

Apunts de FONAMENTS MATEMÀTICS

Rafel Farré

06/09/2019

Els exercicis/problemes en **color blau** són
per fer a les classes de taller.
Els exercicis marcats amb **(R)** són recomanats.

0. SUMATORIS

$$\sum_{i=m}^n f(i) = f(m) + f(m+1) + \dots + f(n-1) + f(n)$$

Exemples:

1. $\sum_{i=1}^{100} i = 1 + 2 + 3 + \dots + 99 + 100.$
2. $\sum_{i=-2}^{50} 2i = -4 - 2 + 0 + 2 + 4 + \dots + 98 + 100.$
3. $\sum_{i=5}^{1000} i^2 = 5^2 + 6^2 + 7^2 + \dots + 999^2 + 1000^2.$
4. $\sum_{i=1}^{30} (-1)^i (2i-1)^2 = -1^2 + 3^2 - 5^2 + \dots + 59^2.$

Exercicis:

Passeu a notació amb sumatori:

1. (R) $-2 + 0 + 2 + 4 + 6 + \dots + 50.$
2. $3 + 5 + 7 + \dots + 55.$
3. $2 - 4 + 6 - \dots + 50.$

4. $-1^2 + 3^2 - 5^2 + 7^2 - \dots - 49^2$.
5. (R) $\frac{2}{1^3} + \frac{5}{5^3} + \frac{8}{9^3} + \frac{11}{13^3} + \dots + \frac{47}{61^3}$.
6. $-3 + 0 + 3 + 6 + 9 + 12 + \dots + 60$.
7. $1^3 - 4^3 + 7^3 - 10^3 + \dots + 61^3$.
8. (R) $\frac{1}{3} - \frac{1}{7} + \frac{1}{11} - \frac{1}{15} + \dots - \frac{1}{39}$.
9. $-\frac{2}{1} + \frac{4}{4^3} - \frac{6}{7^3} + \frac{8}{10^3} - \dots - \frac{42}{61^3}$.

Propietats dels sumatoris

| |
|--|
| $\sum_{i=m}^n (f(i) + g(i)) = \sum_{i=m}^n f(i) + \sum_{i=m}^n g(i)$ |
| $\sum_{i=m}^n c f(i) = c \sum_{i=m}^n f(i)$ |

Exercicis:

10. Expressen les sumes següents en funció de $S = \sum_{n=1}^{10} a_n$:

- a. $\sum_{m=1}^{10} a_m$
- b. $\sum_{i=0}^9 a_n$
- c. $\sum_{j=1}^{10} a_{j-1}$

11. (R) Calculeu:

- a. $\sum_{i=0}^{n+1} a_i - \sum_{i=0}^n a_i$
- b. $\sum_{i=1}^{n+2} a_i - \sum_{i=1}^{n-1} a_i$

12. (R) Proveu que si $n \geq 0$ $\sum_{k=0}^{n+3} r^k - \sum_{k=0}^n r^k = r^n(r + r^2 + r^3)$.

13. (R) Calculeu $\sum_{k=1}^n (k+3)^2$, sabent que $\sum_{k=1}^n k = \frac{n(n+1)}{2}$ i $\sum_{k=1}^n k^2 = \frac{n(n+1)(2n+1)}{6}$.

14. Si $A = \sum_{i=n}^m a_i$ i $B = \sum_{i=n}^m b_i$, expresseu en funció de A i B :

a. $\sum_{i=n}^m 5a_i$

b. $\sum_{i=n}^m (a_i - b_i)$

c. (R) $\sum_{i=n}^m -3b_i$

d. (R) $\sum_{i=n}^m (2a_i + 4b_i)$

15. (R) Canvieu l'índex dels sumatoris següents perquè comencin en $j = 0$

(quedin de la forma $\sum_{j=0}$):

a. $\sum_{i=8}^n i^2$

b. $\sum_{i=-3}^{n+2} (2i + 3)$

16. Expresseu cada una de les sumes següents amb un sol sumatori:

a. $\sum_{k=1}^n (6k - 3) + \sum_{k=1}^n (4 - 5k)$

b. $\sum_{k=1}^n (4k - 1)^2 + \sum_{k=1}^n (4k + 1)^2$

c. $\sum_{k=1}^{100} (2k - 1)^2 + \sum_{k=0}^{99} (2k - 1)^2$

d. $\sum_{k=0}^{99} (2k + 1)^2 + \sum_{i=1}^{100} (3k - 2)^2$

Progressions aritmètiques

Cada terme a_{i+1} s'obté de l'anterior a_i sumant una quantitat d anomenada diferència: $a_{i+1} = a_i + d$.

$$a_i = a_1 + (i - 1)d$$

Exemple: La successió $a_n = 5n - 3$ és una progressió aritmètica amb diferència $d = 5$

La suma d'una progressió aritmètica s'obté mitjançant la fórmula:

$$\sum_{i=m}^n a_i = \frac{(a_m + a_n)(n - m + 1)}{2}$$

Observeu que $n - m + 1$ és el número de termes del sumatori.

Demostració: Ho fem primer pel cas en què el nombre de sumands és parell. Observem que la suma del primer més l'últim és igual que la del segon més el penúltim, que és igual que la del tercer més el antepenúltim Agrupant els sumands de dos en dos obtenim la fórmula, ja que només cal multiplicar $a_m + a_n$ per la meitat del nombre de sumands, que és $\frac{n-m+1}{2}$. Si el nombre de sumands $n - m + 1$ és senar, ens queda un terme desaparellat, que val $\frac{a_m + a_n}{2}$. La resta de sumands dona $\frac{(a_m + a_n)(n-m)}{2}$. Per tant la suma total en aquest cas s'obté amb la mateixa fórmula.

Progressions geomètriques

Cada terme a_{i+1} s'obté de l'anterior a_i multiplicant per una quantitat r anomenada raó: $a_{i+1} = r a_i$.

$$a_i = a_0 r^i = a_1 r^{i-1} = \dots = a_k r^{i-k}$$

Exemple: La successió $a_n = \frac{3}{4} 2^n$ és una progressió geomètrica amb raó $r = 2$

La suma d'una progressió geomètrica amb $r \neq 1$ s'obté mitjançant la fórmula:

$$\sum_{i=m}^n a_i = \frac{a_{n+1} - a_m}{r - 1}$$

Demostració:

Si multipliquem el sumatori per $r - 1$ obtenim:

$$\begin{aligned} \left(\sum_{i=m}^n a_i \right) (r - 1) &= (a_m + r a_m + \dots + r^{n-m} a_m) (r - 1) = \\ a_m (1 + r + \dots + r^{n-m}) (r - 1) &= a_m (r^{n-m+1} - 1) = a_{n+1} - a_m. \end{aligned}$$

Productoris

$$\prod_{i=m}^n f(i) = f(m) \cdot f(m+1) \cdots f(n-1) \cdot f(n)$$

Propietats dels productoris

$$\prod_{i=m}^n f(i) \cdot g(i) = \prod_{i=m}^n f(i) \cdot \prod_{i=m}^n g(i)$$

$$\prod_{i=m}^n f(i)^c = \left(\prod_{i=m}^n f(i) \right)^c$$

$$\prod_{i=m}^n c f(i) = c^{(n-m+1)} \prod_{i=m}^n f(i)$$

Exercicis:

17. (R) Calculeu $\frac{\prod_{i=2}^{n+2} a_i}{\prod_{i=2}^n a_i}$.

18. Si $A = \prod_{i=1}^n a_i$, expresseu en funció de A :

a. $\prod_{i=1}^n i a_i$

b. (R) $\prod_{i=1}^n a_i^k$

c. (R) $\prod_{i=1}^n k a_i$

d. $\prod_{i=1}^n k i a_i^k$

19. Si $A = \prod_{i=n}^m a_i$ i $B = \prod_{i=n}^m b_i$, expresseu en funció de A, B :

a. (R) $\prod_{i=n}^m a_i b_i$

b. $\prod_{i=n}^m \prod_{j=n}^m a_i b_j$

1. LÒGICA I DEMOSTRACIONS

Lògica Proposicional

Enunciat o proposició: frase o expressió correcta del llenguatge natural susceptible de ser certa o falsa. Afirmar alguna cosa que té sentit, sigui certa o falsa.

Exemples:

1. $2 + 3 = 6$.
2. la pissarra és blava.
3. són les 7h en punt.
4. si $2 + 3 = 6$ llavors la pissarra és blava.
5. són les 7h en punt i la pissarra és blava.
6. $2 + 3 = 6$ o la pissarra no és blava.

No són enunciats:

1. $2+3$
2. 6
3. la pissarra
4. Quina hora és?
5. Esborreu la pissarra!

Per poder estudiar el valor de veritat d'un enunciat és molt important reconèixer la seva forma. Observem en els exemples que hi ha uns enunciats indescomponibles o atòmics ($2+3=6$, *són les 7h en punt*, *la pissarra és blava*) i d'altres que es poden construir a partir d'aquests. Per exemple $2+3=6$ o *la pissarra no és blava*.

Per entendre millor la forma d'un enunciat, representarem els enunciats atòmics mitjançant les lletres p, q, r, \dots i farem servir els símbols $\wedge, \vee, \rightarrow$ per denotar la conjunció, la disjunció i la implicació respectivament. També usarem el símbol \neg per denotar la negació. les expressions obtingudes d'aquesta manera en direm **fórmules**. Veiem com es faria a l'exemple anterior.

Exemple: Si usem les lletres p, q, r per denotar respectivament $2 + 3 = 6$, *la pissarra és blava*, *són les 7h en punt*, les frases de l'exemple anterior quedarien formalitzades així:

1. p .
2. q .
3. r .
4. $p \rightarrow q$.
5. $r \wedge q$.
6. $p \vee \neg r$.

Les **fórmules** de la lògica proposicional es construeixen amb els símbols següents:

- **Lletres proposicionals:** p, q, r, s, \dots (**àtoms o fórmules atòmiques**)
- **Connectives lògiques:**
 - binàries: $\wedge, \vee, \rightarrow, \leftrightarrow$
 - unària: \neg

A continuació donem una definició més precisa de *fórmula de la lògica proposicional*. Les fórmules són determinades seqüències finites dels símbols anteriors. Són totes les seqüències que s'obtenen aplicant un nombre finit de vegades les regles següents.

Definició Recursiva:

- Les lletres proposicionals són fórmules
- Si ϕ és una fórmula, $\neg\phi$ també és una fórmula
- Si ϕ, ψ són fórmules i $*$ és una connectiva binària, llavors $(\phi * \psi)$ també és una fórmula

Exemples de fórmules:

$p, q, r, \neg p, (p \rightarrow q), (p \vee q), (\neg p \wedge q), \neg(\neg p \wedge q), ((p \vee q) \rightarrow r),$
 $(\neg(p \rightarrow \neg r) \leftrightarrow (p \vee \neg q)) , \dots$

Notem que:

1. Els parèntesis només es posen a les connectives binàries i **mai** a la negació: no es posa $(\neg p)$. Es fan servir per evitar ambigüitats de lectura. Per exemple, per distingir $(p \vee q) \rightarrow r$ de $p \vee (q \rightarrow r)$.
2. Els parèntesis exteriors se **suprimeixen sempre**: posem $(p \vee q) \rightarrow r$ enlloc de $((p \vee q) \rightarrow r)$.

3. Tot i que a vegades es poden suprimir més parèntesis adoptant un criteri de preferències semblant al que usem amb la suma i producte de números, aquí no ho farem (veure nota).

Nota: A títol informatiu direm que a vegades s'utilitza el conveni següent (reiterem que a l'assignatura no el farem servir): es prioritzen les connectives binàries seguint aquest ordre: $\wedge, \vee, \rightarrow, \leftrightarrow$. Es posen parèntesis de tal manera que s'executi primer \wedge , segon \vee , ... Per exemple, $p \vee q \rightarrow r$ és la fórmula $(p \vee q) \rightarrow r$, $p \wedge q \vee \neg r$ és la fórmula $(p \wedge q) \vee \neg r$, $p \wedge q \leftrightarrow \neg r \vee p$ és la fórmula $(p \wedge q) \leftrightarrow (\neg r \vee p)$.

Significat de les connectives

| ϕ | $\neg\phi$ |
|--------|------------|
| 0 | 1 |
| 1 | 0 |

| ϕ | ψ | $\phi \wedge \psi$ | $\phi \vee \psi$ | $\phi \rightarrow \psi$ | $\phi \leftrightarrow \psi$ |
|--------|--------|--------------------|------------------|-------------------------|-----------------------------|
| 0 | 0 | 0 | 0 | 1 | 1 |
| 0 | 1 | 0 | 1 | 1 | 0 |
| 1 | 0 | 0 | 1 | 0 | 0 |
| 1 | 1 | 1 | 1 | 1 | 1 |

A la fórmula $\phi \rightarrow \psi$, ϕ és l'**antecedent** i ψ és el **conseqüent**.

Les **Taules de veritat** es construeixen aplicant les regles anteriors calculant totes les combinacions de valors possibles dels àtoms. Es comença per les fórmules més senzilles.

Exemple:

| p | q | r | $\neg r$ | $p \rightarrow \neg r$ | $\neg(p \rightarrow \neg r)$ | $\neg q$ | $p \vee \neg q$ | $\neg(p \rightarrow \neg r) \leftrightarrow (p \vee \neg q)$ |
|-----|-----|-----|----------|------------------------|------------------------------|----------|-----------------|--|
| 0 | 0 | 0 | 1 | 1 | 0 | 1 | 1 | 0 |
| 0 | 0 | 1 | 0 | 1 | 0 | 1 | 1 | 0 |
| 0 | 1 | 0 | 1 | 1 | 0 | 0 | 0 | 1 |
| 0 | 1 | 1 | 0 | 1 | 0 | 0 | 0 | 1 |
| 1 | 0 | 0 | 1 | 1 | 0 | 1 | 1 | 0 |
| 1 | 0 | 1 | 0 | 0 | 1 | 1 | 1 | 1 |
| 1 | 1 | 0 | 1 | 1 | 0 | 0 | 1 | 0 |
| 1 | 1 | 1 | 0 | 0 | 1 | 0 | 1 | 1 |

Tipus de fórmules importants:

| |
|---|
| Tautologia: fórmula sempre certa (taula de veritat: columna de 1) |
| Contradicció: fórmula sempre falsa (taula de veritat: columna de 0) |
| Satisfactible: fórmula que és certa per a alguna assignació (taula de veritat conté algun 1) |

insatisfactible = contradicció

Exemples:

- Tautologies: $p \vee \neg p$, $p \rightarrow p$, $(p \wedge q) \rightarrow p$, $p \rightarrow (p \vee q)$, $p \rightarrow (q \rightarrow p)$, $(p \wedge (p \rightarrow q)) \rightarrow q$, $(\neg q \wedge (p \rightarrow q)) \rightarrow \neg p$, $((p \wedge q) \rightarrow r) \wedge (p \rightarrow q) \rightarrow (p \rightarrow r)$, ...
- Contradiccions: $p \wedge \neg p$, $(p \wedge \neg q) \wedge (p \leftrightarrow q)$, la negació de qualsevol tautologia, ...

