

# ÀLGEBRA

Resums de la primera part

Mercè Mora

Facultat d'Informàtica de Barcelona. UPC.

Curs 2006-2007/Q1

---

1. Lògica i raonament
2. Conjunts
3. Aplicacions
4. Comptar
5. Aritmètica

# 1. LÒGICA I RAONAMENT (I). PROPOSICIONS

- *Proposició.* Afirmació que és falsa o certa, però no les dues coses alhora.

▷ Exemples. "Avui plou", "El quadrat de 2 és 5" són proposicions. " $x > 2$ ", "Has llegit aquest llibre?", "Mira!" no són proposicions.

- *Valors de veritat.* Una proposició pren el valor 1 si és certa i 0 si és falsa.

- *Variable proposicional.* Representa una proposició arbitrària, amb un valor de veritat no determinat. Normalment utilitzarem les lletres  $p$ ,  $q$ ,  $r$ , ... per a representar proposicions arbitràries.

- *Connectius lògics.* Serveixen per combinar proposicions i formar-ne de noves.

## 1. LÒGICA I RAONAMENT (II). CONNECTIUS

- *Connectiu*  $\neg$ . Equival a *no* en llenguatge natural.  $\neg p$  és una proposició certa si  $p$  és falsa, i falsa si  $p$  és certa.
- *Connectiu*  $\wedge$ . Equival a *i* en llenguatge natural.  $p \wedge q$  és una proposició certa si  $p$  i  $q$  són certes, i falsa si alguna de les dues és falsa.
- *Connectiu*  $\vee$ . Equival a *o* (inclusiu) en llenguatge natural.  $p \vee q$  és una proposició certa si  $p$  és certa o si  $q$  és certa, i falsa si  $p$  i  $q$  són falses.
- *Connectiu*  $\rightarrow$ . Equival a *Si... llavors...* en llenguatge natural.  $p \rightarrow q$  és una proposició certa si  $p$  és falsa o  $q$  és certa, i és falsa si  $p$  és certa i  $q$  és falsa.

# 1. LÒGICA I RAONAMENT (III). CONNECTIUS

- *Connectiu*  $\leftrightarrow$ . Equival a ...*si, i només si*,... en llenguatge natural.  $p \leftrightarrow q$  és una proposició certa si les dues són certes o les dues són falses, i és falsa si una és certa i l'altra falsa.
- *Connectiu*  $\oplus$ . Equival a *O bé...o bé...* (o exclusiu) en llenguatge natural.  $p \oplus q$  és una proposició certa si una és falsa i l'altra és certa, i és falsa si les dues són certes o les dues són falses.
- *Taules de veritat*. Donen el valor de veritat de proposicions obtingudes amb connectius lògics en funció dels valors de veritat de les variables proposicionals.

$p$	$\neg p$	$p$	$q$	$p \wedge q$	$p \vee q$	$p \rightarrow q$	$p \leftrightarrow q$	$p \oplus q$
0	1	0	0	0	0	1	1	0
0	1	0	1	0	1	1	0	1
1	0	0	0	0	1	0	0	1
1	0	1	1	1	1	1	1	0

*Taules de veritat de connectius lògics*

# 1. LÒGICA I RAONAMENT (IV). TAUTOLOGIES

- *Tautologia*. Proposició certa per a qualsevol valor que prenguin les variables proposicionals. És a dir, tots els valors de la taula de veritat d'una tautologia són 1.

▷ Exemple.  $p \vee \neg p$

- *Contradicció*. Proposició falsa per a qualsevol valor que prenguin les variables proposicionals. És a dir, tots els valors de la taula de veritat d'una contradicció són 0.

▷ Exemple.  $p \wedge \neg p$

▶ *Algunes tautologies.*

$$p \rightarrow p \vee q$$

$$p \wedge q \rightarrow p$$

$$((p \rightarrow q) \wedge p) \rightarrow q$$

$$((p \rightarrow q) \wedge \neg q) \rightarrow \neg p$$

$$((p \vee q) \wedge \neg p) \rightarrow q$$

$$((p \rightarrow q) \wedge (q \rightarrow r)) \rightarrow (p \rightarrow r)$$

# 1. LÒGICA I RAONAMENT (V). EQUIVALÈNCIA LÒGICA

• *Equivalència lògica.* Dues proposicions són *lògicament equivalents* si tenen la mateixa taula de veritat.

▷ Notació. Escrivem  $p \Leftrightarrow q$  si les proposicions  $p$ ,  $q$  són lògicament equivalents.

▶ Algunes equivalències lògiques.

$$\neg(\neg p) \Leftrightarrow p \text{ (doble negació)}$$

$$p \wedge q \Leftrightarrow q \wedge p \text{ (commutativitat)}$$

$$p \vee q \Leftrightarrow q \vee p \text{ (commutativitat)}$$

$$p \wedge (q \wedge r) \Leftrightarrow (p \wedge q) \wedge r \text{ (associativitat)}$$

$$p \vee (q \vee r) \Leftrightarrow (p \vee q) \vee r \text{ (associativitat)}$$

$$p \wedge (q \vee r) \Leftrightarrow (p \wedge q) \vee (p \wedge r) \text{ (distributivitat)}$$

$$p \vee (q \wedge r) \Leftrightarrow (p \vee q) \wedge (p \vee r) \text{ (distributivitat)}$$

$$\neg(p \wedge q) \Leftrightarrow \neg p \vee \neg q \text{ (Llei de De Morgan)}$$

$$\neg(p \vee q) \Leftrightarrow \neg p \wedge \neg q \text{ (Llei de De Morgan)}$$

$$p \rightarrow q \Leftrightarrow \neg p \vee q, \quad \neg(p \rightarrow q) \Leftrightarrow p \wedge \neg q$$

$$p \rightarrow q \Leftrightarrow \neg q \rightarrow \neg p \text{ (contrarecíproc)}$$

## 1. LÒGICA I RAONAMENT (VI). PREDICATS

- *Predicat*. Afirmació que depèn d'una o més variables.  
▷ Notació.  $P(x)$ ,  $P(x, y)$ , etc.
- *Univers de discurs*. Conjunt  $U$  no buit de valors que poden prendre les variables d'un predicat.
- *Quantificadors*  $\forall$ ,  $\exists$ ,  $\exists!$ .  
 $\forall xP(x)$  equival a "per a tot valor de  $x$ ,  $P(x)$ "  
 $\exists xP(x)$  equival a "existeix un valor  $x$  tal que  $P(x)$ "  
 $\exists! xP(x)$  equival a "existeix un únic valor  $x$  tal que  $P(x)$ "

## 1. LÒGICA I RAONAMENT (VII). PREDICATS

▷ *Exemple:* Formalització de predicats. Si  $U = \mathbb{C}$ ,

El quadrat de tot nombre real és positiu:  $\forall x(x \in \mathbb{R} \rightarrow x^2 \geq 0)$

Existeix un nombre real tal que el seu quadrat és 2:

$$\exists x(x \in \mathbb{R} \wedge x^2 = 2)$$

Existeix un únic nombre natural tal que el seu quadrat és 4:

$$\exists! x(x \in \mathbb{N} \wedge x^2 = 4)$$

▷ *Exemple.* Si  $U = \{a, b, c\}$ , llavors:

$$\forall xP(x) \text{ equival a } P(a) \wedge P(b) \wedge P(c)$$

$$\exists xP(x) \text{ equival a } P(a) \vee P(b) \vee P(c)$$

$$\exists! xP(x) \text{ equival a } (P(a) \wedge \neg P(b) \wedge \neg P(c)) \vee$$

$$\vee (\neg P(a) \wedge P(b) \wedge \neg P(c)) \vee (\neg P(a) \wedge \neg P(b) \wedge P(c))$$

# 1. LÒGICA I RAONAMENT (VIII). PREDICATS

► Negació d'expressions amb quantificadors.

$\neg\forall xP(x)$  és equivalent a  $\exists x\neg P(x)$ .

