$$

Tenemos también entonces que

$$cax + cby = c.$$

Puesto que  $a \mid (bc)$  tenemos entonces que  $a \mid (cby)$ , y como  $a \mid (cax)$  tenemos finalmente que  $a \mid (cax + cby)$ , y por lo tanto  $a \mid c$ . □

# Mínimo común múltiplo

## Definiciones

- Sean  $a, b \in \mathbb{Z}$ . Decimos que  $m \in \mathbb{Z}$  es un **múltiplo común** de  $a$  y  $b$  si se tiene que  $a = m \cdot n$  y  $b = m \cdot k$  para algún  $n, k \in \mathbb{Z}$ .
- Sean  $a, b \in \mathbb{Z}$ , no ambos nulos. Llamamos **mínimo común múltiplo** de  $a$  y  $b$ , y lo denotamos por  $\text{mcm}(a, b)$ , al menor de los múltiplos comunes positivos de  $a$  y  $b$ . Es decir,  $m = \text{mcm}(a, b)$  si y sólo si
  - ▶  $a = m \cdot n$  y  $b = m \cdot k$  (ie.  $m$  es múltiplo común).
  - ▶  $\forall m' \in \mathbb{Z}$  tal que  $a = m' \cdot n'$  y  $b = m' \cdot k'$  entonces se tiene que  $m' \geq m$  (ie.  $m$  es el mayor de los múltiplos comunes).

## Teorema (Mínimo común múltiplo)

Sean  $a, b \in \mathbb{Z}$ , no ambos nulos. Existe  $m = \text{mcm}(a, b)$  y es único.

**Observación.** Sean  $a, b \in \mathbb{Z}$  con  $a, b > 0$ ,  $d = \text{mcd}(a, b)$ ,  $m = \text{mcm}(a, b)$ . Se verifica entonces que:

$$dm = ab.$$

# Ecuaciones diofánticas

Una **ecuación diofántica** es una ecuación de la forma

$$ax + by = c$$

donde  $a, b, c \in \mathbb{Z}$  son enteros conocidos, y  $x, y \in \mathbb{Z}$  son las incógnitas de la ecuación.

## Teorema

*La ecuación diofántica  $ax + by = c$  tiene solución en  $\mathbb{Z}$  si y sólo si  $d = \text{mcd}(a, b) \mid c$ , en cuyo caso existen infinitas soluciones. Todas las soluciones son:*

$$x = x_0 + \frac{b}{d}t \quad y = y_0 - \frac{a}{d}t \quad \forall t \in \mathbb{Z},$$

*donde  $x_0, y_0$  es una solución particular de la ecuación diofántica.*

# Ecuaciones diofánticas

## Demostración.

Supongamos que la ecuación  $ax + by = c$  tiene solución y sea  $d = \text{mcd}(a, b)$ . Es claro entonces que  $d \mid a$  y  $d \mid b$ , y por lo tanto  $d \mid (ax + by)$ , es decir,  $d \mid c$ . Recíprocamente, sea  $d = \text{mcd}(a, b)$ , por la identidad de Bezout existen enteros  $x', y' \in \mathbb{Z}$  tales que  $ax' + by' = d$ . Supongamos que  $d \mid c$ , es decir, existe  $e \in \mathbb{Z}$  tal que  $c = de$ . Tenemos entonces que

$$a(x'e) + b(y'e) = de = c$$

Por lo tanto,  $x = x'e$  e  $y = y'e$  es una solución particular de la ecuación  $ax + by = c$ . Digamos  $x_0 = x'e$  e  $y_0 = y'e$ .

# Ecuaciones diofánticas

## Demostración.

Sea  $x$  e  $y$  otra solución particular de la ecuación  $ax + by = c$ . Tenemos entonces que

$$a(x - x_0) + b(y - y_0) = 0.$$

Hacemos

$$\frac{a}{d}(x - x_0) = \frac{b}{d}(y_0 - y).$$

Tenemos entonces que  $\frac{a}{d} \mid \frac{b}{d}(y_0 - y)$ , y puesto que  $\text{mcd}(\frac{a}{d}, \frac{b}{d}) = 1$  por el lema de Euclides tenemos que  $\frac{a}{d} \mid (y_0 - y)$ , es decir,  $\frac{a}{d}t = (y_0 - y)$  para  $t \in \mathbb{Z}$ , o equivalentemente  $y = y_0 - \frac{a}{d}t$ . Sustituyendo  $y$  en la expresión anterior queda

$$\frac{a}{d}(x - x_0) = \frac{b}{d}(y_0 - y_0 + \frac{a}{d}t) \Rightarrow x = x_0 + \frac{b}{d}t.$$

Es decir, todas las soluciones son  $x = x_0 + \frac{b}{d}t$ ,  $y = y_0 - \frac{a}{d}t$ ,  $\forall t \in \mathbb{Z}$ . □

# Ecuaciones diofánticas

## Ejemplo

Consideramos la ecuación  $194x + 70y = 8$ .