Equivalència de fórmules

Quan dues fórmules prenen els mateixos valors de veritat (mateixa taula de veritat) es diuen **equivalents**. Per expressar que les fórmules φ i ψ són equivalents s'escriu

$$\varphi \equiv \psi$$

Totes les tautologies són equivalents. Una tautologia la denotarem per 1. De la mateixa manera totes les contradiccions són equivalents. Una contradicció la denotarem per 0.

Equivalències importants:

Quan no hi apareixen $\rightarrow, \leftrightarrow$ tota equivalència té una equivalència dual consistent en intercanviar \wedge per \vee i 0 per 1. La taula següent conté una llista d'equivalències importants juntament amb la seva dual a la columna de la dreta.

El color vermell indica que són propietats bàsiques a partir de les quals es poden deduir formalment totes les altres.

| | | |
|---------------|---|---|
| Distributiva | $\varphi \wedge (\psi \vee \theta) \equiv (\varphi \wedge \psi) \vee (\varphi \wedge \theta)$ | $\varphi \vee (\psi \wedge \theta) \equiv (\varphi \vee \psi) \wedge (\varphi \vee \theta)$ |
| De Morgan | $\neg(\varphi \wedge \psi) \equiv \neg\varphi \vee \neg\psi$ | $\neg(\varphi \vee \psi) \equiv \neg\varphi \wedge \neg\psi$ |
| Absorció | $\varphi \wedge (\varphi \vee \psi) \equiv \varphi$ | $\varphi \vee (\varphi \wedge \psi) \equiv \varphi$ |
| Idempotència | $\varphi \wedge \varphi \equiv \varphi$ | $\varphi \vee \varphi \equiv \varphi$ |
| Commutativa | $\varphi \wedge \psi \equiv \psi \wedge \varphi$ | $\varphi \vee \psi \equiv \psi \vee \varphi$ |
| Associativa | $\varphi \wedge (\psi \wedge \theta) \equiv (\varphi \wedge \psi) \wedge \theta$ | $\varphi \vee (\psi \vee \theta) \equiv (\varphi \vee \psi) \vee \theta$ |
| Neutre | $\varphi \wedge 1 \equiv \varphi$ | $\varphi \vee 0 \equiv \varphi$ |
| | $\varphi \vee 1 \equiv 1$ | $\varphi \wedge 0 \equiv 0$ |
| Complementari | $\varphi \vee \neg\varphi \equiv 1$ | $\varphi \wedge \neg\varphi \equiv 0$ |
| Doble negació | $\neg\neg\varphi \equiv \varphi$ | |
| | $\neg 1 \equiv 0$ | $\neg 0 \equiv 1$ |

Equivalències importants per a les demostracions (aquí no hi ha dual):

| | | |
|-----------------------------------|--|--|
| Traducció de la \rightarrow | $\varphi \rightarrow \psi \equiv \neg\varphi \vee \psi$ | $\neg(\varphi \rightarrow \psi) \equiv \varphi \wedge \neg\psi$ |
| Traducció de la \leftrightarrow | $\varphi \leftrightarrow \psi \equiv (\varphi \rightarrow \psi) \wedge (\psi \rightarrow \varphi)$ $\varphi \leftrightarrow \psi \equiv (\varphi \wedge \psi) \vee (\neg\varphi \wedge \neg\psi)$ | $\neg(\varphi \leftrightarrow \psi) \equiv (\varphi \wedge \neg\psi) \vee (\psi \wedge \neg\varphi)$ |
| Contrarecíproc | $\varphi \rightarrow \psi \equiv \neg\psi \rightarrow \neg\varphi$ | |
| Reducció a l'absurd | $\varphi \equiv \neg\varphi \rightarrow 0$ | $\varphi \rightarrow \psi \equiv (\varphi \wedge \neg\psi) \rightarrow 0$ |
| \vee al conseqüent | $\psi \vee \theta \equiv \neg\psi \rightarrow \theta$ | $\varphi \rightarrow (\psi \vee \theta) \equiv (\varphi \wedge \neg\psi) \rightarrow \theta$ |
| \vee a l'antecedent | $(\psi \vee \theta) \rightarrow \varphi \equiv (\psi \rightarrow \varphi) \wedge (\theta \rightarrow \varphi)$ | |

Exercici: Demostreu sintàcticament (utilitzant només les **equivalències en vermell**, sense usar taules de veritat) les equivalències següents:

1. $(\varphi \rightarrow \psi) \wedge (\psi \rightarrow \varphi) \equiv (\varphi \wedge \psi) \vee (\neg\varphi \wedge \neg\psi)$.
2. $\varphi \rightarrow \psi \equiv \neg\psi \rightarrow \neg\varphi$.
3. $\varphi \rightarrow \psi \equiv (\varphi \wedge \neg\psi) \rightarrow 0$.
4. $(\psi \vee \theta) \rightarrow \varphi \equiv (\psi \rightarrow \varphi) \wedge (\theta \rightarrow \varphi)$.
5. (R) $\neg(\varphi \leftrightarrow \psi) \equiv (\varphi \wedge \neg\psi) \vee (\neg\varphi \wedge \psi) \equiv (\varphi \vee \psi) \wedge (\neg\varphi \vee \neg\psi)$
(és coneguda com XOR o també \oplus).
6. (R) $\varphi \rightarrow (\psi \vee \theta) \equiv \varphi \wedge \neg\psi \rightarrow \theta$.
7. $\varphi \rightarrow (\psi \wedge \theta) \equiv (\varphi \rightarrow \psi) \wedge (\varphi \rightarrow \theta)$.
8. (R) $(\varphi \wedge \psi) \rightarrow \theta \equiv \varphi \rightarrow (\psi \rightarrow \theta)$.
9. (R) $q \vee (p \wedge (\neg p \vee r)) \equiv (q \vee p) \wedge ((q \vee r) \vee (p \wedge \neg p))$.

Exercici: Són equivalents $p \rightarrow (q \rightarrow (p \rightarrow q))$ i $((p \rightarrow q) \rightarrow p) \rightarrow q$?

Lògica de predicats (o lògica de primer ordre)

Relacions

Per tenir una relació hem de tenir un “domini d’individus” i una propietat d’aquests individus. Una relació d’arietat 1 és una propietat que depèn d’un sol individu. Cada individu del domini té o no té la propietat. Una relació d’arietat 2 té dos arguments;

és una propietat que depèn de dos individus. Podem pensar que és una propietat de les parelles d'individus o que relaciona els individus de la parella entre ells. Cada parella d'individus té o no té la propietat (estan relacionats entre ells o no). Una relació d'arietat 3 és una propietat que depèn de tres individus (relaciona aquests tres individus entre ells), etc.

Exemples:

1. Domini \mathbb{Z} . Les relacions “ser parell”, “ser un quadrat”, “ser múltiple de 4” són relacions d'arietat 1. Les relacions “ser menor que” ($x < y$), “ser igual que” ($x = y$), “ser congruents mòdul 5” ($x \equiv y \pmod{5}$) són relacions d'arietat 2. La relació “ x està entre y i z ” és una relació d'arietat 3. La relació “ x és congruent amb y mòdul z ” és una relació d'arietat 3.
2. Domini: Els alumnes de l'aula. Les relacions “ser alt”, “ser treballador”, “portar ulleres”, ... són relacions d'arietat 1. Les relacions “seure al costat de”, “ser amics”, “calçar el mateix número de sabata”, són relacions d'arietat 2.

Fórmules atòmiques

Es formen a partir dels símbols de relació. De la mateixa manera que les relacions, tenen una arietat que pot ser 1, 2, 3, 4, ...

- Si R és un símbol de relació d'arietat n , la següent és una fórmula atòmica:

$$R(x_1, x_2, \dots, x_n)$$

Notes:

1. A les relacions binàries (arietat 2) es pot usar notació infixa enlloc de prefixa: es pot escriure xRy enlloc de $R(x, y)$. Per exemple s'escriu: $x < y$, $x = y$, $x \leq y$, $x \in y$, ...
2. A les fórmules atòmiques també hi poden aparèixer expressions més complicades enlloc de simples variables. Com ara noms d'individus particulars, nombres... o bé expressions com ara $0, 1, y^2, x^2 + 2x \dots^1$.

Exemple: Si tenim els símbols de relació P d'arietat 1, $Q, <$ d'arietat 2 i R d'arietat 3, les següents són fórmules atòmiques: $P(x)$, $Q(x, y)$, $Q(z, z)$, $x < y$, $R(x, y, z)$, $R(x, z, x)$. També considerem fórmules atòmiques: $x > 0$, $x = y^2$, $1 \leq y^2 + y$ (aquí els símbols de relació són: $>, =, \leq$)

¹ és el que s'acostuma a denominar **termes**, però no volem donar-ne la definició formal

Fórmules de la lògica de predicats

Les fórmules de la lògica de predicats es formen a partir de les atòmiques combinant-les entre elles amb les connectives lògiques ($\wedge, \vee, \rightarrow, \leftrightarrow, \neg$) i els quantificadors:

$$\forall, \exists$$

Definició Recursiva:

- Les fórmules atòmiques són fórmules
- Si φ, ψ són fórmules i $*$ és una connectiva binària llavors $(\varphi * \psi)$ també és una fórmula
- Si φ és una fórmula $\neg\varphi$ també és una fórmula
- Si φ és una fórmula $\forall x\varphi$ i $\exists x\varphi$ també són fórmules

Exemple: Si tenim els símbols de relació P d'arietat 1, $Q, <$ d'arietat 2 i R d'arietat 3:
 $P(x), Q(x,y), x < y, R(x,y,z), \neg R(x,y,z), P(x) \rightarrow Q(x,y),$
 $\forall x(P(x) \rightarrow Q(x,y)), \exists y\forall x(P(x) \rightarrow Q(x,y)), \exists y\forall x(P(x) \rightarrow Q(x,y)) \vee \neg R(x,y,z)$
 $\forall z(\exists y\forall x(P(x) \rightarrow Q(x,y)) \vee \neg R(x,y,z)), \forall x\exists y(x > 0 \rightarrow x = y^2), \dots$

Nota: Igual que a la lògica proposicional, només es posen parèntesis a les connectives binàries i se suprimeix el parèntesi exterior.

Significat de les fórmules de la lògica de predicats

Perquè les fórmules de la lògica de predicats tinguin sentit, necessitem:

- Un domini (o univers) d'individus. És el domini de variació de les variables i sempre és no buit.
- El "significat" o "interpretació" dels símbols de relació. Han de ser relacions concretes entre individus del domini.

Llavors:

- $\forall x\varphi$ significa que *tots els individus x del domini compleixen φ .*
- $\exists x\varphi$ significa que *hi ha (almenys) un individu x del domini que compleix φ .*

Exemple: Domini \mathbb{Z} , símbols de relació: $P(x)$ (x és un parell), $Q(x)$ (x és un quadrat), $M(x)$ (x és múltiple de 4), $x < y$

| fórmula | Significat |
|--|--|
| $\forall x (M(x) \rightarrow P(x))$ | Tot enter múltiple de 4 és parell |
| $\exists x (P(x) \wedge \neg M(x))$ | Hi ha nombres parells que no són múltiples de 4 |
| $\forall x ((P(x) \wedge Q(x)) \rightarrow M(x))$ | Tot parell quadrat és múltiple de 4 |
| $\exists x (P(x) \wedge \neg M(x) \wedge \neg Q(x))$ | Hi ha nombres parells que ni són múltiples de quatre ni són quadrats |
| $P(2) \wedge \neg Q(2) \wedge \neg M(2)$ | 2 és parell però no és quadrat ni múltiple de 4 |
| $\exists x (P(x) \wedge x > 2 \wedge \neg Q(x))$ | Hi ha nombres parells més grans que 2 que no són quadrats |

Nota: A vegades, el domini de variació de les variables s'indica a la fórmula. Així, fórmules de l'exemple anterior les podem escriure: $\forall x \in \mathbb{Z}(M(x) \rightarrow P(x))$, $\exists x \in \mathbb{Z}(P(x) \wedge \neg M(x))$, $\exists x \in \mathbb{Z}(P(x) \wedge \neg M(x) \wedge \neg Q(x))$...

Equivalència

Dues fórmules de la lògica de predicats són equivalents quan prenen el mateix valor de veritat en totes les “interpretacions” possibles (en tot “domini” i en tota tota “interpretació” dels símbols de relació)

Equivalències importants:

| | |
|--|--|
| $\neg \forall x \varphi \equiv \exists x \neg \varphi$ | $\neg \exists x \varphi \equiv \forall x \neg \varphi$ |
| $\forall x \forall y \varphi \equiv \forall y \forall x \varphi$ | $\exists x \exists y \varphi \equiv \exists y \exists x \varphi$ |
| $\forall x (\varphi \wedge \psi) \equiv \forall x \varphi \wedge \forall x \psi$ | $\exists x (\varphi \vee \psi) \equiv \exists x \varphi \vee \exists x \psi$ |

Observació:

- No és certa l'equivalència: de $\forall x \exists y \varphi$ i $\exists y \forall x \varphi$.
Per exemple, si el domini són els nombres naturals $\forall x \exists y (x < y)$ és certa, en canvi $\exists y \forall x (x < y)$ és falsa.
- Tampoc són certes $\forall x (\varphi \vee \psi) \equiv \forall x \varphi \vee \forall x \psi$ ni $\exists x (\varphi \wedge \psi) \equiv \exists x \varphi \wedge \exists x \psi$.

Per exemple, si el domini són els nombres naturals, $P(x)$ és “ x és parell”, $S(x)$ és “ x és senar”, $\forall x(P(x) \vee S(x))$ és certa en canvi $\forall xP(x) \vee \forall xS(x)$ és falsa.

Exercicis. Demostreu les equivalències següents:

1. $\neg \exists x (C(x) \wedge N(x)) \equiv \forall x (C(x) \rightarrow \neg N(x)) \equiv \forall x (N(x) \rightarrow \neg C(x)) \equiv \forall x (\neg C(x) \vee \neg N(x))$.
2. $\neg \forall x (P(x) \rightarrow Q(x)) \equiv \exists x (P(x) \wedge \neg Q(x))$.
3. (R) $\exists x (P(x) \rightarrow Q(x)) \equiv \forall x P(x) \rightarrow \exists x Q(x)$.
4. (R) $\neg \forall x (P(x) \leftrightarrow Q(x)) \equiv \exists x (P(x) \wedge \neg Q(x)) \vee \exists x (Q(x) \wedge \neg P(x))$.
5. (R) Demostreu que la fórmula $\exists x (P(x) \rightarrow \forall y P(y))$ sempre és certa (sigui qui sigui P).