$\neg\exists xP(x)$  és equivalent a  $\forall x\neg P(x)$

► Commutativitat dels quantificadors.

$\forall x\forall yP(x, y) \Leftrightarrow \forall y\forall xP(x, y)$

$\exists x\exists yP(x, y) \Leftrightarrow \exists y\exists xP(x, y)$

$\forall x\exists yP(x, y)$  i  $\exists y\forall xP(x, y)$  NO són equivalents.

## 1. LÒGICA I RAONAMENT (IX). PREDICATS

► Un predicat amb totes les variables quantificades o substituïdes per valors concrets de l'univers de discurs és una proposició.

- La proposició  $\forall xP(x)$  és certa si el predicat  $P(x)$  és cert per a tot valor de  $x \in U$ .
- La proposició  $\exists xP(x)$  és certa si el predicat  $P(x)$  és cert per a almenys un valor de  $x \in U$ .
- La proposició  $\exists!xP(x)$  és certa si el predicat  $P(x)$  és cert per a un i només un valor de  $x \in U$ .

## 1. LÒGICA I RAONAMENT (X)

- *Axioma*. Proposició que assumim certa en una teoria determinada.
  - *Teorema*. Afirmació que es pot provar que és certa en una teoria determinada.
  - *Demostració*. Argument per a provar un teorema. S'utilitzen regles d'inferència que es deriven de tautologies.
- ▷ Notació. Escrivem  $p \Rightarrow q$  si es pot deduir la certesa de  $q$  a partir de la certesa de  $p$ , és a dir, si la proposició  $p \rightarrow q$  és certa.

# 1. LÒGICA I RAONAMENT (XI). REGLES D'INFERÈNCIA

► Tautologia:  $p \rightarrow p \vee q$ . Regla d'inferència (*addició*):

De  $p$  certa, deduïm que  $p \vee q$  és certa.

► Tautologia:  $p \wedge q \rightarrow p$ . Regla d'inferència (*simplificació*):

De  $p \wedge q$  certa, deduïm que  $p$  és certa.

► Tautologia:  $((p \rightarrow q) \wedge p) \rightarrow q$ . Regla d'inferència (*modus ponens*): De  $p \rightarrow q$  i  $p$  certes, deduïm que  $q$  és certa.

► Tautologia:  $((p \rightarrow q) \wedge \neg q) \rightarrow \neg p$ . Regla d'inferència (*modus tollens*): De  $p \rightarrow q$  i  $\neg q$  certes, deduïm que  $\neg p$  és certa.

## 1. LÒGICA I RAONAMENT (XII). REGLES D'INFERÈNCIA

► Tautologia:  $((p \vee q) \wedge \neg p) \rightarrow q$ . Regla d'inferència (*sil·logisme disjuntiu*): De  $p \vee q$  i  $\neg p$  certes, deduïm que  $q$  és certa.

► Tautologia:  $((p \rightarrow q) \wedge (q \rightarrow r)) \rightarrow (p \rightarrow r)$ . Regla d'inferència (*sil·logisme hipotètic*): De  $p \rightarrow q$  i  $q \rightarrow r$  certes, deduïm que  $p \rightarrow r$  és certa.

► Errors més freqüents (*fallàcies*).

De  $p \rightarrow q$  i  $q$  certes, NO es pot deduir que  $p$  sigui certa.

De  $p \rightarrow q$  i  $\neg p$  certes, NO es pot deduir que  $\neg q$  sigui certa.

# 1. LÒGICA I RAONAMENT (XIII). DEMOSTRACIÓ DE $p \rightarrow q$

► Com demostrar  $p \rightarrow q$ .

1. *Provar que  $p$  és sempre falsa.* Si  $p$  és falsa, llavors la implicació  $p \rightarrow q$  és certa.

2. *Provar que  $q$  és sempre certa.* Si  $q$  és certa, llavors la implicació  $p \rightarrow q$  és certa

3. *Prova directa.* Deduir  $q$  a partir de  $p$ .

4. *Contrarecíproc.* És equivalent a demostrar  $\neg q \rightarrow \neg p$

5. *Reducció a l'absurd.* És equivalent a deduir una contradicció a partir de  $p \wedge \neg q$

6. *Demostració per casos.*  $(p_1 \vee p_2 \vee \dots \vee p_r) \rightarrow q$  és equivalent a demostrar  $p_1 \rightarrow q$  i  $p_2 \rightarrow q$  i ... i  $p_r \rightarrow q$

## 1. LÒGICA I RAONAMENT (XIV). DEMOSTRACIONS

- ▶ Demostrar  $p \rightarrow (q \wedge r)$  equival a demostrar  $p \rightarrow q$  i  $p \rightarrow r$ .
- ▶ Demostrar  $p \rightarrow (q \vee r)$  equival a demostrar  $(p \wedge \neg q) \rightarrow r$ .
- ▶ Demostrar  $p \leftrightarrow q$  equival a demostrar  $p \rightarrow q$  i  $q \rightarrow p$
- ▶ Demostrar que les condicions  $p_1, p_2, \dots, p_r$  són equivalents equival a demostrar  $p_1 \leftrightarrow p_2 \leftrightarrow \dots \leftrightarrow p_r$ , o bé  $p_1 \rightarrow p_2 \rightarrow \dots \rightarrow p_r \rightarrow p_1$ .

# 1. LÒGICA I RAONAMENT (XV). DEMOSTRACIONS I QUANTIFICADORS

► Demostració de  $\forall xP(x)$ .

▷ Fer una demostració genèrica de  $P(x)$ , és a dir, que sigui vàlida per a qualsevol valor de  $x$ .

▷ Reducció a l'absurd: arribar a contradicció a partir de  $\exists x\neg P(x)$

► Demostració de  $\exists xP(x)$ .

▷ Trobar un element concret  $c$  tal que la proposició  $P(c)$  sigui certa

▷ Reducció a l'absurd: arribar a contradicció a partir de  $\forall x\neg P(x)$

► Demostrar  $\neg\forall xP(x)$  és equivalent a demostrar  $\exists x\neg P(x)$ . En aquest cas, si  $c$  és tal que la proposició  $\neg P(c)$  és certa, direm que  $c$  és un *contraexemple* de  $\forall xP(x)$

► Demostrar  $\neg\exists xP(x)$  és equivalent a demostrar  $\forall x\neg P(x)$

## 1. LÒGICA I RAONAMENT (XVI). PRINCIPI D'INDUCCIÓ SIMPLE

► Considerem una propietat  $P(n)$  que depèn de  $n \in \mathbb{Z}$ , i  $n_0 \in \mathbb{Z}$ .

Si es compleixen les dues condicions següents:

1.  $P(n_0)$  és certa,

2.  $\forall n \geq n_0, (P(n) \text{ certa} \implies P(n+1) \text{ certa})$ ,

llavors  $\forall n \geq n_0, P(n)$  és certa.

► Considerem una propietat  $P(n)$  que depèn de  $n \in \mathbb{Z}$ , i  $n_0 \in \mathbb{Z}$ .

Si es compleixen les dues condicions següents:

1.  $P(n_0)$  és certa,

2.  $\forall n > n_0, (P(n-1) \text{ certa} \implies P(n) \text{ certa})$ ,

llavors  $\forall n \geq n_0, P(n)$  és certa.

## 1. LÒGICA I RAONAMENT (XVII). PRINCIPI D'INDUCCIÓ COMPLETA

► Considerem una propietat  $P(n)$  que depèn de  $n \in \mathbb{Z}$ , i  $n_0 \in \mathbb{Z}$ .  
Si es compleixen les dues condicions següents:

1.  $P(n_0)$  és certa,
  2.  $\forall n > n_0, ((\forall k, n_0 \leq k < n, P(k) \text{ certa}) \implies P(n) \text{ certa})$ ,
- llavors  $\forall n \geq n_0, P(n)$  és certa.

## 2. CONJUNTS (I)

- *Conjunt*: col·lecció d'objectes, que anomenem *elements* del conjunt.