- Mediante el algoritmo de Euclides encontramos que  $\text{mcd}(194, 70) = 2$  y puesto que  $2 \mid 8$  sabemos que la ecuación dada tiene solución.
- Mediante el algoritmo extendido de Euclides encontramos una solución particular. Tenemos que  $194 \cdot 13 + 70 \cdot (-36) = 2$ . Luego multiplicando ambos lados de la igualdad por 4 obtenemos una solución particular de la ecuación dada:  $x_0 = 52$ ,  $y_0 = -144$ .
- Todas las soluciones de la ecuación son

$$\begin{cases} x = 52 + \frac{70}{2}t = 52 + 35t \\ y = -144 - \frac{194}{2}t = -144 - 97t \end{cases} \quad \forall t \in \mathbb{Z}$$

# Números primos

## Definiciones

- Decimos que un entero  $p$  con  $p > 1$  es **primo** si los únicos divisores positivos de  $p$  son 1 y el propio  $p$ .
- En caso contrario, decimos que  $p$  es compuesto. Es decir, un entero  $n$  con  $n > 1$  es **compuesto** si existen  $a, b \in \mathbb{Z}$  con  $1 < a < n < y$   
 $1 < b < n$  tales que  $n = ab$ .

**Propiedades.** Sea  $p \in \mathbb{Z}$  un número primo. Se verifica entonces que:

- Si  $a \in \mathbb{Z}$ , entonces  $p \mid a$  o  $p$  y  $a$  son coprimos.
- Si  $a, b \in \mathbb{Z}$  y  $p \mid (ab)$ , entonces  $p \mid a$  o  $p \mid b$ .



# Números primos

## Teorema (Teorema fundamental de la aritmética)

Todo entero  $p$  con  $p > 1$  admite una descomposición en factores primos

$$n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k},$$

donde  $p_1, p_2, \dots, p_k$  son primos distintos y  $e_1, e_2, \dots, e_k$  son enteros positivos. Esta factorización es única, independientemente del orden de los factores.

**Observación.** Sean  $a = p_1^{e_1} \cdots p_k^{e_k}$  y  $b = p_1^{f_1} \cdots p_k^{f_k}$ . Se verifica que:

- $ab = p_1^{e_1+f_1} \cdots p_k^{e_k+f_k}$
- $a^b = p_1^{e_1 \cdot b} \cdots p_k^{e_k \cdot b}$
- $\text{mcd}(ab) = p_1^{\min(e_1, f_1)} \cdots p_k^{\min(e_k, f_k)}$

# Números primos

## Demostración.

- **Existencia.** Sea  $S \subseteq \mathbb{N} \setminus \{1\}$  el conjunto de enteros que no admiten una descomposición en factores primos. Por reducción al absurdo, supongamos que  $S \neq \emptyset$ . Por el axioma de buena ordenación existe un primer entero  $n_0 = \min S$ . Entonces,  $n_0$  no es primo y por lo tanto existen enteros  $a, b \in \mathbb{N} \setminus \{1\}$  con  $a, b < n_0$  tal que  $n_0 = ab$ . Puesto que  $a, b \notin S$  ambos se pueden expresar como producto de factores primos como

$$a = p_1 p_2 \cdots p_k, \quad b = q_1 q_2 \cdots q_l.$$

Por lo tanto, podríamos expresar  $n_0$  como producto de factores primos,  $n_0 = p_1 \cdots p_k q_1 \cdots q_l$  lo que contradice la hipótesis de partida.

# Números primos

## Demostración.

- **Unicidad.** Sea  $T \subseteq \mathbb{N} \setminus \{1\}$  el conjunto de enteros que no admiten una descomposición única en factores primos. Por reducción al absurdo, supongamos que  $T \neq \emptyset$ . Por el axioma de buena ordenación existe un primer entero  $m_0 = \min T$ , tal que

$$m_0 = p_1 \cdots p_k = q_1 \cdots q_l,$$

con  $p_i, q_j \in \mathbb{N} \setminus \{1\}$ ,  $p_i, q_j < m_0$  para todo  $i, j$ . Ahora, como  $p_1 \mid m_0$  se tiene que  $p_1 \mid q_1 \cdots q_l$  y por lo tanto  $p_1 \mid q_i$  para algún  $i \in \{1, \dots, l\}$ . Supongamos sin pérdida de generalidad que  $p_1 \mid q_1$ . Como  $p_1$  y  $q_1$  son ambos primos tenemos necesariamente que  $p_1 = q_1$ . Queda entonces  $m_1 = p_2 \cdots p_k = q_2 \cdots q_l$ , pero como  $m_1 \notin T$  se contradice la hipótesis de partida.



# Números primos

## Teorema (Teorema de Euclides)

*Existen infinitos números primos.*

### **Demostración.**

Supongamos que existe un número finito de números primos, por ejemplo, los primos  $p_1, p_2, \dots, p_k$ . Sea  $m = p_1 p_2 \cdots p_k + 1$ . Puesto que  $m > 1$  por el teorema fundamental de la aritmética  $m$  es divisible por algún primo, digamos  $p \in \{p_1, \dots, p_k\}$ . Luego  $p \mid m$  y  $p \mid p_1 p_2 \cdots p_k$ , por lo que  $p$  debe dividir también a  $m - p_1 p_2 \cdots p_k = 1$ , lo que es imposible.  $\square$

# Criba de Eratóstenes

## Teorema (Proposición de Fermat)

*Un entero  $n \in \mathbb{Z}$  con  $n > 1$  es compuesto si y sólo si es divisible por algún primo  $p \leq \sqrt{n}$ .*

**Criba de Eratóstenes.** Se trata de un método para obtener los números primos menores que  $n$

- Escribimos la lista de enteros  $2, 3, \dots, n$ .
- Marcamos el primer entero de la lista 2 como primo, y tachamos todos los múltiplos de 2.
- Buscamos el siguiente entero de la lista no tachado, lo marcamos, y tachamos todos los múltiplos de ese primo.
- Repetimos el mismo procedimiento hasta haber marcado o tachado todos los elementos de la lista.