Formalització

Formalitzar consisteix en expressar en un llenguatge “formal” un enunciat. En el nostre cas consistirà en trobar una fórmula de la lògica de predicats. Quan formalitzem amb quantificadors es pressuposen:

- Un domini (o univers) d'individus.
- Unes relacions entre individus.

Hi ha dos **patrons** que apareixen de manera habitual:

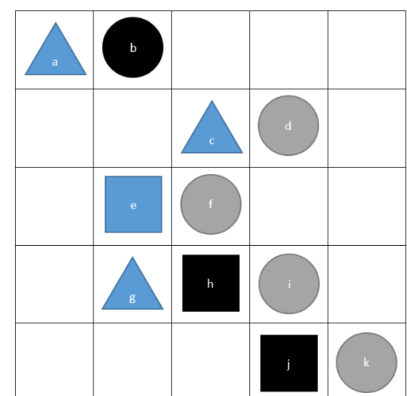
1. $\forall x (A(x) \rightarrow B(x))$ Tots els individus de tipus A (que tenen la propietat A) tenen la propietat B
2. $\exists x (A(x) \wedge B(x))$ Hi ha individus de tipus A que tenen la propietat B

ULL: Si volem expressar que x té les propietats P i Q , no es pot posar $P(Q(x))$, s'ha de posar $P(x) \wedge Q(x)$

Exercicis:

1. Un món de Tarski està format per una graella i diverses formes geomètriques que tenen un color i que poden portar una etiqueta, com a la figura. Considerem els símbols de relació següents:

$T(x)$: x és un triangle
 $C(x)$: x és un cercle
 $Q(x)$: x és un quadrat
 $B(x)$: x és blau
 $N(x)$: x és negre



$G(x)$: x és gris

$E(x,y)$: x està a l'esquerra de y

$S(x,y)$: x està a sobre de y

$K(x,y)$: x té el mateix color que y

Usant els símbols indicats, formalitzeu les frases següents:

- a. Hi ha un quadrat negre.
 - b. Tots els cercles són blaus;
 - c. No hi ha cap cercle negre.
 - d. a està a sobre de e .
 - e. Tots els cercles estan a sobre de d .
 - f. Hi ha un cercle que té el mateix color que d .
 - g. (R) d està a l'esquerra de qualsevol cercle.
 - h. (R) Alguna forma geomètrica és blava.
 - i. Algun cercle és blau.
 - j. Tots els quadrats són negres.
 - k. (R) Tots els triangles estan a l'esquerra de d .
 - l. Hi ha un triangle a l'esquerra de d .
 - m. (R) Hi ha un triangle que està a sobre de d però no a l'esquerra de a .
 - n. Algun triangle no és gris.
 - o. Tot triangle està a l'esquerra de a o a sobre de b .
 - p. (R) Cap quadrat té el mateix color que b .
2. Usant els predicats del problema anterior, expresseu en llenguatge natural les proposicions següents i determineu si a la figura anterior són certes o falses:
- a. $\forall x(B(x) \rightarrow (T(x) \vee Q(x)))$
 - b. $\exists y(C(y) \wedge \neg S(y, d))$
 - c. (R) $\forall x(N(x) \rightarrow (T(x) \vee Q(x)))$
 - d. $\exists y(C(y) \wedge S(y, d))$
 - e. (R) $\exists y(C(y) \wedge \neg E(y, d))$
 - f. $\forall x(T(x) \rightarrow \exists y(Q(y) \wedge K(x, y)))$
3. En aquest exercici el domini és el conjunt dels enters. A més de les variables, connectives i quantificadors, podeu utilitzar només els símbols següents:
- $|$, $<$, \cdot , $=$, $+$, P , Q , $0, 1, 2, 3, 4, \dots$
- $x | y$ formalitza x divideix y (o y és múltiple de x).
- $P(x)$ formalitza x és primer.
- $Q(x)$ formalitza x és un quadrat.

Formalitzeu els enunciats següents:

- a. 1 no és primer.
- b. Tot enter múltiple de 6 és també múltiple de 3 i de 2.

- c. Hi ha nombres senars que són primers i d'altres senars que no són primers.
 - d. Cap nombre primer és un quadrat.
 - e. (R) Tot enter múltiple de 3 i de 5 és múltiple de 15 .
 - f. x és un nombre parell (amb una variable lliure: la x). Les variables lliures d'una fórmula són les que no estan sota l'efecte d'un quantificador.
 - g. 2 és primer i és parell.
 - h. Tot quadrat parell és múltiple de 4 .
 - i. (R) La suma de dos senars és parell.
 - j. Tot nombre parell més gran que 2 és suma de dos primers.
 - k. (R) Tot enter positiu és suma de quatre quadrats.
4. En aquest exercici suposem que totes les variables prenen valors enters. A més de les variables, connectives lògiques i quantificadors, **només** podeu utilitzar els símbols següents: $<, \cdot, =, +, 0, 1, 2, 3, 4, \dots$ (Ull, ara no podem usar: $|, P, Q$). Formalitzeu:
- a. (R) x divideix y (x, y són variables lliures).
 - b. x és un quadrat (x variable lliure).
 - c. (R) x és un nombre primer (x variable lliure).
 - d. (R) 2 és l'únic nombre primer parell.
 - e. 2 és el nombre primer més petit.
 - f. (R) Hi ha infinits nombres primers (pista: sempre n'hi un més gran que un donat).
 - g. Tots els apartats de l'exercici anterior.

Veracitat i quantificadors

Com es justifica (o demostra) que un enunciat és cert? En general, depèn de la seva "forma". Normalment, encara que a vegades de manera no explícita, hi ha quantificadors. La justificació dependrà, en primer lloc, de si els quantificadors són existencials o universals.

Demostració d'un existencial $\exists xP(x)$:

El mètode més senzill és donar un element a del domini que tingui la propietat P . Un sol exemple és suficient.

Exemples:

1. $\exists x \in \mathbb{R} (x > 0 \wedge x^2 - 1 < 0)$ és cert.
2. $\exists x \in \mathbb{Z} (x \text{ parell} \wedge x \equiv 1 \bmod 5)$ és cert.

Això mateix s'aplica a la demostració que un enunciat universal és fals, ja que $\neg \forall x P(x) \equiv \exists x \neg P(x)$. La demostració de la falsedat de $\forall x P(x)$ es fa donant un element a del domini que **no** tingui la propietat P ; a rep el nom de **contraexemple**.

Exemples:

3. $\forall x \in \mathbb{R} (x > 0 \rightarrow x \geq 1)$ és fals.
4. $\forall x \in \mathbb{Z} (x \equiv 1 \bmod 3 \rightarrow x \text{ senar})$ és fals.

Exercicis: Dieu quins enunciats són certs i quins són falsos:

1. (R) $\exists x \in \mathbb{R} (x > 2 \wedge x < 5)$.
2. (R) $\forall x \in \mathbb{Z} (x^2 \text{ múltiple de } 16 \rightarrow x \text{ múltiple de } 8)$.
3. $\exists x \in \mathbb{R} (x > 5 \wedge x < 2)$.
4. $\forall x \in \mathbb{R} (x > 2 \rightarrow x < 5)$.
5. $\exists x \in \mathbb{R} (x^2 - x > 1 \wedge x^2 + x < 1)$.

Demostració d'un universal $\forall x P(x)$:

Hem de veure que tots els elements del domini satisfan la propietat P . Si hi ha pocs elements, ho podem verificar un a un. Si n'hi ha molts o infinits no quedarà més remei que donar-ne una "demostració". Una demostració és un raonament que segueix unes certes regles. Tot i que fer una demostració pot arribar a ser molt difícil, la comprovació que aquesta és correcte no hauria de ser-ho. Però això requereix que la demostració estigui ben escrita. A l'apartat següent explicarem com es fa això. El mateix s'aplica a la demostració que un existencial és fals.

Exemples/exercicis. $A = \{0, 1, 2, 3\}$

1. Justifiqueu que són certes:

- a. $\forall x \in A \ x^2 \leq 3x$
 - b. $\forall x \in A \ (|x - 1| < 2 \vee x^2 - 9 = 0)$
2. Justifiqueu que són falses:
- a. $\exists x \in A \ (|x + 4| = 2)$
 - b. $\exists x \in A \ (x^3 + 2x^2 - x = 4)$

Quantificadors barrejats

Demostració de:

- $\exists y \forall x P(x, y)$: donar un element y que tingui la propietat $P(x, y)$ per a cada x . Fem $y = a$ i demostrem que $\forall x P(x, a)$ és cert. La y no pot dependre de x .
Exemple: $\exists y \in \mathbb{N} \forall x \in \mathbb{N} \ y \leq x$ és cert. Fem $y = 0$ i veiem que $\forall x \in \mathbb{N} \ 0 \leq x$.
- $\forall x \exists y P(x, y)$: per a cada x cal donar una y que satisfà $P(x, y)$. La y normalment dependrà de x . Fem $y = E(x)$ i demostrem que $\forall x P(x, E(x))$ és cert.
Exemple: $\forall x \in \mathbb{N} \exists y \in \mathbb{N} \ x < y$ és cert. Fem $y = x + 1$ i veiem que $\forall x \in \mathbb{N} \ x < x + 1$.
- La demostració de la falsedat de $\exists x \forall y P(x, y)$ o de $\forall x \exists y P(x, y)$ es pot fer veient que els seus negats són certs.

Fet: La fórmula $\exists y \forall x P(x, y)$ “implica”² $\forall x \exists y P(x, y)$, però no és cert el recíproc en general.

Exercicis: En aquest exercici el domini és \mathbb{R} . Justifiqueu la veritat o falsedat de:

1. $\forall x \exists y (3x + 2y - 1 = 0)$.
2. $\exists y \forall x (3x + 2y - 1 = 0)$.
3. $\exists y \forall x \ x y = 0$.
4. $\forall x \exists y (xy - 1 = 0)$.
5. (R) $\forall x \exists y (x \neq 0 \rightarrow xy - 1 = 0)$.

² Això vol dir que sempre que la primera fórmula és certa, la segona també. Això es coneix com a conseqüència lògica.

6. (R) $\exists y \forall x \ x y = x$.
7. $\exists y \forall x \ x y = 1$.
8. (R) $\forall x \exists y \ (xy + 2y - 1 = 0)$.

| Volem demostrar | Què cal fer |
|--|---|
| $\exists x \in A \ P(x)$ Cert | Donar un exemple : Donar $a \in A$ tal que $P(a)$ |
| $\forall x \in A \ P(x)$ Fals | Donar un contraexemple : Donar $a \in A$ tal que $\neg P(a)$ |
| $\exists y \in A \ \forall x \in A \ P(x, y)$ Cert | Donar $a \in A$ tal que $\forall x \in A \ P(x, a)$ ³ |
| $\forall x \in A \ \exists y \in A \ P(x, y)$ Cert | Per a cada $x \in A$ donar $y = E(x)$ tal que $\forall x \in A \ P(x, E(x))$ ⁴ |

³ La y no pot dependre de x: és constant

⁴ La y acostuma a dependre de x, encara que en alguna ocasió pot ser constant

Demostracions

Per justificar la veracitat d'un enunciat amb quantificadors universals haurem de donar una demostració. Això és imprescindible si el domini de variació dels quantificadors és infinit o molt gran. Quan fem demostracions fem servir un llenguatge "semi-formal". Cal saber reconèixer la "forma" (l'hem de saber formalitzar) però no usarem la formalització. Per exemple, el quantificador universal no s'escriu, se sobreentén⁵.

A més, en el llenguatge semi-formal (fora de les fórmules), farem servir:

i, o, no, \Rightarrow , \Leftrightarrow

enlloc de:

\wedge , \vee , \neg , \rightarrow , \leftrightarrow

Aquests últims els reservem per les fórmules. La coma, es fa servir per representar també la conjunció. Igualment escriurem *A implica B* o *si A llavors B* com a alternativa a $A \Rightarrow B$. La majoria de vegades es treballa amb implicacions \Rightarrow . Quan estem fent una demostració de $A \Rightarrow B$, *A* rep el nom de **Hipòtesi** i *B* de **Tesi**.

Exemple: Volem demostrar que:

"per tot enter n , si n és senar llavors $n^2 + 4n - 1$ és parell"

Això, ho escriurem així (que n és un enter qualsevol es sobreentén):

n senar $\Rightarrow n^2 + 4n - 1$ parell

En primer ordre es pot formalitzar així:

$\forall x (S(x) \rightarrow P(x^2 + 4x - 1))$,

on $S(x)$ formalitza " x és senar", $P(x)$ formalitza " x és parell", i el domini són els enters.

Algunes implicacions bàsiques.

Les podem usar en qualsevol moment com a petits passos en una demostració:

Passos lògics:

⁵A vegades tampoc s'escriuen els quantificadors existencials, que també se sobreenten. Encara que això pot causar confusió al principi, es reconeixen pel context.

1. $A, B \Rightarrow A$
2. $A \Rightarrow A \vee B$
3. $A \vee B, \text{no } A \Rightarrow B$
4. $A, A \Rightarrow B \Rightarrow B$
5. $\text{no } B, A \Rightarrow B \Rightarrow \text{no } A$
6. $ABSURD \Rightarrow A$
7. $A \Rightarrow B, B \Rightarrow C \Rightarrow A \Rightarrow C$

La manera de veure que cada un d'aquest passos és correcte és comprovar que cada una de les fórmules següents són tautologies:

1. $(p \wedge q) \rightarrow p$
2. $p \rightarrow (p \vee q)$
3. $((p \vee q) \wedge \neg p) \rightarrow q$
4. $(p \wedge (p \rightarrow q)) \rightarrow q$
5. $(\neg q \wedge (p \rightarrow q)) \rightarrow \neg p$
6. $0 \rightarrow p$
7. $((p \rightarrow q) \wedge (q \rightarrow r)) \rightarrow (p \rightarrow r)$

El color vermell indica que són propietats bàsiques a partir de les quals es poden demostrar totes les altres.

Passos bàsics de la igualtat (aquí a, b, c, \dots són nombres reals):

1. $a = a$ (reflexiva)
2. $a = b \Rightarrow b = a$ (simètrica)
3. $a = b, b = c \Rightarrow a = c$ (transitiva)
4. $a = b \Rightarrow E(a) = E(b)$ (aquí $E(x)$ és una expressió on apareix x)
5. $a = b \Rightarrow a + c = b + c$
6. $a = b \Rightarrow ac = bc$
7. $a = b \Rightarrow a^2 = b^2$
8. $a = b, a' = b' \Rightarrow a + a' = b + b'$

$$9. \ a = b, \ a' = b' \Rightarrow \ aa' = bb'$$

Exercici (per fer més envant)⁶: Demostreu que totes les propietats 5,6,7,... surten de les **4 primeres** (pista: prendre $E(x)$ adequades).