- ▷ Terminologia: un element *pertany* a un conjunt o *està contingut* a un conjunt; un conjunt *conté* un element;

- ▷ Notació: escriurem  $a \in A$  si  $a$  és un element del conjunt  $A$  i  $a \notin A$  si no ho és

- Conjunts *iguals*: tenen els mateixos elements.

- ▷ Observació: a un conjunt no hi ha elements repetits, ni es té en compte l'ordre dels elements

- Conjunt *buit*: no conté cap element

- ▷ Notació:  $\emptyset$  o bé  $\{\}$  representen el conjunt buit

## 2. CONJUNTS (II)

- Descripció d'un conjunt.

Per extensió: enumerem tots els seus elements.

▷ Exemple.  $A = \{1, 30, \emptyset, \otimes, *, 2/3\}$

Per comprensió: donem una propietat que caracteritza els elements del conjunt.

▷ Exemple.  $A = \{x \mid x = 3k, k \in \mathbb{Z}\}$

- Conjunts numèrics:

$$\mathbb{N} = \{0, 1, 2, \dots\}$$

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

$$\mathbb{Q} = \{p/q \mid p, q \in \mathbb{Z}, q \neq 0\}$$

$\mathbb{R}$  conjunt format per tots els nombres reals

$\mathbb{C}$  conjunt format per tots els nombres complexos

## 2. CONJUNTS (III). SUBCONJUNTS

- $B$  és un *subconjunt* de  $A$  si tot element de  $B$  és de  $A$ 
  - ▷ Notació: escriurem  $B \subset A$  ó  $B \subseteq A$  si  $B$  és subconjunt de  $A$ ;  
 $B \not\subset A$  si  $B$  no és subconjunt de  $A$ ;  $B \subsetneq A$  si  $B \subset A$  i  $A \neq B$

▶  $B \subset A \iff (\forall x)(x \in B \Rightarrow x \in A)$

▶  $\emptyset \subset A$ , per a tot conjunt  $A$

▶  $A = B \iff A \subset B$  i  $B \subset A$

▶  $A = B \iff (\forall x)(x \in A \Rightarrow x \in B$  i  $x \in B \Rightarrow x \in A)$

- Conjunt de les parts:  $\mathcal{P}(A) = \{B \mid B \subset A\}$ 
  - ▶  $\emptyset \in \mathcal{P}(A)$  i  $A \in \mathcal{P}(A)$ , per a tot conjunt  $A$

## 2. CONJUNTS (IV). CARDINAL

• Cardinal d'un conjunt: si existeix un natural  $n$  tal que  $A$  té  $n$  elements direm que  $A$  és un conjunt *finit de cardinal  $n$*  o bé que  $A$  és un  $n$ -conjunt. Un conjunt és *infinit* si no és finit.

▷ Notació:  $\#A$ ,  $|A|$

Exemples:  $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$  són infinits;

$\{x \mid x \in \mathbb{Z}, -203 \leq x \leq 1078\}$  és finit.

► Si  $A$  és un conjunt finit,

1)  $B \subseteq A \Rightarrow |B| \leq |A|$

2)  $B \subsetneq A \Rightarrow |B| < |A|$

3)  $B \subseteq A \Rightarrow (|B| = |A| \Leftrightarrow A = B)$

►  $|A| = n \Rightarrow |\mathcal{P}(A)| = 2^n$

## 2. CONJUNTS (V). PRODUCTE CARTESIÀ

- *Parell ordenat*: element de la forma  $(a, b)$

Igualtat de parells ordenats:  $(a, b) = (c, d) \Leftrightarrow a = c$  i  $b = d$

- *Producte cartesià* dels conjunts  $A$  i  $B$ :

$$A \times B = \{(a, b) | a \in A, b \in B\}$$

► Si  $A$  i  $B$  són finits,  $|A \times B| = |A| \cdot |B|$

- *n-pla ordenada*: element de la forma  $(a_1, a_2, \dots, a_n)$

Igualtat de n-ples ordenades:  $(a_1, a_2, \dots, a_n) = (b_1, b_2, \dots, b_n) \Leftrightarrow a_i = b_i, \forall i \in \{1, 2, \dots, n\}$

- *Producte cartesià* dels conjunts  $A_1, A_2, \dots, A_n$ :

$$A_1 \times \dots \times A_n = \{(a_1, \dots, a_n) | a_1 \in A_1, \dots, a_n \in A_n\}$$

► Si  $A_1, \dots, A_n$  són finits,  $|A_1 \times A_2 \times \dots \times A_n| = |A_1| \cdot |A_2| \cdot \dots \cdot |A_n|$

## 2. CONJUNTS (VI). INTERSECCIÓ

• La *intersecció* dels conjunts  $A$  i  $B$  és el conjunt format per tots els elements que són alhora de  $A$  i de  $B$ . La *intersecció* dels conjunts  $A_i, i \in I$ , és el conjunt format pels elements que són alhora de tots els conjunts  $A_i, i \in I$ .

▷ Notació:  $A \cap B = \{x \mid x \in A \text{ i } x \in B\}$

$$\bigcap_{i \in I} A_i = \{x \mid \forall i \in I, x \in A_i\}$$

► Si  $A, B, C$  són conjunts amb elements d' $U$ , conjunt universal,

$$A \cap A = A$$

$$A \cap B \subset A, A \cap B \subset B$$

$$A \cap \emptyset = \emptyset, A \cap U = A$$

$$A \cap B = B \cap A$$

$$A \cap (B \cap C) = (A \cap B) \cap C$$

$$A \subset B \iff A = A \cap B$$

► Si  $A, B$  són conjunts finits,  $|A \cap B| \leq |A|, |A \cap B| \leq |B|$

•  $A$  i  $B$  són conjunts *disjunts* si  $A \cap B = \emptyset$

## 2. CONJUNTS (VII). UNIÓ

• La *unió* dels conjunts  $A$  i  $B$  és el conjunt format per tots els elements que són de  $A$  o de  $B$ . La *unió* dels conjunts  $A_i$ ,  $i \in I$ , és el conjunt format pels elements que són d'algun dels conjunts  $A_i$ ,  $i \in I$ .

▷ Notació:  $A \cup B = \{x \mid x \in A \text{ ó } x \in B\}$

$$\bigcup_{i \in I} A_i = \{x \mid \exists i \in I, x \in A_i\}$$

► Si  $A, B, C$  són conjunts amb elements d' $U$ , conjunt universal,

$$A \cup A = A$$

$$A \subset A \cup B, B \subset A \cup B$$

$$A \cup \emptyset = A, A \cup U = U$$

$$A \cup B = B \cup A$$

$$A \cup (B \cup C) = (A \cup B) \cup C$$

$$A \subset B \iff A \cup B = B$$

$$A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$$

$$A \cup (B \cap C) = (A \cup B) \cap (A \cup C)$$

## 2. CONJUNTS (VIII). UNIÓ

► Si  $A, B$  són conjunts finits,  $|A| \leq |A \cup B|$ ,  $|B| \leq |A \cup B|$

► Si  $A$  i  $B$  són conjunts finits disjunts,  $|A \cup B| = |A| + |B|$

► Si  $A_1, \dots, A_n$  són conjunts finits disjunts dos a dos,  
 $|A_1 \cup \dots \cup A_n| = |A_1| + \dots + |A_n|$

► *Principi d'inclusió-exclusió.*

Si  $A, B$  són conjunts finits,  $|A \cup B| = |A| + |B| - |A \cap B|$

Si  $A, B, C$  són conjunts finits,

$$|A \cup B \cup C| = |A| + |B| + |C| - |A \cap B| - |A \cap C| - |B \cap C| + |A \cap B \cap C|$$

## 2. CONJUNTS (IX). DIFERÈNCIA

• La *diferència* dels conjunts  $A$  i  $B$  és el conjunt format per tots els elements que són de  $A$  i no són de  $B$ .