Propietats bàsiques de la suma i el producte (aquí $a, b, c, ..$ són nombres reals):

1. $a + (b + c) = (a + b) + c$ (Associativa de la suma)
2. $a + b = b + a$ (Commutativa de la suma)
3. $a + 0 = a$ (0 és el neutre de la suma)
4. $a + (-a) = 0$ ($-a$ és l'invers de a per la suma)
5. $a(bc) = (ab)c$ (Associativa del producte)
6. $ab = ba$ (Commutativa del producte)
7. $a1 = a$ (1 és el neutre del producte)
8. $a \neq 0 \Rightarrow a \cdot (1/a) = 1$ ($1/a$ és l'invers de a pel producte)
9. $a(b + c) = ab + ac$ (distributiva)

Passos bàsics de l'ordre (aquí $a, b, c, ..$ són nombres reals):

1. $a \leq a$ (reflexiva de \leq)
2. $a \leq b, b \leq a \Rightarrow a = b$ (antisimètrica de \leq)
3. $a \leq b, b \leq c \Rightarrow a \leq c$ (transitiva de \leq)
4. $a \leq b$ o $b \leq a$ (total)
5. $a \leq b \Rightarrow a + c \leq b + c$ (compatibilitat amb la suma)
6. $a \leq b, c \geq 0 \Rightarrow ac \leq bc$ (compatibilitat amb el producte)
7. $a \leq b, c \leq d \Rightarrow a + c \leq b + d$
8. $a \leq b \Rightarrow -b \leq -a$
9. $a^2 \geq 0$
10. $0 \leq a \leq b \Rightarrow a^2 \leq b^2$
11. És cert $(a \leq b \Rightarrow a^2 \leq b^2)$?
12. $a \leq b \Rightarrow a^3 \leq b^3$
13. (n natural parell) $0 \leq a \leq b \Rightarrow a^n \leq b^n$

⁶ Quan hàgim fet els diferents mètodes de demostració: contrarecíproc, reducció absurd,...

14. (n natural senar) $a \leq b \Rightarrow a^n \leq b^n$
15. El recíproc de l'anterior

Exercici (per fer més envant): Demostreu que totes aquestes propietats es dedueixen de les **6 primeres**. Demostreu també les següents tenint en compte que $a < b$ és una abreviatura de $a \leq b \wedge a \neq b$.

16. $a < b, b < c \Rightarrow a < c$.
17. $a < b$ o $a > b$ o $a = b$.
18. $a < b \Rightarrow a + c < b + c$.
19. $a < b, c > 0 \Rightarrow ac < bc$.
20. $a < b, c \leq d \Rightarrow a + c < b + d$.
21. $a < b \Rightarrow -a > -b$.
22. $0 < a < b \Rightarrow a^2 < b^2$.
23. És cert $(a < b \Rightarrow a^2 < b^2)$?
24. $a < b \Rightarrow a^3 < b^3$.
25. (n natural parell) $0 < a < b \Rightarrow a^n < b^n$.
26. (n natural senar) $a < b \Rightarrow a^n < b^n$.
27. El recíproc de l'anterior.

Altres:

1. a natural, b natural $\Rightarrow a + b$ natural, ab natural.⁷
2. a enter, b enter $\Rightarrow -a$ enter, $a + b$ enter, ab enter.
3. a racional, b racional $\Rightarrow -a$ racional, $a + b$ racional, ab racional.
4. b racional, $b \neq 0 \Rightarrow 1/b$ racional.
5. a racional, b racional, $b \neq 0 \Rightarrow a/b$ racional.

Exercici: (per fer més envant): Demostreu que totes surten de la **primera** (pista: un **enter** és un element de la forma $\pm a$ amb a natural. Un **racional** és un nombre de la forma n/m amb n, m enters, $m \neq 0$).

⁷ Podem definir els naturals així: **0 és natural i si a és natural, $a+1$ és natural**. No hi ha més naturals que els que es construeixen aplicant un nombre finit de vegades aquestes regles.

A vegades les implicacions \Rightarrow són reversibles i podem usar el \Leftrightarrow en lloc de la implicació. Per exemple, els passos 5 i 8 de l'ordre són reversibles, mentre que el 19 no ho és.

Prova directa.

Volem demostrar $A \Rightarrow B$.

Sortim de la hipòtesi A i arribem a la tesi B . Els passos són petites implicacions que han d'estar molt clares. Poden ser, per exemple, qualsevol dels passos esmentats anteriorment. Si cal, les expliquem. Esquemàticament, ho podem resumir així:

| |
|--|
| Volem demostrar $A \Rightarrow B$. |
| $A \Rightarrow A' \Rightarrow A'' \Rightarrow \dots \Rightarrow B$ |

Exercicis: Demostreu que:

1. El quadrat d'un nombre enter senar és senar.
2. La suma d'un nombre parell i un nombre senar és senar.
3. El producte de dos quadrats és un quadrat.
4. (R) La suma de dos nombres senars és parell.
5. El producte de dos nombres senars és senar.
6. El quadrat d'un nombre parell és parell.
7. (R) n és enter. Si n és senar llavors $5n^2 - 1$ és parell.

Prova pel contrarecíproc.

Es basa en: $p \rightarrow q \equiv \neg q \rightarrow \neg p$

| |
|---|
| Volem demostrar $A \Rightarrow B$. |
| $\neg B \Rightarrow \dots \Rightarrow \neg A$ |

Exercicis: Demostreu que:

8. n és enter. Si n^2 és parell llavors n és parell.
9. x, y són reals. Si $x + y \leq 2$ llavors $x \leq 1$ o $y \leq 1$.
10. n és enter. Si $3n^2 + 6n + 5$ és parell llavors $n + 1$ és parell.
11. Aquí a, b, c són nombres reals positius. Si $c = ab$ llavors $a \leq \sqrt{c}$ o $b \leq \sqrt{c}$.
12. (R) n és enter. Si $5n^2 + 1$ és senar llavors n és parell.
13. n és enter. Si n^3 és senar llavors n també és senar.
14. n, m són enters. Si nm és parell llavors n és parell o m és parell.
15. (R) Siguin x, y nombres reals positius. Demostreu que si $xy > 1$ llavors $x > 1$ o $y > 1$

Reducció a l'absurd

Es basa en: $p \equiv \neg p \rightarrow 0$

| |
|--|
| Volem demostrar A |
| $\neg A \Rightarrow \dots \Rightarrow \text{Contradicció}$ |

Exercicis: Demostreu que:

16. $\sqrt{2}$ és irracional.
17. Si triem 15 dies diferents d'un calendari, n'hi ha 3 que cauen el mateix dia de la setmana.
18. Demostreu que $a + b$ és parell o $b + c$ és parell o $c + a$ és parell.
19. No hi ha cap nombre racional r tal que $r^3 + r + 1 = 0$ (useu que un zero racional, en forma reduïda, $\frac{a}{b}$ del polinomi $a_n x^n + \dots + a_1 x + a_0$ compleix que a divideix a_0 i b divideix a_n).

20. Donats n nombres reals a_1, \dots, a_n , algun d'ells ha de ser més gran o igual que la seva mitjana aritmètica $\frac{a_1 + \dots + a_n}{n}$.
 21. Idem per a la mitjana geomètrica. Aquí suposem que els nombres són tots positius.
 22. (R) a, b, c reals. Demostreu que $a \leq \frac{b+c}{2}$ o $b \leq \frac{a+c}{2}$ o $c \leq \frac{a+b}{2}$.
 23. (R) $\log_2 3$ és irracional.
 24. $2\sqrt{2}-2$ és irracional. (usar 16)
 25. Donats n nombres reals, algun d'ells ha de ser menor o igual que la mitjana aritmètica dels restants.
 26. Idem per a la mitjana geomètrica. Aquí suposem que els nombres són tots positius.
 27. (R) Demostreu que $a + c$ és senar o $b - a$ és senar o $b + c - 1$ és senar.
-

Reducció a l'absurd II

Es basa en: $p \rightarrow q \equiv (p \wedge \neg q) \rightarrow 0$

| | | |
|--|---------------------|-----------------------------------|
| Volem demostrar $A \Rightarrow B$. | | |
| $A, \neg B$ | \Rightarrow | \Rightarrow <i>Contradicció</i> |

Exercicis: Demostreu que:

28. La suma d'un nombre racional i un irracional és irracional.
29. Si a, b, c són nombres enters i $a + b + c = 0$, com a mínim un d'ells és parell.
30. Si n és un quadrat llavors $n + 2$ no és un quadrat (n enter).
31. Si p és primer llavors \sqrt{p} és irracional. (podeu usar que si a^2 és múltiple de p llavors a és múltiple de p).
32. Si p és un primer senar llavors $\log_2 p$ és irracional.
33. a, b, c són reals positius. Si $c = ab$ llavors o $a \leq \sqrt{c}$ o $b \leq \sqrt{c}$.
34. (R) El resultat de multiplicar un racional no nul que és un quadrat per un racional que no és un quadrat és un nombre racional que no és un quadrat (que un nombre racional sigui un quadrat vol dir que és igual al quadrat d'un

cert nombre racional).

35. Si a, b, c són nombres enters i $a + 3 = b + c$, com a mínim un d'ells és senar.
-

Prova d'una disjunció

Es basa en: $(q \vee r) \equiv (\neg q \rightarrow r)$

| |
|--|
| Volem provar $B \vee C$ |
| $\neg B \Rightarrow \dots \Rightarrow C$ |

També val amb més disjuntands: $p_1 \vee \dots \vee p_n \equiv (\neg p_1 \wedge \dots \wedge \neg p_{n-1}) \rightarrow p_n$

| |
|---|
| Volem provar $B_1 \vee \dots \vee B_n$: |
| $\neg B_1, \neg B_2, \dots, \neg B_{n-1} \Rightarrow \dots \Rightarrow B_n$ |

Exercicis:

36. n és enter. Demostreu que n és senar o n^2 és múltiple de 4.
37. a, b són reals. Demostreu que $a \leq \frac{a+b}{2}$ o $b \leq \frac{a+b}{2}$.
38. a, b, c són reals. Demostreu que $a \leq \frac{a+b+c}{3}$ o $b \leq \frac{a+b+c}{3}$ o $c \leq \frac{a+b+c}{3}$.
39. a, b són reals positius. Demostreu que o $a \leq \sqrt{ab}$ o $b \leq \sqrt{ab}$.
40. n és enter. Demostreu que n o $n^2 + 1$ és senar.
41. a, b, c són reals positius. Demostreu que $a \leq \sqrt[3]{abc}$ o $b \leq \sqrt[3]{abc}$ o $c \leq \sqrt[3]{abc}$.
42. a, b, c són reals. Demostreu que $a \leq \frac{b+c}{2}$ o $b \leq \frac{a+c}{2}$ o $c \leq \frac{a+b}{2}$.
43. (R) a, b són enters. Demostreu que $a - b$ és parell o $b - c$ és parell o $c - a$ és parell.
-

Disjunció al conseqüent

Es basa en: $p \rightarrow (q \vee r) \equiv (p \wedge \neg q \rightarrow r)$

| |
|--|
| Volem provar $A \Rightarrow (B \vee C)$ |
| $A, \neg B \Rightarrow \dots \Rightarrow C$ |

Amb més disjuntands:

$$p \rightarrow (q_1 \vee \dots \vee q_n) \equiv (p \wedge \neg q_1 \wedge \dots \wedge \neg q_{n-1}) \rightarrow q_n$$

| |
|--|
| Volem provar $A \Rightarrow (B_1 \vee \dots \vee B_n)$ |
| $A, \neg B_1, \neg B_2, \dots, \neg B_{n-1} \Rightarrow \dots \Rightarrow B_n$ |

Exercicis: Demostreu que:

44. La suma d'un nombre racional i un irracional és irracional (amb contrarecíproc).
45. x, y reals. Si $x + y \leq 2$ llavors $x \leq 1$ o $y \leq 1$.
46. a, b, c són enters. Si $a + 5 = c - b$ llavors a és senar o b és senar o c és senar.
47. x, y, z reals. Si $x < \frac{2y+z}{3}$ llavors $y \geq \frac{2z+x}{3}$ o $z \geq \frac{2x+y}{3}$.
48. a, b, c, d són enters. Si $a + b + c + d$ és parell llavors $a + b$ és parell o $a + c$ és parell o $a + d$ és parell. Podem afirmar que els tres són parells? Val el recíproc?
49. a, b, c són nombres reals positius. Si $c = ab$ llavors $a \leq \sqrt{c}$ o $b \leq \sqrt{c}$.
50. (R) a, b, c, d són nombres reals positius. Si $d = abc$ llavors $a \leq \sqrt[3]{d}$ o $b \leq \sqrt[3]{d}$ o $c \leq \sqrt[3]{d}$.
51. a, b, c són nombres real. Si $c = a + b$ llavors $2a \leq c$ o $2b \leq c$.
52. a, b, c són enters. Si $a + c$ és senar llavors $a + b$ és senar o $b + c$ és senar.
53. a, b, c són enters. Si $a + b + c$ és senar llavors $a - b$ és parell o c és parell.
54. x, y, z reals. Si $x < \frac{2y+3z}{5}$ llavors $y \geq \frac{2z+3x}{5}$ o $z \geq \frac{2x+3y}{5}$.
55. a, b, c són enters. Si $1 - a - 3b - 5c = 0$ llavors $a + b + c$ és senar o

- $a - b - c$ és senar o $a + b - c$ és senar. Podem afirmar que els tres són senars? Val el recíproc?
56. a, b, c són enters. Si $12 + a - b - 3c = 0$ llavors $a + 3b - c$ és parell o $a - b - 5c$ és parell o $a + b - c$ és parell.
57. a, b, c, d són enters. Si $a + b + c + d$ és senar llavors $a + b$ és senar o $a + c$ és senar o $a + d$ és senar. Podem afirmar que els tres són senars? Val el recíproc?
-

Prova per casos

Es basa en la tautologia:

$$(p_1 \vee \cdots \vee p_n) \rightarrow (p \leftrightarrow (p_1 \rightarrow p) \wedge \cdots \wedge (p_n \rightarrow p))$$

Es pot usar en qualsevol moment.

| Volem demostrar B , distingim els casos A_1, \dots, A_n | | |
|---|-------|-----------------|
| <u>Cas 1:</u> A_1 | | |
| $A_1 \Rightarrow$ | | $\Rightarrow B$ |
| ... | | |
| <u>Cas n:</u> A_n | | |
| $A_n \Rightarrow$ | | $\Rightarrow B$ |

Important: Cal que els diferents casos exhaureixin **totes** les possibilitats (es compleix $A_1 \vee \cdots \vee A_n$).

Exercicis: Demostreu que:

58. n és enter. $n^2 + n$ és parell. (2 casos)
59. La suma de dos nombres enters de la mateixa paritat és parell (2 casos).
60. Si n és enter, llavors $n^2 \geq n$ (2 o 3 casos).

61. n és enter. El residu de la divisió de n^2 per 4 no és mai 3 (4 casos).
62. Si x, y, z són nombres reals llavors:
- $\max(x, y) + \min(x, y) = x + y$ (2 casos).
 - $z \leq x$ i $z \leq y \Leftrightarrow z \leq \min(x, y)$ (2 casos).
63. Si la suma de dos nombres enters és parell llavors tenen la mateixa paritat. (amb contrarecíproc)
64. n és enter. $3n^2 + n + 3$ es senar (2 casos).
65. (R) n és enter. $n^3 + 2n$ es múltiple de 3 (3 casos).
66. Tot quadrat perfecte que no és múltiple de 3 és de la forma $3k + 1$ (2 o 3 casos).
67. n és enter. Si n no és múltiple de 3 llavors $n^2 - 1$ és múltiple de 3 (2 casos).
68. Si x, y són nombres reals llavors $|xy| = |x| \cdot |y|$ (4 casos).
69. Si x, y són nombres reals llavors $||x| - |y|| \leq |x - y|$ (6 o 8 casos).
70. Si x, y, z són nombres reals llavors:
- (R) $z \geq x$ i $z \geq y \Leftrightarrow z \geq \max(x, y)$ (2 casos).
 - (R) $\min(\min(x, y), z) = \min(x, \min(y, z)) = \min(x, y, z)$ (6 casos).
 - $\max(\max(x, y), z) = \max(x, \max(y, z)) = \max(x, y, z)$ (6 casos).
 - $\min(z + x, z + y) = z + \min(x, y)$ (2 casos).
 - $\max(z + x, z + y) = z + \max(x, y)$ (2 casos).
71. El quadrat d'un nombre enter mai acaba en 8 (10 casos).
72. Tot cub perfecte és de la forma $9k$ o $9k - 1$ o $9k + 1$ per a algun k (3 casos).
73. m, n són enters. Si $m + n$ és senar llavors mn és parell (2 casos).
-

Disjunció a l'antecedent: $(B \vee C) \Rightarrow A$

Es basa en: $(q \vee r) \rightarrow p \equiv (q \rightarrow p) \wedge (r \rightarrow p)$

És equivalent a fer una prova per casos (distingim segons B o C).

| Volem demostrar $(B \vee C) \Rightarrow A$ | | |
|--|---------------------|-----------------|
| B | \Rightarrow | $\Rightarrow A$ |
| C | \Rightarrow | $\Rightarrow A$ |

També val amb més casos:

| Volem demostrar $(B_1 \vee \cdots \vee B_n) \Rightarrow A$ | | |
|--|-------|-----------------|
| $B_1 \Rightarrow$ | | $\Rightarrow A$ |
| | | |
| $B_n \Rightarrow$ | | $\Rightarrow A$ |

Exercicis: Demostreu que:

74. n és enter. Si el residu de n al dividir per 4 és 1 o 3, el residu de n^2 és 1.
 75. n és enter. Si n acaba en 3 o en 7 llavors n^2 acaba en 9 (Pista: n acaba en 9 sii $n = 10k + 9$ per algun k enter).
 76. (R) m, n són enters. Si mn és senar llavors m i n són senars. (amb contrarecíproc)
 77. x és enter. Demostrar que si el residu de dividir x per 6 és 0, 3 o 4 llavors x^2 i x tenen el mateix residu al dividir-los per 6 (Pista: el residu de dividir x per 6 és 4 sii $n = 6k + 4$ per algun k enter. Idem els altres residus).
-

Demostració d'una equivalència

Es basa en: $p \leftrightarrow q \equiv (p \rightarrow q) \wedge (q \rightarrow p)$

| Volem demostrar $A \Leftrightarrow B$ |
|---------------------------------------|
| $A \Rightarrow B$ |
| $B \Rightarrow A$ |

Equivalència de 3 o més.

$$\begin{aligned}\text{Es basa en: } & (p_1 \leftrightarrow p_2) \wedge (p_2 \leftrightarrow p_3) \wedge \dots \wedge (p_{n-1} \leftrightarrow p_n) \equiv \\ & \equiv (p_1 \rightarrow p_2) \wedge (p_2 \rightarrow p_3) \wedge \dots \wedge (p_{n-1} \rightarrow p_n) \wedge (p_n \rightarrow p_1)\end{aligned}$$

| Volem demostrar que A_1, A_2, \dots, A_n són equivalents (dos a dos) | |
|---|-------------------|
| A_1 | $\Rightarrow A_2$ |
| A_2 | $\Rightarrow A_3$ |
| ... | |
| A_{n-1} | $\Rightarrow A_n$ |
| A_n | $\Rightarrow A_1$ |

Nota: Podem canviar l'ordre dels enunciats A_1, A_2, \dots, A_n

Exercicis: Demostreu que:

78. n és enter. n és senar si i només si $n^2 + 3$ és parell.
79. n, m és enters. Són equivalents:
- $5n + 3m$ és senar,
 - $n - 3m$ és senar,
 - n i m tenen diferent paritat .
80. x és real. Són equivalents:
- x irracional.
 - $x + 1$ irracional.
 - $x/3$ és irracional .
81. a, b són reals. Són equivalents:
- $a > \frac{a+b}{2}$.
 - $a > b$.
 - $b < \frac{a+b}{2}$.
82. n és enter. mn és parell si i només si n és parell o m és parell .
83. n és enter. Són equivalents:
- $n = 3k + 1$ per a algun k enter.
 - $n^2 + n = 9k + 2$ per a algun k enter.

- c. $n^2 + n$ no és múltiple de 3.
84. n, m són enters. Són equivalents:
- n i m tenen la mateixa paritat,
 - $n + m$ és parell,
 - $n - m$ és parell .
85. n és enter. Són equivalents:
- n parell,
 - $n + 1$ senar,
 - $3n^2 + 1$ senar .
86. x és real. Són equivalents:
- x és racional,
 - $3x - 1$ és racional,
 - $(x + 1)/2$ és racional .
87. a, b, c són reals. Són equivalents:
- $a > \frac{b+c}{2}$
 - $a > \frac{a+b+c}{3}$
 - $a - b > \frac{c-b}{2}$
88. (R) a, b són reals. Són equivalents (pista: $(a - b)^2 \geq 0$):
- $a^2 + b^2 = 2ab$
 - $a^2 + b^2 \leq 2ab$
 - $a = b$
89. a, b són reals positius. Són equivalents:
- $a > \sqrt{ab}$
 - $a > b$
 - $b < \sqrt{ab}$
90. (R) n és enter. Són equivalents:
- El residu de dividir n per 4 és 3 .
 - $n(n + 2)(n + 3)$ no és múltiple de 4 .
 - $2n^2 + n - 1$ és múltiple de 4 .
91. a, b són enters. Són equivalents:
- $a + b, ab$ parells.
 - a, b parells.
 - $a + b, a + 2b$ parells .
92. n és enter. Són equivalents:
- n és el producte de dos enters consecutius.

b. $4n + 1$ és un quadrat.

Demostració de la unicitat

Quan diem que “hi ha com a molt un x satisfent $P(x)$ ” o bé “si hi ha un x que satisfà $P(x)$ aquest és únic” estem expressant:

$$\forall x, y (P(x) \wedge P(y) \rightarrow x = y)$$

| | | |
|--|---------------------|---------------------|
| Volem veure: hi ha com a molt un x tal que $P(x)$. | | |
| $P(x), P(y)$ | \Rightarrow | $\Rightarrow x = y$ |

Nota: No afirmem que l’element x existeixi, només que no n’hi dos de diferents. O més precisament, que n’hi ha com a molt un (potser no n’hi ha cap).

Exercicis:

1. En una operació $(A, *)$ associativa ($\forall x, y, z \in A (x * (y * z) = (x * y) * z)$) el neutre (u és neutre sii $\forall x \in A (x * u = u * x = x)$), en cas d’existir, és únic.
2. En una operació $(A, *)$ associativa amb neutre u , l’invers y d’un element x (aquell element y que verifica $x * y = y * x = u$), si existeix, és únic.
3. (R) La inversa d’una matriu, si existeix, és única.

Nota: Quan volem veure que “hi ha un únic x tal que $P(x)$ ” haurem de veure dues coses: que l’element x existeix i que és únic.

Exemple: El quocient i el residu de la divisió euclidiana existeixen i són únics.

2. INDUCCIÓ



Inducció simple

El mètode de demostració per inducció simple es basa en el principi següent:

$$\forall n \geq n_0 P(n) \quad \equiv \quad P(n_0) \wedge \forall n > n_0 (P(n-1) \rightarrow P(n))$$

| | |
|---|---------------------------|
| Volem demostrar | $\forall n \geq n_0 P(n)$ |
| $P(n_0)$ $\forall n > n_0 (P(n-1) \rightarrow P(n))$ | |

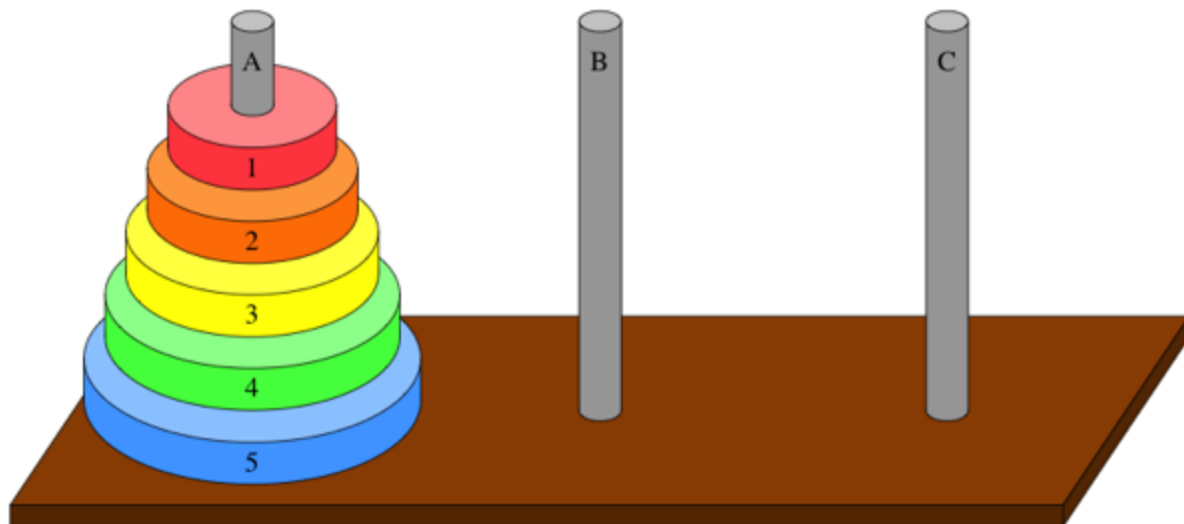
Ho presentem així:


-
- Pas Base. $P(n_0)$
 - Pas inductiu. Sigui $n > n_0$:
 - Hipòtesi d'Inducció: $P(n - 1)$
 - Volem veure(tesi): $P(n)$

En efecte:

Exercicis:

1. $\sum_{i=1}^n \frac{1}{i(i+1)} = \frac{n}{n+1}$ per a $n \geq 1$.
2. $\sum_{i=2}^n \frac{i-1}{i!} = 1 - \frac{1}{n!}$ per a $n \geq 2$.
3. $\prod_{k=2}^n (1 - \frac{1}{k}) = \frac{1}{n}$ per a $n \geq 2$.
4. $2^n \leq 2n!$ per a $n \geq 1$.
5. $\sum_{i=1}^n 1/i \leq n/2 + 1$ si $n \geq 1$.
6. Calculeu el mínim nombre de passos per resoldre el problema de les torres de Hanoi amb n discs. (Pista: considereu $f(n)$ el mínim nombre de passos per resoldre el problema amb n discs i trobeu una fórmula recurrent per calcular-la).



7. Demostreu que $2 \cdot 3^n + 5^{2n-1}$ és múltiple de 11 per a $n \geq 1$.
8. Sigui $n \geq 1$. Demostreu per inducció que si suprimim un quadrat 1×1 a un tauler d'escacs de mida $2^n \times 2^n$, la resta es pot recobrir amb peces com les de la figura.
- 
9. $\frac{1}{1 \cdot 3} + \frac{1}{3 \cdot 5} + \frac{1}{5 \cdot 7} + \cdots + \frac{1}{(2n-1)(2n+1)} = \frac{n}{2n+1}$ per a $n \geq 1$.
10. $\sum_{i=1}^n \frac{i}{2^i} = 2 - \frac{n+2}{2^n}$ per a $n \geq 1$.
11. (R) $\sum_{i=0}^n 2^i i! (2i+1) = 2^{n+1} (n+1)! - 1$ per a $n \geq 0$.
12. $\prod_{i=3}^n (1 - \frac{2}{i}) = \frac{2}{n(n-1)}$ per a $n \geq 3$.
13. Definim una successió recurrent mitjançant $a_0 = 1$, $a_{n+1} = (n+1)a_n + 1$ per a $n \geq 0$. Demostreu per inducció que $\sum_{i=0}^n \frac{1}{i!} = \frac{a_n}{n!}$ per a tot $n \geq 0$ (Càlcul del nombre e).
14. $4^n < n!$ per a $n \geq 9$.
15. (R) $\sum_{i=0}^n \frac{1}{2^{i+1}} \leq n/3 + 1$ si $n \geq 0$.
16. $(1+x)^n \geq 1+nx$ ($n \geq 0$, $x \geq 0$).
17. (difícil). Demostreu que $(\frac{n}{e})^n < n!$ per a $n \geq 1$ (Pista: useu que $(1 + \frac{1}{n})^n < e$).

18. Demostreu que $2^{3n+1} + 3 \cdot 5^{2n+1}$ és múltiple de 17 per a $n \geq 0$.

19. Demostreu que $\sum_{i=1}^n i!$ és de la forma de $90k + 63$ per a $n \geq 5$.

20. Calculeu unes quantes potències de la matriu

$$A = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}$$

Conjectureu una fórmula per calcular A^n i demostreu-la per inducció. (per si no la “trobeu” [aquí](#) teniu la fórmula).

21. Demostreu que la suma dels angles interiors d'un polígon de n costats és $180(n - 2)$ per a $n \geq 3$.

Variante: A vegades és necessari fer més d'un cas inicial:

Ho presentem així:

-
- Pas Base. $P(n_0), \dots, P(n_1)$
 - Pas inductiu. Sigui $n > n_1$:
 - Hipòtesi d'Inducció: $P(n - 1)$
 - Volem veure: $P(n)$
-

Exemple: $5^n \leq 27n!$ per a $n \geq 0$.

Inducció completa

El mètode de demostració per inducció completa es basa en el principi següent:

$$\forall n \geq n_0 \, P(n) \quad \equiv \quad P(n_0) \wedge \forall n > n_0 \, (P(n_0) \wedge \dots \wedge P(n-1) \rightarrow P(n))$$

| | |
|--|---------------------------|
| Volem demostrar | $\forall n \geq n_0 P(n)$ |
| $P(n_0)$ $\forall n > n_0 (P(n_0) \wedge \dots \wedge P(n-1) \rightarrow P(n))$ | |

Ho fem així:

-
- Pas Base: $P(n_0)$
 - Pas inductiu: per a $n > n_0$:
 - H.I. $P(n_0), P(n_0 + 1), \dots, P(n-1)$
 - Volem veure: $P(n)$
-

Els exercicis/problemes en **color fúcsia**
es faran a les classes de teoria.