▷ Notació:  $A \setminus B = \{x \mid x \in A \text{ i } x \notin B\}$

▶  $A, B$  conjunts qualssevol,

$$A \setminus B \subset A$$

$$A \setminus A = \emptyset,$$

$$A \setminus \emptyset = A$$

$$A \setminus B = A \setminus (A \cap B)$$

▶ Si  $A, B$  són conjunts finits,  $|A \setminus B| = |A| - |A \cap B|$

## 2. CONJUNTS (X). COMPLEMENTARI

• El *complementari* del conjunt  $A$ , format per elements d'un conjunt universal  $U$ , és el conjunt  $U \setminus A$  format per tots els elements que no són de  $A$ .

▷ Notació:  $\bar{A} = U \setminus A = \{x \mid x \notin A\}$

▶  $A \cap \bar{A} = \emptyset, A \cup \bar{A} = U$

$$\overline{\bar{A}} = A$$

$$\overline{A \cap B} = \bar{A} \cup \bar{B}, \overline{A \cup B} = \bar{A} \cap \bar{B}$$

$$A \subseteq B \Leftrightarrow \bar{B} \subseteq \bar{A}$$

▶ Si  $A$  és un conjunt finit format per elements d'un conjunt universal  $U$ ,  $|\bar{A}| = |U| - |A|$ .

## 2. CONJUNTS (XI). DIFERÈNCIA SIMÈTRICA

• La *diferència simètrica* dels conjunts  $A$  i  $B$  és el conjunt format pels elements que són de  $A$  ó de  $B$  però no de tots dos conjunts alhora.

▷ Notació:  $A\Delta B = A\oplus B = \{x \mid x \in A \cup B \text{ i } x \notin A \cap B\}$

▶  $A\Delta B = A\oplus B = A \cup B \setminus A \cap B = (A \setminus B) \cup (B \setminus A)$

## 2. CONJUNTS (XII). REPRESENTACIÓ BINÀRIA

• Si  $U = \{x_1, x_2, \dots, x_n\}$  és un conjunt finit, associem a cada conjunt  $A \subset U$  la paraula binària  $(a_1, a_2, \dots, a_n)$  de longitud  $n$

tal que 
$$\begin{cases} a_i = 1, & \text{si } x_i \in A, \\ a_i = 0, & \text{si } x_i \notin A. \end{cases}$$

Direm que  $(a_1, a_2, \dots, a_n)$  és la *representació binària* de  $A$ .

► La representació binària de  $U$  és  $(1, 1, \dots, 1)$

La representació binària de  $\emptyset$  és  $(0, 0, \dots, 0)$

► Si les representacions binàries de  $A, B \subset U$  són respectivament  $(a_1, a_2, \dots, a_n)$  i  $(b_1, b_2, \dots, b_n)$ , llavors la representació

binària de:  $A \cap B$  és  $(\dots, a_i \wedge b_i, \dots)$

$A \cup B$  és  $(\dots, a_i \vee b_i, \dots)$

$\bar{A}$  és  $(\dots, \neg a_i, \dots)$

$A \setminus B$  és  $(\dots, a_i \wedge \neg b_i, \dots)$

$A \oplus B$  és  $(\dots, a_i \oplus b_i, \dots)$

## 2. CONJUNTS (XIII). NOMBRES BINOMIALS

• El *nombre binomial*  $\binom{n}{k}$  és el nombre de subconjunts de cardinal  $k$  d'un conjunt de cardinal  $n$ .

$$\blacktriangleright \binom{n}{0} = 1; \binom{n}{n} = 1;$$

$$\blacktriangleright \binom{n}{1} = n; \binom{n}{n-1} = n; \binom{n}{2} = \frac{n(n-1)}{2};$$

$$\blacktriangleright \binom{n}{k} = \binom{n-1}{k} + \binom{n-1}{k-1}, \text{ si } n \geq 2, 1 \leq k \leq n-1;$$

$$\blacktriangleright \binom{n}{k} = \frac{n!}{k!(n-k)!}, \text{ si } 0 \leq k \leq n.$$

## 2. CONJUNTS (XIV). NOMBRES BINOMIALS

► Teorema del binomi.  $(a + b)^n = \sum_{k=0}^n \binom{n}{k} a^k b^{n-k}$

►  $\forall n \geq 0, \sum_{k=0}^n \binom{n}{k} = 2^n$  ;  $\forall n \geq 1, \sum_{k=0}^n (-1)^k \binom{n}{k} = 0$ .

►  $\binom{n}{k} = \binom{n}{n-k}$  ;  $\binom{n}{k} = \frac{n}{k} \binom{n-1}{k-1}$ .

►  $\sum_{r=0}^k \binom{n}{r} \binom{m}{k-r} = \binom{n+m}{k}$  (Identitat de Vandermonde)

### 3. APLICACIONES (I)

- Una *aplicació*  $f$  entre dos conjunts no buits  $A$ ,  $B$  és una correspondència que a cada element de  $A$  li assigna un únic element de  $B$ .

▷ Notació:  $f : A \longrightarrow B$  representa una aplicació de  $A$  en  $B$ . Direm que  $A$  és el *conjunt de sortida* o *domini* i  $B$  el *conjunt d'arribada* de  $f$ . Escriurem  $f(a) = b$  si  $f$  assigna l'element  $b \in B$  a l'element  $a \in A$ . Direm que  $b$  és la *imatge* de  $a$  per  $f$  i que  $a$  és una *antiimatge* de  $b$  per  $f$ .

## 4. APLICACIONS (II). FUNCIONS IMPORTANTS

- Funció *part entera inferior*.  $f : \mathbb{R} \longrightarrow \mathbb{Z}$ ,  
 $f(x) = \lfloor x \rfloor = \max\{n \in \mathbb{Z} \mid n \leq x\}$
  - Funció *part entera superior*.  $f : \mathbb{R} \longrightarrow \mathbb{Z}$ ,  
 $f(x) = \lceil x \rceil = \min\{n \in \mathbb{Z} \mid n \geq x\}$
  - Funció *polinòmica*.  $f : \mathbb{R} \longrightarrow \mathbb{R}$ ,  $f(x) = a_n x^n + \dots + a_1 x + a_0$
  - Funció *exponencial*. Fixat  $a \in \mathbb{R}$ ,  $f_a : \mathbb{R} \longrightarrow \mathbb{R}$ ,  $f_a(x) = a^x$
  - Funció *logarítmica*. Fixat  $a \in \mathbb{R}$ ,  $f_a : \mathbb{R}^+ \longrightarrow \mathbb{R}$ ,  $f_a(x) = \log_a x$
  - Funció *factorial*.  $f : \mathbb{N} \longrightarrow \mathbb{N}$  definida recursivament:  
 $f(0) = 1$ ,  $f(n) = n f(n-1)$ , si  $n \geq 1$ .  
Per tant,  $f(n) = n(n-1)(n-2) \dots 3 \cdot 2 \cdot 1 = n!$
- Per a  $n$  suficientment gran,
- $$1 \leq \ln n \leq n \leq n \ln n \leq n^2 \leq n^3 \leq 2^n \leq 3^n \leq n! \leq n^n$$

### 3. APLICACIONES (III)

Si  $f : A \longrightarrow B$  és una aplicació,  $X \subset A$  i  $Y \subset B$ ,

- El *conjunt imatge* de  $X$  és  $f(X) = \{f(x) | x \in X\} \subset B$ ; en particular, el *conjunt imatge* de  $f$  és  $\text{Im}f = f(A) = \{f(a) | a \in A\}$
  - El *conjunt antiimatge* de  $Y$  és  $f^{-1}(Y) = \{a \in A | f(a) \in Y\} \subset A$ . Si  $b \in B$  escriurem  $f^{-1}(b) = f^{-1}(\{b\}) = \{a \in A | f(a) = b\} \subset A$ .
- ▷ Observació:  $f^{-1}(b)$ ,  $b \in B$ , pot ser buit, tenir un únic element o tenir-ne més d'un.