Exercicis:

22. En un país, totes les ciutats estan connectades per carreteres d'un sol sentit. Demostreu que es pot fer un recorregut passant per totes les ciutats un sol cop. Pista: trieu una ciutat C i considereu d'una banda totes les ciutats a les que es pot anar desde C i a l'altra totes desde les quals es pot anar a C .
23. Demostreu que si tenim una rajola de xocolata de de $n \times m$ preses, es faci com es faci s'han de fer $nm - 1$ talls per deixar-la en trossos d'una presa.
24. Demostreu que tot nombre enter $n \geq 2$ es descomposa en producte de primers. (Pista: Useu que si un enter positiu n no és primer llavors $n = rs$ per a uns certs r, s enters, amb $2 \leq r, s < n$).

25. Definim recursivament $f : \mathbb{N} \rightarrow \mathbb{N}$ així: $f(1) = 0$ $f(n) = 2f(E(n/2)) + n$, si $n > 1$. Demostreu que $f(n) \leq n \log_2 n$ per a $n \geq 1$. (Demostrem que el nombre de comparacions que es fa amb Mergesort és $O(n \log_2 n)$).
- Nota: $E(x)$ és la part entera inferior del nombre real x .
26. Definim $f :: \mathbb{N} \rightarrow \mathbb{N}$ així: $f(1) = 0$, si $n \geq 2$, $f(n) = f(n/p) + 1$, on p és el primer més petit que divideix n . Què calcula f ? Demostreu-ho per inducció.
27. La longitud d'una fórmula proposicional és el nombre total de símbols (comptant parèntesis i repeticions) que té (aquí no suprimim els parèntesis exteriors). Demostreu que: $l(\varphi) = n(\varphi) + 4cb(\varphi) + 1$ ($l(\varphi)$ és la longitud de φ i $n(\varphi)$ és el nombre de negacions de φ i $cb(\varphi)$ és el nombre de connectives binàries de φ). Doneu una definició recursiva de la longitud de la fórmula.
28. Els joc dels mistos. Hi ha dues piles amb el mateix nombre de mistos i dos jugadors. Cada jugador tria una pila i treu com a mínim un misto d'aquesta pila. Juguen alternativament. El joc acaba quan no queden mistos i guanya l'últim que treu algun misto. Demostreu que si el segon jugador treu cada cop els mateixos mistos que el primer, guanya.
29. (difícil) Definim $x_1 = 1$, $x_{2r} = 2x_r$, $x_{2r+1} = 2x_{r+1}$ per $r > 0$. Demostreu que $x_n = 2^{ES(\log_2 n)}$ per a $n \geq 1$.
- Nota: $ES(x)$ és la part entera superior del nombre real x .

Aquesta és la versió **amb més casos inicials**:

(Se suposa que $n_0 \leq n_1$)

-
- Pas Base: $P(n_0), P(n_0 + 1), \dots, P(n_1)$
 - Pas inductiu: per a $n > n_1$:
 - H.I. $P(n_0), P(n_0 + 1), \dots, P(n - 1)$
 - Volem veure: $P(n)$
-

Exercicis:

30. Definim una successió a_n recursivament fent $a_0 = 0$, $a_1 = 2$, $a_n = 4a_{n-1} - 4a_{n-2}$ per a $n \geq 2$. Demostreu que $a_n = n2^n$ per a $n \geq 0$.
31. Demostreu que tot $n \geq 12$ es pot posar de la forma $n = 5a + 4b$ amb a, b naturals. (Pista: considereu 4 casos inicials).
32. (R) Definim una successió a_n recursivament fent $a_0 = 1$, $a_1 = 2$, $a_2 = 6$, $a_n = 6a_{n-1} - 11a_{n-2} + 6a_{n-3}$ per a $n > 2$. Demostreu que $a_n = 1 - 2^n + 3^n$ per a $n \geq 0$.
33. Definim una successió recurrent mitjançant $a_0 = -2$ i $a_{n+1} = 3a_n + 6$ per a $n \geq 0$. Demostreu per inducció que $a_n = 3^n - 3$ per a tot $n \geq 0$.
34. (R) El problema de les piles. Tenim una pila de n caixes i la volem convertir en n piles de 1 caixa. Això ho farem subdividint cada pila de k caixes en dues piles de r i s caixes, on $r + s = k$, $r, s > 0$. Li demanem a un operari que efectuï aquesta feina i cada vegada que divideix una pila de $r + s$ caixes en dues piles de r i s caixes li paguem rs euros. Demostreu que al final, independentment de l'estratègia que l'operari hagi seguit, si al principi hi ha n caixes, li pagarem $n(n-1)/2$ euros.
35. Només tenim monedes de 3 i de 4 cèntims. Demostreu que per a tot $n \geq 9$ es pot pagar una factura de n cèntims amb monedes de 3 i 4 cèntims (Pista: feu 3 casos inicials).
36. (R) Definim $f: \mathbb{N} \rightarrow \mathbb{N}$ així: $f(1) = 2$, si $n \geq 2$, $f(n) = (f(n/p))^2$, on p és el primer més petit que divideix n . Demostreu per inducció que $f(p_1^{\alpha_1} \cdots p_k^{\alpha_k}) = 2^{2^{\alpha_1 + \cdots + \alpha_k}}$ per a $n \geq 2$.
37. Considerem $f: \mathbb{N} \rightarrow \mathbb{N}$ definida per $f(n) = n$ si $n \leq 2$, $f(n) = f(E(n/3)) + f(ES(2n/3))$, altrament. Aquí E és part entera inferior i ES part entera superior. Demostreu que $f(n) \leq 2n - 1$ per a $n \geq 1$. (Pista: useu que $E(n/3) + ES(2n/3) = n$).
- Nota: $ES(x)$ és la part entera superior del nombre real x .
38. (R) Definim recursivament $f: \mathbb{N} \rightarrow \mathbb{N}$ així: $f(1) = 1$, $f(n) = f(E(n/2)) + 1$, si $n > 1$. Demostreu que $f(n) \leq \log_2 n + 1$ per a $n \geq 1$.

39. Definim recursivament $f : \mathbb{N} \rightarrow \mathbb{N}$ així: $f(1) = 0$ $f(n) = 4f(E(n/4)) + n$, si $n > 1$. Demostreu que $f(n) \leq n \log_4 n$ per a tot $n \geq 1$.
40. Demostreu que tot nombre enter $n \geq 0$ es pot escriure en base 2 (pista: feu la divisió euclidiana per 2).
41. (R) Tenim una funció de \mathbb{N} en \mathbb{R} que sabem que compleix $f(1) = 0$, $f(p) = 1$ si p és primer i $f(ab) \leq 2f(a) + f(b)$. Demostreu que $f(p_1^{\alpha_1} \cdots p_k^{\alpha_k}) \leq 2\alpha_1 + \cdots + 2\alpha_k - 1$.
42. Definim $a_0 = 1$, $a_n = a_0 - a_1 + \cdots + (-1)^{n-1} a_{n-1}$ si $n > 0$. Demostreu que $a_n = 0$ per a $n \geq 2$.
43. (Dues Induccions). Demostreu primer per inducció simple que $2 + 2 \cdot 2! + 3 \cdot 3! + \cdots + (n-1) \cdot (n-1)! = n!$ per a tot $n \geq 3$. Ara useu aquesta fórmula per fer el següent. Definim $a_1 = 1$, $a_n = a_1 + 2a_2 + \cdots + (n-1)a_{n-1}$ per $n \geq 2$. Demostreu per inducció completa que $a_n = n!/2$ per $n \geq 2$.
44. (R) Definim $x_1 = 1$, $x_{2r} = 2x_r$, $x_{2r+1} = 2x_{r+1}$ per $r > 0$. Demostreu que $x_n \leq n^2$ per a $n \geq 1$.
45. Definim una successió a_n recursivament fent $a_1 = 3$, $a_2 = 5$, $a_n = 3a_{n-1} - 2a_{n-2}$ per a $n > 2$. Demostreu que $a_n = 2^n + 1$ per a $n \geq 1$.
46. Definim una successió a_n recursivament fent $a_0 = 1$, $a_1 = 1$, $a_2 = 0$, $a_n = 4a_{n-1} - 5a_{n-2} + 2a_{n-3} + 2$ per a $n > 2$. Demostreu que $a_n = 2^n - n^2$ per a $n \geq 0$.
47. (R) Definim recursivament l'altura d'una fórmula proposicional ϕ així: $h(p) = 0$, $h(\neg\phi) = 1 + h(\phi)$, $h(\phi * \psi) = \max\{h(\phi), h(\psi)\} + 1$.
- Demostreu que el nombre de lletres proposicionals de ϕ és $\leq 2^{h(\phi)}$.
 - Demostreu que per a cada $n \geq 0$ hi ha una fórmula d'altura n que compleix la igualtat.
 - (difícil) Demostreu que per a cada $n \geq 0$ i cada m amb $1 \leq m \leq 2^n$ existeix una fórmula d'altura n amb exactament m lletres proposicionals. (Pista: feu inducció completa sobre n . Useu que tot nombre $\leq 2^n$ és de la forma $2^r + s$ amb $r < n$ i $s \leq 2^r$).

3. CONJUNTS I RELACIONS

Els conjunts són un nou tipus d'objecte.

Idea: Mena de “bossa” que conté certs objectes a l'interior, de manera desordenada. Només importa quins objectes hi són i quins no. També podem pensar en una espècie de llista on no importa l'ordre i no hi poden haver repeticions. No podem “cridar” el primer element, només podem demanar si un determinat objecte hi és o no (això és un Booleà, que s'anomena “funció característica”).

Quan un objecte x és al conjunt A direm que x **és un element de** A o que x **pertany a** A . Ho notem per $x \in A$.

Quan un objecte x no és al conjunt A direm que x **no és un element de** A o que x **no pertany a** A . Ho notem per $x \notin A$.

Notem que:

- Els elements poden ser de qualsevol tipus (números, conjunts, fórmules, llistes ...).
- Quan posem $x \in A$, A ha de ser conjunt, mentre que x pot ser qualsevol tipus d'objecte.

Descripció d'un conjunt

Per descriure un conjunt hem de dir quins elements té (i quins no té). Hi ha dues maneres de fer-ho:

Per **extensió**: Donem la “llista” (cal recordar que no importa l'ordre i no hi ha repeticions) dels seus elements entre claus:

$$A = \{1, 3, 5, 7, 9\}.$$

Per **comprensió**: Donem una propietat $P(x)$ que caracteritza els seus elements (una

propietat $P(x)$ que tenen tots els seus elements i ningú més):

$$A = \{ x \mid P(x) \} .$$

Exemple:

1. $A = \{x \mid x \text{ és enter senar, } 0 \leq x \leq 10\} .$

2. $B = \{x \mid x \in \mathbb{Z}, x \text{ és parell}\} .$

Notem que: Si $A = \{x \mid P(x)\}$ llavors,

per a tot x :

$$x \in A \Leftrightarrow P(x) \text{ cert}$$

Notació alternativa

Si volem definir el conjunt de tots els elements de B que satisfan la propietat P es pot fer alternativament així:

$$\{ x \in B \mid P(x) \} = \{ x \mid x \in B, P(x) \}$$

Exemple: $\{x \in \mathbb{Z} \mid x \text{ és parell}\} = \{x \mid x \in \mathbb{Z}, x \text{ és parell}\} .$

Notem que: Si $A = \{ x \in B \mid P(x) \}$

per a tot $x \in B$:

$$x \in A \Leftrightarrow P(x) \text{ cert}$$

Però **no** es compleix per a tot x (hi poden haver $x \notin B$ que compleixin $P(x)$).

Igualtat entre conjunts (principi d'extensionalitat)

Dos conjunts A, B són iguals si i només si tenen els mateixos elements:

$$A = B \quad \Leftrightarrow \quad \forall x (x \in A \leftrightarrow x \in B)$$

Exemple: els conjunts $\{1, 3, 5, 7, 9\}$ i $\{x \mid x \text{ és enter senar, } 0 \leq x \leq 10\}$ són iguals.
Són el mateix conjunt!

Conjunt buit

És el conjunt que no té elements i es denota per \emptyset :

$$\emptyset = \{\} = \{x \mid x \neq x\}$$

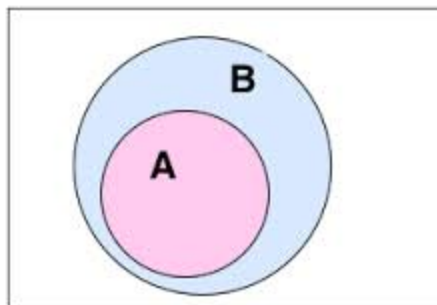
Inclusió entre conjunts (\subseteq)

Idea: A és una “part” de B : A conté “només alguns”(potser tots!) dels elements de B . Aquesta idea s'expressa més clarament dient que tots els elements de A també són elements de B :

Definició:

$$A \subseteq B \quad \Leftrightarrow \quad \forall x (x \in A \rightarrow x \in B) \text{ cert}$$

Es llegeix dient que A **és subconjunt de** B (o que A **està inclòs a** B)



Exemple: $A = \{1, 3, 5\}$, $B = \{1, 3, 5, 7, 9\}$ $A \subseteq B$.

Notem que: el principi d'extensionalitat s'expressa així:

$$A = B \quad \Leftrightarrow \quad A \subseteq B, B \subseteq A$$

Per tant, quan volem demostrar una igualtat entre conjunts, tenim una segona manera de fer-ho: demostrar les dues inclusions.

Propietats:

- $\emptyset \subseteq A$.
- $A \subseteq A$.
- $A \subseteq B$ i $B \subseteq C$ implica $A \subseteq C$.

Exercicis:

1. Demostreu les tres propietats anteriors.
2. Siguin $X = \{1, 2, 3, 4\}$, $Y = \{\{1, 2\}, \{3, 4\}\}$, $Z = \{\{1\}, \{2, 3\}, \{4\}\}$. Dieu quines afirmacions són certes i quines són falses:
 - $1 \in X, 1 \in Y, 1 \in Z$.
 - $\{1\} \in X, \{1\} \in Y, \{1\} \in Z, \{1\} \subseteq X, \{1\} \subseteq Y, \{1\} \subseteq Z$.
 - $\{3, 4\} \in X, \{3, 4\} \in Y, \{3, 4\} \in Z, \{3, 4\} \subseteq X, \{3, 4\} \subseteq Y, \{3, 4\} \subseteq Z$.
3. Demostreu que les dues fórmules següents són equivalents:
 - a. $\forall x (x \in A \leftrightarrow x \in B)$.
 - b. $\forall x (x \in A \rightarrow x \in B) \wedge \forall x (x \in B \rightarrow x \in A)$.

Operacions amb conjunts

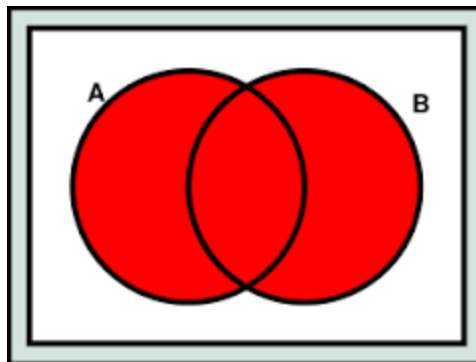
UNIÓ

Donats dos conjunts A i B definim el **conjunt unió** (o reunió) de A i B així:

$$A \cup B = \{x \mid x \in A \vee x \in B\}$$

Això es pot expressar de manera equivalent així:

$$x \in A \cup B \Leftrightarrow x \in A \vee x \in B$$



Exemple:

1. Si $A = \{1, 3, 5, 7, 9\}$ i $B = \{5, 6, 7, 8, 9, 10\}$
 $A \cup B = \{1, 3, 5, 6, 7, 8, 9, 10\}$.
2. Si $A = \{x \in \mathbb{Z} \mid x \text{ és parell}\}$ i $B = \{x \in \mathbb{Z} \mid x \text{ és senar}\}$
 $A \cup B = \mathbb{Z}$.

Propietats:

1. $A \cup A = A$.
2. $A \cup \emptyset = A$.
3. $A \cup B = B \cup A$.
4. $A \cup (B \cup C) = (A \cup B) \cup C$.

5. $A \subseteq A \cup B$, $B \subseteq A \cup B$.
6. $A \subseteq B \Leftrightarrow A \cup B = B$.
7. $A \cup B \subseteq C \Leftrightarrow A \subseteq C$, $B \subseteq C$.

Exercici:

1. Demostreu les propietats 1., 3., 5., 7. anteriors.
2. Demostreu les propietats 2.(R), 4., 6. anteriors.

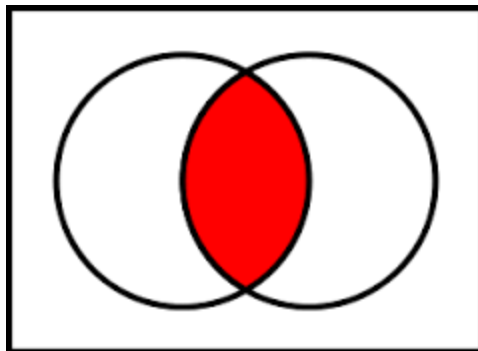
INTERSECCIÓ

Donats dos conjunts A i B definim el **conjunt intersecció** de A i B així:

$$A \cap B = \{x \mid x \in A \wedge x \in B\}$$

Això es pot expressar de manera equivalent així:

$$x \in A \cap B \Leftrightarrow x \in A \text{ i } x \in B$$



Exemple:

3. Si $A = \{1, 3, 5, 7, 9\}$ i $B = \{5, 6, 7, 8, 9, 10\}$
 $A \cap B = \{5, 7, 9\}$.
4. Si $A = \{x \in \mathbb{Z} \mid x \text{ és parell}\}$ i $B = \{x \in \mathbb{Z} \mid x \text{ és senar}\}$
 $A \cap B = \emptyset$.

Propietats:

1. $A \cap A = A$.
2. $A \cap \emptyset = \emptyset$.
3. $A \cap B = B \cap A$.
4. $A \cap (B \cap C) = (A \cap B) \cap C$.
5. $A \cap B \subseteq A$, $A \cap B \subseteq B$.
6. $A \subseteq B \Leftrightarrow A \cap B = A$.
7. $C \subseteq A \cap B \Leftrightarrow C \subseteq A \wedge C \subseteq B$.

Exercici:

1. Demostreu les propietats 2., 4. i 6. anteriors.
2. Demostreu les propietats 1., 3., 5. i 7.(R) anteriors.

Quan dos conjunts A, B no tenen elements comuns es diu que són **disjunts**:

$$A \text{ i } B \text{ són disjunts} \Leftrightarrow A \cap B = \emptyset$$

Exercici.

Expresseu mitjançant quantificadors i \in el següents fets:

3. $A = \emptyset$.
4. $\neg(A \subseteq B)$.
5. A i B son disjunts.
6. $A \subset B$. ($A \subset B$ vol dir $A \subseteq B$ i que són diferents)
7. $A \neq \emptyset$.
8. $\neg(A \subset B)$.
9. (R) $A \neq B$.
10. A i B no són disjunts.

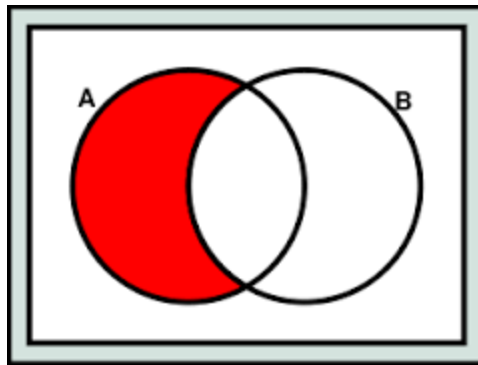
DIFERÈNCIA

Donats dos conjunts A i B definim el **conjunt diferència** de A i B així:

$$A - B = \{x \mid x \in A \wedge x \notin B\}$$

Això es pot expressar de manera equivalent així:

$$x \in A - B \Leftrightarrow x \in A \text{ i } x \notin B$$



Exemple:

5. Si $A = \{1, 3, 5, 7, 9\}$ i $B = \{5, 6, 7, 8, 9, 10\}$:

$$A - B = \{1, 3\}$$

6. Si $A = \{x \in \mathbb{Z} \mid x \text{ és parell}\}$ i $B = \{x \in \mathbb{Z} \mid x \text{ és senar}\}$:

$$A - B = A$$

Propietats:

1. $A - A = \emptyset$
2. $A - \emptyset = A$
3. $\emptyset - A = \emptyset$
4. $A - B \subseteq A$,
5. $(A - B) \cap B = \emptyset$
6. $A \subseteq B \Leftrightarrow A - B = \emptyset$
7. $C \subseteq A - B \Leftrightarrow C \subseteq A \wedge C \cap B = \emptyset$

Exercici:

1. Demostreu les propietats 1., 3., 5. i 7. anteriors.
2. Demostreu les propietats 2., 4. (R) i 6. anteriors

Altres propietats:**1. (distributiva)**

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

2. $A \cap (A \cup B) = A, \quad A \cup (A \cap B) = A$
3. $A - (B \cup C) = (A - B) \cap (A - C)$
4. $A \cup B = (A - B) \cup (B - A) \cup (A \cap B)$ i la unió és disjunta (els conjunts $(A - B), (B - A), (A \cap B)$ són disjunts 2 a 2)

Exercicis:

3. Demostreu les propietats 1. i 3. anteriors.
4. Demostreu que $A - (B - C) \subseteq (A - B) \cup C$. Val la igualtat?
5. Demostreu que $A \cup B = A \cap B$ sii $A = B$.
6. Demostreu que $(A - B) \cup (B - A) = A$ sii $B = \emptyset$.
7. Demostreu les propietats 2, i 4. anteriors.
8. Raoneu si és cert o fals i demostreu-ho:
 - a. $A - (A - B) = A \cap B$.
 - b. $(A - B) \cup B = A \cup B$.
 - c. (R) $(A \cup B) - B = A$.
 - d. (R) $(A \cup B) - (A \cap B) = (A - B) \cup (B - A)$.
 - e. $A - (B \cup C) = (A - B) \cup (A - C)$.
 - f. (R) Si $A \cup B = \emptyset$ llavors $A = B = \emptyset$.
 - g. Si $A \cap B = A \cap C$ llavors $B = C$.
9. Demostreu que $(A - B) \cap (A - C) \subseteq A - (B \cap C)$. Val la igualtat?
10. Demostreu que $A - B \subseteq C$ sii $A - C \subseteq B$ (Pista: contrarecíprocs).
11. Demostreu que si $B \cap C = \emptyset$ llavors $(A - B) \cup C \subseteq (A \cup B \cup C) - (A \cap B)$.
12. (R) Demostreu que si $B \subseteq C$ llavors $A - C \subseteq A - B$.
13. (R) Demostreu que $(A - B) \cup (B - A) = A \cup B$ sii $A \cap B = \emptyset$.

14. Demostreu que si $A \cap C \subseteq B \cap C$ i $A \cup C \subseteq B \cup C$ llavors $A \subseteq B$. (Pista: distingir segons $x \in C$ o no). Deduiu que si $A \cap C = B \cap C$ i $A \cup C = B \cup C$ llavors $A = B$.
15. Demostreu que si $A \cap B \neq \emptyset$ i $B \cap C^c = \emptyset$ llavors $A \cap C \neq \emptyset$.
16. Demostreu que $(A - B) - C \subseteq A - (B \cup C)$. Val la igualtat?
17. Demostreu que si $A \cap B = \emptyset$ llavors $A - B = A$. Val el recíproc?
18. Demostreu que si $A \cup C = B \cup C$ llavors $A - C = B - C$. Val el recíproc?
19. Definim la diferència simètrica $\Delta(A, B)$ de A, B així:
 $\Delta(A, B) = (A - B) \cup (B - A)$. Demostreu que:
- h. $\Delta(A, B) = \emptyset \Leftrightarrow A = B$
 - i. $\Delta(A, C) \subseteq \Delta(A, B) \cup \Delta(B, C)$
 - j. $\Delta(A, \Delta(B, C)) = \Delta(\Delta(A, B), C)$

COMPLEMENTARI

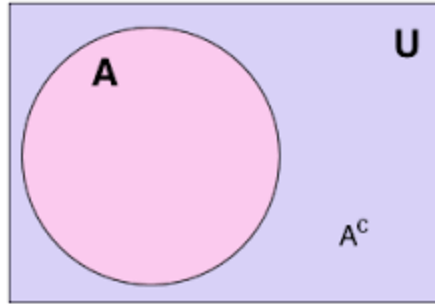
Suposem que hi ha un conjunt *gran* o *univers* Ω i tots els objectes amb els que treballarem en són elements. En particular tots els altres conjunts són subconjunts d'aquest.

Donat un conjunt A (subconjunt de Ω) definim el **conjunt complementari** de A així:

$$A^C = \Omega - A = \{x \in \Omega \mid x \notin A\}$$

Això es pot expressar de manera equivalent així:

$$x \in A^C \Leftrightarrow x \in \Omega \wedge x \notin A$$



Si suposem que $x \in \Omega$:

$$x \in A^C \Leftrightarrow x \notin A$$

Propietats: Suposem que $A, B, C \subseteq \Omega$

1. $(A^C)^C = A$.
2. $\emptyset^C = \Omega$, $\Omega^C = \emptyset$.
3. $A \cap A^C = \emptyset$, $A \cup A^C = \Omega$.
- 4.

$$\text{(De Morgan)} \quad (A \cup B)^C = A^C \cap B^C, \quad (A \cap B)^C = A^C \cup B^C.$$

5.

$$A - B = A \cap B^C$$

6. $B = A^C \Leftrightarrow A \cap B = \emptyset, A \cup B = \Omega$
7. $A \subseteq B \Leftrightarrow B^C \subseteq A^C \Leftrightarrow A \cap B^C = \emptyset \Leftrightarrow A^C \cup B = \Omega$.
8. $A \subseteq B^C \Leftrightarrow B \subseteq A^C \Leftrightarrow A \cap B = \emptyset \Leftrightarrow A^C \cup B^C = \Omega$.
9. $A^C \subseteq B \Leftrightarrow B^C \subseteq A \Leftrightarrow A^C \cap B^C = \emptyset \Leftrightarrow A \cup B = \Omega$.

Exercicis:

1. Demostreu les propietats 2., 4., 6., 8., anteriors.
2. Demostreu les propietats 1., 3., 5., 7.(R), 9., anteriors.

PARTS D'UN CONJUNT

Donat un conjunt A definim el **conjunt de les parts** (o conjunt potència) de A així:

$$P(A) = \{ x \mid x \subseteq A \}$$

Això es pot expressar de manera equivalent així:

$$x \in P(A) \Leftrightarrow x \subseteq A$$

Exemples:

$$P(\emptyset) = \{\emptyset\}$$

$$P(\{1\}) = \{\emptyset, \{1\}\}$$

$$P(\{1, 2\}) = \{\emptyset, \{1\}, \{2\}, \{1, 2\}\}$$

$$P(\{1, 2, 3\}) = \{\emptyset, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}, \{1, 2, 3\}\}$$

$$P(\{1, 2, 3, 4\}) = \{\emptyset, \{1\}, \{2\}, \{3\}, \{4\}, \{1, 2\}, \{1, 3\}, \{1, 4\}, \{2, 3\}, \{2, 4\}, \{3, 4\}, \\ \{1, 2, 3\}, \{1, 2, 4\}, \{1, 3, 4\}, \{2, 3, 4\}, \{1, 2, 3, 4\}\}$$

Nota: El nombre d'elements d'un conjunt A rep el nom de **cardinal de** A i es denota per $|A|$. Tenim: $|P(A)| = 2^{|A|}$.

Propietats:

$$\emptyset \in P(A).$$

$$A \in P(A).$$

Exercicis:

Demostreu:

1. Les 2 propietats anteriors.
2. $\{a\} \in P(A) \Leftrightarrow a \in A$.
3. $P(A \cap B) = P(A) \cap P(B)$.
4. $P(A) \cup P(B) \subseteq P(A \cup B)$. Val la igualtat?
5. $|P(A)| = 2^{|A|}$ per inducció simple sobre $|A|$.
6. $\{a, b\} \in P(A) \Leftrightarrow a \in A, b \in A$.

7. (R) $P(A) \cup P(B) = P(A \cup B) \Leftrightarrow A \subseteq B \text{ o } B \subseteq A$.
8. Si $A \subseteq B$ llavors $P(A) \subseteq P(B)$. Val el recíproc?
9. $A \cap B = \emptyset$ llavors $P(A) \cap P(B) = \{\emptyset\}$. Val el recíproc?
10. $P(A - B) \subseteq (P(A) - P(B)) \cup \{\emptyset\}$.
11. $\{A, B\} \in P(P(C)) \Rightarrow \{A \cup B\} \in P(P(C))$. Val el recíproc?
12. Són equivalents:
 - a. Per a tot x, y : $y \in x \in A \Rightarrow y \in A$.
 - b. Per a tot x : $x \in A \Rightarrow x \subseteq A$.
 - c. $A \subseteq P(A)$.
 - d. $A \in P(P(A))$.
13. $A \subseteq P(A)$ implica $P(A) \subseteq P(P(A))$. Val el recíproc?
14. (R) $A \subseteq P(A), B \subseteq P(B) \Rightarrow A \cup B \subseteq P(A \cup B)$.
15. $A \subseteq P(A), B \subseteq P(B) \Rightarrow A \cap B \subseteq P(A \cap B)$.