### 3. APLICACIONES (IV)

- Igualtat d'aplicacions: Dues aplicacions  $f, g$  son iguals si tenen el mateix conjunt de sortida  $A$ , el mateix conjunt d'arribada,  $B$ , i a més  $f(a) = g(a)$  per a tot  $a \in A$ .
- ▶ Si  $A, B$  són conjunts finits tals que  $|A| = n$ ,  $|B| = m$ , llavors el nombre d'aplicacions  $f : A \longrightarrow B$  és  $m^n$ .

### 3. APLICACIONES (V)

● Composició d'aplicacions: la composició de les aplicacions  $f : A \longrightarrow B$  i  $g : B \longrightarrow C$  és l'aplicació  $g \circ f : A \longrightarrow C$  tal que  $(g \circ f)(a) = g(f(a))$  per a tot  $a \in A$ .

► La composició d'aplicacions és associativa: si  $f : A \longrightarrow B$ ,  $g : B \longrightarrow C$ ,  $h : C \longrightarrow D$ , llavors  $h \circ (g \circ f) = (h \circ g) \circ f$ .

► La composició d'aplicacions no és en general commutativa: si  $f, g : A \longrightarrow A$ , en general NO és cert  $f \circ g = g \circ f$

### 3. APLICACIONES (VI). APLICACIONES INJECTIVAS

• *Aplicación inyectiva*: aplicación  $f : A \longrightarrow B$  tal que elementos diferentes de  $A$  tienen imágenes diferentes.

► Si  $f : A \longrightarrow B$ , las condiciones siguientes son equivalentes:

▷  $f$  es inyectiva

$$\triangleright \forall a, a' \in A, a \neq a' \implies f(a) \neq f(a')$$

$$\triangleright \forall a, a' \in A, f(a) = f(a') \implies a = a'$$

$$\triangleright \forall b \in B, |f^{-1}(b)| \leq 1$$

► Si  $A, B$  son conjuntos finitos tales que  $|A| = n, |B| = m$ , entonces el número de aplicaciones inyectivas  $f : A \longrightarrow B$  es

$$m^n = \underbrace{m(m-1)(m-2)\dots(m-n+1)}_{n \text{ factores}}$$

► Si  $A, B$  son conjuntos finitos tales que  $|A| = n, |B| = m$  i  $f : A \longrightarrow B$  es una aplicación inyectiva,  $|A| \leq |B|$ .

### 3. APLICACIONES (VII). APLICACIONES EXHAUSTIVAS

• *Aplicació exhaustiva*: aplicació  $f : A \longrightarrow B$  tal que tot element de  $B$  té almenys una antiimatge.

► Si  $f : A \longrightarrow B$ , les condicions següents són equivalents:

▷  $f$  és exhaustiva

▷  $\forall b \in B, \exists a \in A$  tal que  $f(a) = b$

▷  $\text{Im}f = B$

▷  $\forall b \in B, |f^{-1}(b)| \geq 1$

▷  $\forall b \in B, f^{-1}(b) \neq \emptyset$

► El càlcul del nombre d'aplicacions exhaustives no és immediat.

► Si  $A, B$  són conjunts finits tals que  $|A| = n, |B| = m$  i  $f : A \longrightarrow B$  és una aplicació exhaustiva,  $|B| \leq |A|$ .

### 3. APLICACIONES (VIII). APLICACIONES BIJECTIVAS

● *Aplicación biyectiva*: aplicación  $f : A \longrightarrow B$  inyectiva i exhaustiva ahora.

▶  $f : A \longrightarrow B$  és una aplicació bijectiva si per a tot  $b \in B$  existeix un únic  $a \in A$  tal que  $f(a) = b$ .

▶ Si  $A, B$  són conjunts finits tals que  $|A| = n, |B| = m$  i  $f : A \longrightarrow B$  és una aplicació bijectiva, llavors  $|A| = |B|$ .

▶ Si  $A, B$  són conjunts finits tals que  $|A| = |B| = n$ , llavors el nombre d'aplicacions bijectives  $f : A \longrightarrow B$  és  $n^n = n(n - 1)(n - 2) \dots 3 \cdot 2 \cdot 1 = n!$

### 3. APLICACIONES (IX). INVERSA

- Aplicació *identitat* en  $A$ :  $I_A : A \longrightarrow A$  tal que  $Id_A(a) = a$  per a tot  $a \in A$
- $f : A \longrightarrow B$  és *invertible* si existeix una aplicació  $f^{-1} : B \longrightarrow A$  tal que  $f^{-1} \circ f = I_A$  i  $f \circ f^{-1} = I_B$ . Direm que  $f^{-1}$  és l'*aplicació inversa* de  $f$ .
- $f : A \longrightarrow B$  és invertible si i només si  $f$  és bijectiva. En aquest cas, l'*aplicació inversa* de  $f$  és  $f^{-1} : B \longrightarrow A$  tal que  $f^{-1}(b) = a$  si  $f(a) = b$ .

## 4. COMPTAR (I). PERMUTACIONS

- Una  $k$ -permutació d'un  $n$ -conjunt  $X$ , és una successió de  $k$  elements diferents de  $X$
- Una permutació d'un  $n$ -conjunt  $X$ , és una  $n$ -permutació de  $X$

Notació:

▷  $P(n, k)$  = nombre de  $k$ -permutacions d'un  $n$ -conjunt.

▷  $P(n) = P(n, n)$  = nombre de permutacions d'un  $n$ -conjunt

Càlcul:

▶  $P(n, k) = n(n - 1)(n - 2) \dots (n - k + 1) = n^{\underline{k}} = \frac{n!}{(n-k)!}$ , si

$1 \leq k \leq n$ ;  $P(n, k) = 0$  si  $k > n$

▶  $P(n) = P(n, n) = n^{\underline{n}} = n!$

## 4. COMPTAR (II). PERMUTACIONS

Exemples.

▷ El nombre d'aplicacions injectives  $f : A \longrightarrow B$ , on  $|A| = k$ ,  $A = \{a_1, \dots, a_k\}$ , i  $|B| = n$  és  $P(n, k)$ : podem identificar l'aplicació amb la successió  $(f(a_1), f(a_2), \dots, f(a_k))$  d'elements diferents de  $B$ .

▷ El nombre de paraules de longitud  $k$  i alfabet  $X$ ,  $|X| = n$ , amb totes les lletres diferents és  $P(n, k)$ : cada paraula és una successió  $(a_1, \dots, a_k)$  d'elements diferents de  $X$ .

## 4. COMPTAR (III). PERMUTACIONS AMB REPETICIÓ

- Una *k*-permutació amb repetició d'un *n*-conjunt *X*, és una successió de *k* elements no necessàriament diferents de *X*

▷ Notació:  $PR(n, k)$  = nombre de *k* permutacions amb repetició d'un *n*-conjunt

▶ Càlcul:  $PR(n, k) = n^k$ , si  $k \geq 1$

## 4. COMPTAR (IV). PERMUTACIONS AMB REPETICIÓ

Exemples.

▷ El nombre d'aplicacions  $f : A \longrightarrow B$ , on  $|A| = k$ ,  $A = \{a_1, \dots, a_k\}$  i  $|B| = n$  és  $PR(n, k)$ : podem identificar l'aplicació amb la successió  $(f(a_1), f(a_2), \dots, f(a_k))$  d'elements de  $B$ .

▷ El nombre de paraules de longitud  $k$  i alfabet  $X$ ,  $|X| = n$ , és  $PR(n, k)$ : cada paraula és una successió  $(a_1, \dots, a_k)$  d'elements de  $X$ .

## 4. COMPTAR (V). NOMBRE D'APLICACIONS

► Nombre d'aplicacions  $f : A \longrightarrow B$ ,  $|A| = k$ ,  $|B| = n$ :

APLICACIONS	APL. INJECTIVES	APL. BIJECTIVES
$n^k$	$\begin{cases} n^k, & \text{si } k \leq n, \\ 0, & \text{si } k > n. \end{cases}$	$\begin{cases} n!, & \text{si } k = n, \\ 0, & \text{si } k \neq n. \end{cases}$

*Principi de les caselles.*

► Si  $f : A \longrightarrow B$  és una aplicació i  $|A| > |B|$ , llavors  $f$  no pot ser injectiva

► Si distribuim  $n$  objectes en  $m$  capsos i  $n > m$ , almenys una capsa contindrà dos o més objectes

► Si distribuim  $n$  objectes en  $m$  capsos i  $n > rm$ , almenys una capsa contindrà  $r+1$  o més objectes

## 4. COMPTAR (VI). COMBINACIONS

- Una  $k$ -combinació d'un  $n$ -conjunt  $X$ , és un  $k$ -subconjunt de  $X$

▷ Notació:  $C(n, k) = \binom{n}{k}$  = nombre de  $k$ -subconjunts d'un  $n$ -conjunt.

▶  $C(n, k) k! = P(n, k)$

▶  $C(n, k) = \binom{n}{k} = \frac{n!}{k!(n-k)!}$

## 4. COMPTAR (VII). SELECCIONS

Nombre de  $k$ -seleccions d'un  $n$ -conjunt. Si  $X$  és un conjunt de cardinal  $n$ , volem comptar el nombre de maneres de seleccionar  $k$  elements de  $X$ , en els casos següents:

- ▷ s'admeten o no repeticions
- ▷ es té o no en compte l'ordre dels elements seleccionats:

# seleccions	sense repetició	amb repetició
ordenades	$P(n, k) = n^k$	$PR(n, k) = n^k$
no ordenades	$C(n, k) = \binom{n}{k}$	—

## 4. COMPTAR (VIII)

- Una *successió* d'elements de  $X$  és una aplicació  $f : \mathbb{N} \longrightarrow X$ . El *terme*  $n$ -èssim de la successió és  $f(n)$ .  $(a_n)_{n \geq 0}$  representa la successió tal que  $a_n = f(n)$ .  $(a_n)_{n \geq n_0}$  representa la successió que comença amb el terme  $a_{n_0}$ . En aquest cas es pot interpretar que  $a_n = 0$  si  $n < n_0$ .
- Una successió és *recurrent* si a partir d'un determinat valor de  $n$ , cada terme s'obté en funció dels anteriors.

## 4. COMPTAR (IX). PROGRESSIONS ARITMÈTIQUES

• *Progressió aritmètica.* Successió  $(a_n)_{n \geq n_0}$  recurrent tal que  $\forall n > n_0, a_n = a_{n-1} + d$ , on  $d$  és un valor constant que anomenem *diferència*.

Si  $(a_n)_{n \geq 0}$  és una progressió aritmètica de diferència  $d$ :

▶ Terme general en funció de  $a_0$  i  $d$ :  $a_n = a_0 + n d, \forall n \geq 0$

▶ Terme general en funció de  $a_k$  i  $d$ :  $a_n = a_k + (n - k) d, \forall n \geq k$

▶ Suma dels  $n$  primers termes:

$$a_0 + a_1 + \cdots + a_{n-1} = \frac{a_0 + a_{n-1}}{2} n$$

▶ Suma de termes consecutius:

$$a_k + a_{k+1} + \cdots + a_n = \frac{a_k + a_n}{2} (n - k + 1) \text{ (primer terme + \u00faltim terme, dividit per 2, multiplicat pel nombre de termes)}$$

## 4. COMPTAR (X). PROGRESSIONS GEOMÈTRIQUES

• *Progressió geomètrica*. Successió recurrent  $(a_n)_{n \geq n_0}$  tal que  $\forall n > n_0, a_n = r a_{n-1}$ , on  $r$  és un valor constant que anomenem *raó*.

Si  $(a_n)_{n \geq 0}$  és una progressió geomètrica de raó  $r$ :

▶ Terme general en funció de  $a_0$  i  $r$ :  $a_n = a_0 r^n, \forall n \geq 0$

▶ Terme general en funció de  $a_k$  i  $r$ :  $a_n = a_k r^{(n-k)}, \forall n \geq k$

▶ Suma dels  $n$  primers termes:

$$a_0 + a_1 + \cdots + a_n = \frac{a_n r - a_0}{r - 1}$$

▶ Suma de termes consecutius:

$$a_k + a_{k+1} + \cdots + a_n = \frac{a_n r - a_k}{r - 1} \text{ (últim terme per la raó menys primer terme, dividit per la raó menys 1)}$$

## 4. COMPTAR (XI): EXPRESSIONS AMB $\Sigma$ , $\Pi$

▷  $\sum_{i \in I} f(i)$  representa la suma de tots els termes  $f(i)$ ,  $i \in I$ .

▷  $\prod_{i \in I} f(i)$  representa el producte de tots els termes  $f(i)$ ,  $i \in I$ .

▷  $\sum_{i=n}^m f(i)$  representa la suma dels termes  $f(n), f(n+1), \dots, f(m)$

▷  $\prod_{i=n}^m f(i)$  representa el producte dels termes  $f(n), f(n+1), \dots, f(m)$

## 4. COMPTAR (XII): EXPRESSIONS AMB $\Sigma$ , $\Pi$

▷ Exemples.

$$\sum_{i=1}^n i = 1 + 2 + \dots + n = \frac{(1+n)n}{2} ; \quad \sum_{i=1}^n 1 = n ; \quad \sum_{i=1}^n 3 = 3n$$

$$\prod_{i=1}^n i = 1 \cdot 2 \cdot \dots \cdot n = n! ; \quad \prod_{i=1}^n 1 = 1 ; \quad \prod_{i=1}^n 3 = 3^n$$

$$\sum_{i=5}^9 i^2 = 25 + 36 + 49 + 64 + 81 = 255$$

$$\prod_{\substack{p \text{ primer} \\ 2 \leq p \leq 10}} \left(1 - \frac{1}{p}\right) = \left(1 - \frac{1}{2}\right) \left(1 - \frac{1}{3}\right) \left(1 - \frac{1}{5}\right) \left(1 - \frac{1}{7}\right) = \frac{8}{35}$$

## 4. COMPTAR (XIII): EXPRESSIONS AMB $\Sigma$ , $\Pi$

$$\blacktriangleright \sum_{i \in I} (f(i) + g(i)) = \sum_{i \in I} f(i) + \sum_{i \in I} g(i)$$

$$\blacktriangleright \text{Si } c \text{ no depèn de } i, \sum_{i \in I} c f(i) = c \sum_{i \in I} f(i)$$

▷ Exemples.

$$\sum_{i=1}^n i^2 = 1^2 + 2^2 + \dots + n^2 = \frac{n(n+1)(2n+1)}{6}$$

$$\sum_{i=1}^n i^3 = 1^3 + 2^3 + \dots + n^3 = \frac{n^2(n+1)^2}{4}$$

## 4. COMPTAR (XIV): EXPRESSIONS AMB $\Sigma$ , $\Pi$

Es poden considerar expressions amb 2 o més índexs (en aquest cas,  $X$  és un conjunt de parells ordenats o  $n$ -ples de índexs) o bé expressions amb més d'una suma o producte:

▷  $\sum_{(i,j) \in X} f(i,j)$  representa la suma de  $f(i,j)$ ,  $(i,j) \in X$ .

▷  $\prod_{(i,j) \in X} f(i,j)$  representa el producte de  $f(i,j)$ ,  $(i,j) \in X$ .

▶  $\sum_{i \in I} \sum_{j \in J} f(i,j) = \sum_{(i,j) \in I \times J} f(i,j)$

▶  $\prod_{i \in I} \prod_{j \in J} f(i,j) = \prod_{(i,j) \in I \times J} f(i,j)$

## 4. COMPTAR (XV): EXPRESSIONS AMB $\Sigma$ , $\Pi$

Exemples.

$$\begin{aligned} \triangleright \sum_{j=1}^m \sum_{i=1}^n i j &= \sum_{j=1}^m \left( j \sum_{i=1}^n i \right) = \sum_{j=1}^m j \frac{n(1+n)}{2} = \\ &= \frac{n(1+n)}{2} \sum_{j=1}^m j = \frac{n(1+n)m(1+m)}{2} \end{aligned}$$

$$\begin{aligned} \triangleright \sum_{j=1}^n \sum_{i=j}^n i j &= \sum_{j=1}^n \left( j \sum_{i=j}^n i \right) = \sum_{j=1}^n j \frac{(j+n)(n-j+1)}{2} = \\ &= \sum_{j=1}^n \frac{n(n+1)j + j^2 - j^3}{2} = \frac{n(n+1)}{2} \sum_{j=1}^n j + \frac{1}{2} \sum_{j=1}^n j^2 - \frac{1}{2} \sum_{j=1}^n j^3 = \\ &= \frac{n^2(n+1)^2}{4} + \frac{n(n+1)(2n+1)}{2 \cdot 6} - \frac{n^2(n+1)^2}{2 \cdot 4} = \frac{n(n+1)(n+2)(3n+1)}{24} \end{aligned}$$

## 5. ARITMÈTICA (I). DIVISIBILITAT A $\mathbb{Z}$

• Si  $a, b \in \mathbb{Z}$ ,  $a \neq 0$ , direm que  $a$  divideix  $b$  (o bé  $a$  és divisor de  $b$ , o bé  $b$  és múltiple de  $a$ ) si existeix un enter  $c \in \mathbb{Z}$  tal que  $b = a \cdot c$ .

▷ Notació. Si  $a$  divideix  $b$ , escriurem  $a|b$  o bé  $b = a \cdot c$ .

► Si  $a, b, c, r, s$  són enters qualssevol tals que  $a, b \neq 0$ , llavors

$$a|a$$

$$a|b, b|c \Rightarrow a|c$$

$$a|b, b|a \Rightarrow b = \pm a$$

$$a|b, a|c \Rightarrow a|b + c$$

$$a|b \Rightarrow a|bc$$

$$a|b, a|c \Rightarrow a|br + cs$$

$$a|b \Rightarrow \pm a | \pm b$$

$$a|b \Rightarrow |a| \leq |b|$$

► Si  $n, d$  són enters,  $n, d \geq 1$ , el nombre de múltiples de  $d$  entre 1 i  $n$  és  $\lfloor \frac{n}{d} \rfloor$ .

## 5. ARITMÈTICA (II). TEOREMA DE LA DIVISIÓ. MÀXIM COMÚ DIVISOR

► *Teorema de la divisió.* Per a tot parell d'enters  $a$  i  $b$ ,  $a \neq 0$ , existeixen enters  $q, r$  únics tals que  $b = aq + r$ ,  $0 \leq r < |a|$ .

▷  $q, r$  s'anomenen respectivament *quocient* i *residu* de la divisió entera de  $b$  per  $a$ .

► Si  $a, b \in \mathbb{Z}$ ,  $a \neq 0$ , llavors  $a|b \Leftrightarrow$  el residu de fer la divisió entera de  $b$  per  $a$  és 0.

•  $d$  és *divisor comú* de  $a$  i  $b$  si divideix  $a$  i  $b$  alhora.

• Si  $a, b$  son enters, no tots dos nuls, el *màxim comú divisor* de  $a$  i  $b$  és el màxim de tots els divisors comuns de  $a$  i  $b$ .

▷ Notació. Escriurem  $\text{mcd}(a, b)$  o bé simplement  $(a, b)$ .

►  $(a, b) = d \Leftrightarrow \begin{cases} d|a, d|b \\ r|a, r|b \Rightarrow r \leq d \end{cases}$

## 5. ARITMÈTICA (III). MÀXIM COMÚ DIVISOR

► Si  $a, b$  són enters no nuls,  
 $(a, b)$  és un enter positiu únic

$$(a, b) = (\pm a, \pm b)$$

$$\text{Si } a > 0, a|b \Leftrightarrow (a, b) = a$$

$$b = aq + r \Rightarrow (a, b) = (a, r)$$

- Dos enters  $a, b$  són *relativament primers* si  $(a, b) = 1$

## 5. ARITMÈTICA (IV). ALGORISME D'EUCLIDES. IDENTITAT DE BÉZOUT

► *Algorisme d'Euclides.* Considerem  $a, b$  enters,  $a \geq b > 0$ . Si  $b|a$ , llavors  $(a, b) = b$ . Si  $b \nmid a$ , fem successivament les divisions enteres següents fins obtenir residu 0:

$$a = bq + r_0$$

$$b = r_0q_0 + r_1$$

$$r_0 = r_1q_1 + r_2$$

$$r_1 = r_2q_2 + r_3$$

...

$$r_{n-2} = r_{n-1}q_{n-1} + r_n$$

$$r_{n-1} = r_nq_n + 0.$$

Llavors  $(a, b) = r_n$ .

► *Identitat de Bézout.* Si  $(a, b) = d$ , existeixen enters  $s, t$  tals que  $as + bt = d$ .

## 5. ARITMÈTICA (V). ALGORISME D'EUCLIDES. IDENTITAT DE BÉZOUT

► Càlcul del m.c.d. i de la identitat de Bézout. Si  $a, b$  són enters,  $a > b > 0$ , considerem les divisions successives obtingudes a l'algorisme d'Euclides:

1	0	$s_0$	$s_1$	$\cdots$	$s_{n-2}$	$s_{n-1}$	$s_n$
0	1	$t_0$	$t_1$	$\cdots$	$t_{n-2}$	$t_{n-1}$	$t_n$
	$q$	$q_0$	$q_1$	$\cdots$	$q_{n-2}$	$q_{n-1}$	$q_n$
$a$	$b$	$r_0$	$r_1$	$\cdots$	$r_{n-2}$	$r_{n-1}$	$r_n$
$r_0$	$r_1$	$r_2$	$r_3$	$\cdots$	$r_n$	0	

on:  $s_0 = 1$ ,  $t_0 = -q$ ,  $s_1 = -s_0 q_0 = -q_0$ ,  $t_1 = 1 - t_0 q_0 = 1 + q q_0$ ,  
 $\forall i \geq 2$ ,  $s_i = s_{i-2} - s_{i-1} q_{i-1}$ ,  $t_i = t_{i-2} - t_{i-1} q_{i-1}$ .

Llavors:  $\forall i \geq 0$ ,  $r_i = a s_i + b t_i$

En particular:  $(a, b) = r_n = a s_n + b t_n$

## 5. ARITMÈTICA (VI). CONSEQUÈNCIES DE LA IDENTITAT DE BÉZOUT

- ▶  $r|a, r|b \Rightarrow r|(a, b)$
- ▶ Si  $a, b, s, t$  són enters tals que  $as + bt = 1$ , llavors  $(a, b) = 1$
- ▶ Si  $(a, b) = d$ , llavors  $\left(\frac{a}{d}, \frac{b}{d}\right) = 1$
- ▶ Si  $r > 0$ , llavors  $(ra, rb) = r(a, b)$
- ▶  $a|bc$  i  $(a, b) = 1 \Rightarrow a|c$
- ▶ L'equació  $ax + by = c$  té solució en  $\mathbb{Z}$  si, i només si,  $(a, b)|c$ .  
▷ Càlcul d'una solució. Si  $d = (a, b)|c$ , llavors  $\frac{c}{d} \in \mathbb{Z}$ . A partir de la identitat de Bézout,  $d = as + bt \Rightarrow c = d\frac{c}{d} = as\frac{c}{d} + bt\frac{c}{d}$ . Una solució és  $x = s\frac{c}{d}$ ,  $y = t\frac{c}{d}$ .

## 5. ARITMÈTICA (VII). NOMBRES PRIMERS. FACTORITZACIÓ D'ENTERS

- Un enter  $p \geq 2$  és *primer* si els únics divisors positius de  $p$  són 1 i  $p$
- ▶ Si  $p$  és primer,  $p|ab \Rightarrow p|a$  ó  $p|b$
- ▶ *Teorema fonamental de l'aritmètica.* Tot enter  $a \geq 2$  es pot expressar com a producte de nombres primers de forma única, llevat l'ordre dels factors.
- ▶ *Notació exponencial.* Tot enter  $a \geq 2$  es pot expressar de forma única com  $a = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$ , on  $p_1 < p_2 < \dots < p_k$  són primers i  $\forall i, \alpha_i > 0$ .

## 5. ARITMÈTICA (VIII). NOMBRES PRIMERS. FACTORITZACIÓ D'ENTERS

- ▶ Hi ha infinits nombres primers
- ▶ Tot enter  $n \geq 2$  no primer té almenys un factor primer  $p \leq \sqrt{n}$
- ▶ Taula dels primers  $p \leq n$ : Garbell d'Eratóstenes

## 5. ARITMÈTICA (IX). MÍNIM COMÚ MÚLTIPLE

●  $m$  és múltiple comú de  $a$  i  $b$  si  $m$  és múltiple de  $a$  i de  $b$  alhora.

● Si  $a, b$  són enters no nuls, el *mínim comú múltiple* de  $a$  i  $b$  és el mínim de tots els naturals no nuls que són múltiples comuns de  $a$  i  $b$ .

▷ Notació. Escriurem  $\text{mcm}(a, b)$  o bé  $[a, b]$ .

$$\blacktriangleright [a, b] = m \Leftrightarrow m \geq 1 \text{ i } \begin{cases} m = a, m = b \\ r = a, r = b, r \geq 1 \Rightarrow m \leq r \end{cases}$$

▶ Si  $a, b$  són enters positius,  $(a, b) \cdot [a, b] = a \cdot b$

▶  $a|r, b|r \Rightarrow [a, b]|r$

## 5. ARITMÈTICA (X). MÀXIM COMÚ DIVISOR I MÍNIM COMÚ MÚLTIPLE

► Si  $a, b \geq 2$  són enters, podem suposar  $a = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$  i  $b = p_1^{\beta_1} p_2^{\beta_2} \dots p_k^{\beta_k}$ , on  $p_1 < p_2 < \dots < p_k$  són tots els factors primers de  $a$  o de  $b$  i  $\forall i, \alpha_i \geq 0, \beta_i \geq 0$ . (És a dir, si un nombre primer no és factor de  $a$  o de  $b$  apareix amb exponent 0).

$$\text{Llavors, } (a, b) = \prod_{i=1}^k p_i^{\min\{\alpha_i, \beta_i\}} \quad , \quad [a, b] = \prod_{i=1}^k p_i^{\max\{\alpha_i, \beta_i\}} .$$

## 5. ARITMÈTICA (XI). CONGRUÈNCIES

• Enters *congruents mòdul m*:  $a \equiv b \pmod{m} \Leftrightarrow m|b - a$

► Les condicions següents són equivalents:

(1)  $m|b - a$

(2)  $b = a + m$

(3) la divisió entera de  $a$  i  $b$  entre  $m$  dóna el mateix residu

(4)  $\{a + mk \mid k \in \mathbb{Z}\} = \{b + mk \mid k \in \mathbb{Z}\}$

► Propietats:

(1)  $a \equiv a \pmod{m}$

(2)  $a \equiv b \pmod{m} \Rightarrow b \equiv a \pmod{m}$

(3)  $a \equiv b \pmod{m}, b \equiv c \pmod{m} \Rightarrow a \equiv c \pmod{m}$

(4)  $a \equiv b \pmod{m}, a' \equiv b' \pmod{m} \Rightarrow$   
 $\Rightarrow a + a' \equiv b + b' \pmod{m}, aa' \equiv bb' \pmod{m}$

(5)  $a \equiv b \pmod{m}, d|m \Rightarrow a \equiv b \pmod{d}$

(6)  $a \equiv b \pmod{r}, a \equiv b \pmod{s} \Rightarrow a \equiv b \pmod{[r, s]}$

(7)  $ra \equiv rb \pmod{m} \Leftrightarrow a \equiv b \pmod{m/(m, r)}$

## 5. ARITMÈTICA (XII). EQUACIONS AMB CONGRUÈNCIES

► L'equació  $a + x \equiv b \pmod{m}$  sempre té solució, i és  $x \equiv b - a \pmod{m}$

► L'equació  $ax \equiv b \pmod{m}$  té solució  $\Leftrightarrow (a, m) | b$ .

En aquest cas, podem trobar una solució a partir de la identitat de Bézout:

$(a, m) = d = as + mt \Rightarrow x = \frac{sb}{d}$  és una solució

## 5. ARITMÈTICA (XIII). INVERS MODULAR

● *Invers modular.*  $a' \in \mathbb{Z}$  és *invers mòdul*  $m$  de  $a \in \mathbb{Z}$  si  $a a' \equiv 1 \pmod{m}$ .

► Existeix un invers mòdul  $m$  de  $a \in \mathbb{Z} \Leftrightarrow ax \equiv 1 \pmod{m}$  té solució  $\Leftrightarrow (a, m) = 1$ .

En aquest cas, podem trobar una solució a partir de la identitat de Bézout:

$(a, m) = 1 = a s + m t \Rightarrow s$  és una solució.

## 5. ARITMÈTICA (XIV). POTENCIACIÓ MODULAR

► Càlcul de  $a^k \pmod{m}$ .

Escrivim  $k$  en base 2:  $k = (k_n k_{n-1} \dots k_1 k_0)_2$ , és a dir,

$$k = k_n 2^n + k_{n-1} 2^{n-1} + \dots + k_1 2 + k_0, \text{ on } k_i \in \{0, 1\}.$$

$$\begin{aligned} \text{Llavors } a^k &= a^{k_n 2^n + k_{n-1} 2^{n-1} + \dots + k_1 2 + k_0} = \\ &= a^{k_n 2^n} \cdot a^{k_{n-1} 2^{n-1}} \cdot \dots \cdot a^{k_1 2} \cdot a^{k_0} \end{aligned}$$

Calculem successivament les potències  $a, a^2, a^4, a^8, \dots, a^{2^n}$  mòdul  $m$  i fem el producte de les potències  $a^{2^i}$  tals que  $k_i = 1$ .

▷ Exemple. Calcular  $12^{39} \pmod{35}$ .

$$39 = (100111)_2 \Rightarrow 39 = 2^5 + 2^2 + 2 + 1 \Rightarrow$$

$$\Rightarrow 12^{39} = 12^{2^5 + 2^2 + 2 + 1} = 12^{32 + 4 + 2 + 1} = 12^{32} \cdot 12^4 \cdot 12^2 \cdot 12$$

Calculem les potències  $12^{2^i}$  mòdul 35:

$$12^2 = 144 \equiv 4 \qquad 12^4 \equiv 4^2 = 16$$

$$12^8 \equiv 16^2 = 256 \equiv 11 \qquad 12^{16} \equiv 11^2 = 121 \equiv 16$$

$$12^{32} \equiv 16^2 = 256 \equiv 11$$

Per tant,  $12^{39} \equiv 11 \cdot 16 \cdot 4 \cdot 12 = 8448 \equiv 13 \pmod{35}$

## 5. ARITMÈTICA (XV). EL CONJUNT $\mathbb{Z}_m$

- Fixat un enter  $m \geq 2$ , per a cada  $a \in \mathbb{Z}$  la *classe de  $a$  mòdul  $m$*  és el conjunt d'enters:

$$\bar{a} = \{b \mid a \equiv b \pmod{m}\} = \{a + km \mid k \in \mathbb{Z}\}$$

- El conjunt *d'enters mòdul  $m$* ,  $m \geq 2$ , és:

$$\mathbb{Z}_m = \{\bar{a} \mid a \in \mathbb{Z}\}.$$

- ▶ El conjunt  $\mathbb{Z}_m$  té exactament  $m$  elements:

$$\mathbb{Z}_m = \{\bar{a} \mid a \in \mathbb{Z}\} = \{\bar{0}, \bar{1}, \bar{2}, \dots, \overline{m-1}\}.$$

- ▶ Definim una suma i un producte a  $\mathbb{Z}_m$ :

$$\text{Suma. } \bar{a} + \bar{b} = \overline{a + b}$$

$$\text{Producte. } \bar{a} \cdot \bar{b} = \overline{a \cdot b}$$