PRODUCTE CARTESIÀ

Parella ordenada

La parella ordenada d'objectes no la definirem formalment. Idea: la **parella ordenada** és com una llista (o vector) de longitud 2 posada entre parèntesis: (a, b)
 La propietat fonamental (que podem prendre com a "definició") de les parelles ordenades és la següent:

$$(a, b) = (c, d) \Leftrightarrow a = c, b = d$$

Producte cartesià

Donats dos conjunts A, B definim el **conjunt producte cartesià** de A per B així:

$$A \times B := \{ x \mid x = (a, b) \text{ per a uns certs } a \in A \text{ i } b \in B \}$$

Aquest conjunt també l'escriurem, de manera més informal, així:

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

Exemple:

$$\{1, 2, 3, 4\} \times \{a, b\} = \{ (1, a), (2, a), (3, a), (4, a), (1, b), (2, b), (3, b), (4, b) \}$$

Això es pot expressar de manera equivalent així:

$$x \in A \times B \Leftrightarrow x = (a, b) \text{ per a uns certs } a \in A \text{ i } b \in B$$

Sabent que els elements de $A \times B$ són tots parells ordenats, també es pot expressar així:

$$(a, b) \in A \times B \Leftrightarrow a \in A \wedge b \in B$$

Notem que: $|A \times B| = |A| \cdot |B|$

Exercici: Demostreu aquesta fórmula per inducció.

Propietats:

1. $A \times \emptyset = \emptyset$, $\emptyset \times A = \emptyset$.
2. $A \times (B \cap C) = (A \times B) \cap (A \times C)$.
3. $A \times (B \cup C) = (A \times B) \cup (A \times C)$.
4. $A \times (B - C) = (A \times B) - (A \times C)$.

Exercicis: Demostreu:

1. Les propietats 1. i 2. anteriors.
2. $A \times B = B \times A \Leftrightarrow A = B \text{ o } A = \emptyset \text{ o } B = \emptyset$.
3. Les propietats 3. i 4.(R) anteriors.
4. (R) $A \times B = C \times D$, $B \neq \emptyset$, $D \neq \emptyset \Rightarrow A = C$.
5. $(A \times A) - (B \times B) = A \times (A - B) \cup (A - B) \times A = A \times (A - B) \cup (A - B) \times (B \cap A)$.
6. $A \times B = (C \times D) \cup (E \times F)$, $B \neq \emptyset$, $D \neq \emptyset$, $F \neq \emptyset \Rightarrow A = C \cup E$.

7. (difícil) $(A \times A) - (B \times B) = (A - B) \times (A - B) \Leftrightarrow A \cap B = \emptyset \vee A \subseteq B.$

RECEPTES: Demostracions amb conjunts



Demostració de la igualtat entre conjunts (1a. manera)

| | |
|--------------------|---|
| Volem veure: | $A = B$ |
| Sigui x qualsevol: | $x \in A \Leftrightarrow \dots \Leftrightarrow \dots \Leftrightarrow x \in B$ |

Demostració d'una inclusió entre conjunts

| | |
|--------------------|---|
| Volem veure: | $A \subseteq B$ |
| Sigui x qualsevol: | $x \in A \Rightarrow \dots \Rightarrow \dots \Rightarrow x \in B$ |

Demostració de la igualtat entre conjunts (2a. manera)

| |
|--|
| Volem veure: $A = B$ |
| Demostrem dues coses: $A \subseteq B, \quad B \subseteq A$ |

Demostració que un conjunt és buit

Una bona estratègia per provar que un conjunt és buit és fer-ho per reducció a l'absurd (encara que no és pas l'únic mètode).

| |
|--|
| Volem veure: $A = \emptyset$ |
| Per reducció a l'absurd: $\exists x \in A \Rightarrow \dots \Rightarrow \dots \Rightarrow Absurd$ |

Més generalment:

Demostració on intervé que un conjunt és buit

En aquest tipus de demostracions una bona estratègia és usar contrarecíproc o reducció a l'absurd per tal que la condició “ser buit” hi apareixi negada.

Notem que:

- $A \neq \emptyset \Leftrightarrow \exists x \ x \in A$
- $A \not\subseteq B \Leftrightarrow \exists x (x \in A \wedge x \notin B)$
- $A \neq B \Leftrightarrow \exists x (x \in A \wedge x \notin B) \vee \exists x (x \in B \wedge x \notin A)$

Exercici: Useu aquesta estratègia per a demostrar que:

1. $A \cap \emptyset = \emptyset$
2. $A - A = \emptyset$
3. $\emptyset - A = \emptyset$
4. $(A - B) \cap B = \emptyset$

5. $A \cap A^C = \emptyset$
6. $\Omega^C = \emptyset$
7. $A \times \emptyset = \emptyset, \emptyset \times A = \emptyset$
8. (R) $A \subseteq B$ si i només si $A - B = \emptyset$
9. $C \subseteq (A - B)$ si i només si $C \subseteq A$ i $C \cap B = \emptyset$

RELACIONS D'EQUIVALÈNCIA

Aquí només treballarem amb relacions binàries.

Idea intuïtiva: una relació binària en un conjunt A “relaciona” parelles d'elements de A . Cada parella d'elements de A poden estar o no estar relacionats. Determinar la relació consisteix en indicar quines parelles estan relacionades i quines no.

Siguin $x, y \in A$. Si estan relacionats per la relació R ho escriurem així:

$$xRy$$

Quan no estan relacionats ho denotarem per:

$$x \not R y$$

Exemples:

Al conjunt \mathbb{Z} , les relacions següents:

- e. “tenir el mateix residu mòdul 4”
- f. “ser més petit o igual que”
- g. “ser més gran que”

Al conjunt A dels alumnes d'aquesta classe, les relacions següents:

- h. “seure al costat de”
- i. “calçar el mateix número que”
- j. “residir a menys d'un km de”

A un conjunt A qualsevol, les relacions següents:

- k. “ser igual que”
- l. la relació “buida”(ningú està relacionat amb ningú)
- m. la relació “total”(tothom està relacionat amb tothom)

Una relació R en A està determinada pel conjunt dels parells que “estan

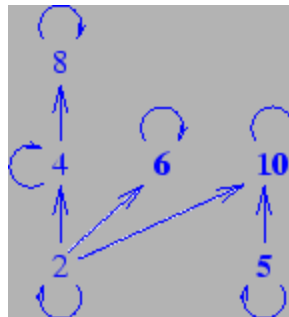
relacionats” per la relació.

Exemple: $A = \{2, 4, 5, 6, 8, 10\}$

$R = \{ (2, 2), (2, 4), (2, 6), (2, 10), (4, 4), (4, 8), (5, 5), (5, 10), (6, 6), (8, 8), (10, 10) \}$

Això vol dir, per exemple, que $2R4$ (2 està relacionat amb 4, ja que la parella $(2, 4) \in R$) en canvi 2 no està relacionat amb 3 perquè la parella $(2, 3) \notin R$.

També es poden representar les relacions mitjançant diagrames de Venn amb fletxes: cada fletxa representa una parella relacionada. L'exemple anterior seria:



En tot conjunt A sempre hi ha les relacions següents:

- La identitat en A (o igualtat), definida per: $x I_A y \Leftrightarrow x = y$:
 $I_A = \{ (x, y) \in A \times A \mid x = y \} = \{ (x, x) \mid x \in A \}$
- La relació buida (ningú està relacionat amb ningú): $R = \emptyset$
- La relació total (tothom està relacionat amb tothom) $R = A \times A$

Propietats importants que *poden tenir* les relacions:

| | |
|----------------------|--|
| Reflexiva | $\forall x \in A \ xRx$ |
| Simètrica | $\forall x, y \in A \ (xRy \rightarrow yRx)$ |
| Transitiva | $\forall x, y, z \in A \ (xRy \wedge yRz \rightarrow xRz)$ |
| Antisimètrica | $\forall x, y \in A \ (xRy \wedge yRx \rightarrow x = y)$ |

Una **relació d'equivalència** és una relació binària que és reflexiva, simètrica i transitiva.

Exercicis:

Sigui R una relació en A . Demostreu que:

1. R és reflexiva $\Leftrightarrow I_A \subseteq R$.
2. Si R és simètrica, transitiva i compleix $\forall x \in A \exists y \in A (xRy)$ llavors R és reflexiva.
3. La intersecció de relacions d'equivalència és relació d'equivalència. Més precisament: si R, S són relacions d'equivalència en A llavors la relació T definida per $xTy \Leftrightarrow xRy \wedge xSy$ és d'equivalència.
4. Si R és transitiva, llavors la relació S definida per

$$xSy \Leftrightarrow x = y \vee (xRy \wedge yRx)$$
 és d'equivalència.
5. Si R és simètrica i antisimètrica llavors $R \subseteq I_A$.
6. Si R és reflexiva, simètrica i antisimètrica llavors $R = I_A$. Val el recíproc?
7. (R) Una relació R en A es diu *circular* si verifica $\forall x, y, z \in A (xRy \wedge yRz \rightarrow zRx)$. Demostreu que una relació binària és d'equivalència \Leftrightarrow és reflexiva i circular.
8. (R) Suposem que R és irreflexiva ($\forall x \neg xRx$) i transitiva. Definim S així: $xSy \Leftrightarrow xRy \vee x = y$. Demostreu que S és reflexiva, antisimètrica i transitiva.
9. Suposem que R és reflexiva, antisimètrica i transitiva. Definim S així: $xSy \Leftrightarrow xRy \wedge x \neq y$. Demostreu que S és irreflexiva ($\forall x \neg xSx$) i transitiva.
10. (difícil i llarg) Sigui S una relació binària qualsevol en A . Definim la relació R així: $xRy \Leftrightarrow$ existeixen x_1, \dots, x_n amb $n \geq 1$ tals que $x = x_1$, $y = x_n$ i per a tot $1 \leq i < n$ es compleix: $(x_i S x_{i+1} \vee x_{i+1} S x_i)$. Demostreu que R és la més petita relació d'equivalència que conté (estén) S . Per fer això, heu de veure tres coses: 1. Que R és una relació d'equivalència. 2. Que R conté S . 3. Que si T és una relació d'equivalència que conté S llavors $R \subseteq T$ (aquí heu d'usar inducció).

11. (difícil i llarg) Sigui S una relació binària qualsevol en A . Demostreu que existeix una relació binària R en A que és la més petita relació que estén S i que es reflexiva i transitiva. Pista: modifiqueu convenientment la definició de l'exercici 10 i verifiqueu que es compleixen totes les propietats.

Classes d'equivalència i conjunt quocient

Si R és una relació d'equivalència en A i $a \in A$ la **classe de** a es defineix així:

$$\bar{a} = \{ x \in A \mid xRa \}$$

Per tant, donats $a, b \in A$ tenim:

$$b \in \bar{a} \Leftrightarrow bRa$$

Observeu que la classe de a és un subconjunt de A .

El **conjunt quocient**, que denotem per A/R , és el conjunt de totes les classes:

$$A/R = \{ x \mid x = \bar{a} \text{ per a un cert } a \in A \} = \{ \bar{a} \mid a \in A \}$$

Notem que:

1. Cada classe d'equivalència és un subconjunt del domini A .
2. El conjunt quocient A/R és un subconjunt de $P(A)$ (exercici: demostrar-ho).

Propietats de tota relació d'equivalència:

1. $x \in \bar{x}$.
2. Si $x \in \bar{y}$ llavors $\bar{x} = \bar{y}$.
3. Si $x \notin \bar{y}$ llavors $\bar{x} \cap \bar{y} = \emptyset$.
4. Les classes formen una "partició" de A . És a dir:

- a. Cada classe és no buida (ja que $x \in \bar{x}$).
- b. Dues classes diferents són disjunts: $\forall x, y \in A (\bar{x} \neq \bar{y} \rightarrow \bar{x} \cap \bar{y} = \emptyset)$.
- c. La reunió de totes les classes és A .

Exercicis:

1. Demostreu que la relació “tenir el mateix residu mòdul 4” a \mathbb{Z} és d’equivalència i que el seu conjunt quocient és $\{\bar{0}, \bar{1}, \bar{2}, \bar{3}\}$.
2. Si $A \subseteq \mathbb{Z}$, la relació “tenir els mateixos divisors primers” és d’equivalència a A . Calculeu el conjunt quocient quan $A = \{1, 2, \dots, 11, 12\}$.
3. Si B, C són conjunts i $B \subseteq C$, al conjunt $A = P(C)$ definim la relació següent: Donats $x, y \in P(C)$:

$$xRy \Leftrightarrow x \cap B = y \cap B.$$

Demostreu que és una relació d’equivalència. Si $C = \{1, 2, 3, 4\}$ i $B = \{1, 2\}$, calculeu totes les classes de R i el conjunt quocient A/R .

4. Sigui $A \subseteq \mathbb{Z}$, i a un enter fixat. La relació:

$$xRy \Leftrightarrow \text{mcm}(x, a) = \text{mcm}(y, a)$$

és una relació d’equivalència a A . Calculeu el conjunt quocient quan $A = \{1, 2, \dots, 11, 12\}$ i $a = 8$.

5. Si R és una relació d’equivalència a A i $x, y \in A$, demostreu que: $x, y \in \bar{z} \Rightarrow \bar{x} = \bar{y}$.
6. Si R és una relació d’equivalència a A i $x, y \in A$, demostreu que són equivalents:
 - a. xRy .
 - b. $x \in \bar{y}$.
 - c. $\bar{x} \cup \bar{y} = \bar{y}$.
 - d. $\bar{x} = \bar{y}$.
 - e. Existeix $z \in A$ tal que $\bar{z} \subseteq \bar{x} \cap \bar{y}$.
 - f. Per a tot $z \in A$, si $\bar{x} \cap \bar{z} \neq \emptyset$ llavors $\bar{y} \cap \bar{z} \neq \emptyset$.

7. Sigui $A \subseteq \mathbb{Z}$, i a un enter fixat. Demostreu que la relació en el conjunt A :

$$xRy \Leftrightarrow \text{mcd}(x, a) = \text{mcd}(y, a)$$

és una relació d’equivalència a A . Calculeu el conjunt quocient quan $A = \{1, 2, \dots, 11, 12\}$ i $a = 8$.

8. (R) Sigui $A \subseteq \mathbb{Z}$, i s l’aplicació $s: \mathbb{N} \rightarrow \mathbb{N}$ definida per $s(n) =$ la suma dels

dígits de n expressat en base 10. Demostreu que la relació

$$xRy \Leftrightarrow s(x) = s(y)$$

és una relació d'equivalència a A . Calculeu el conjunt quocient quan $A = \{4, 44, 42, 22, 36, 8, 11, 35, 13, 15, 17, 18, 51, 33, 6\}$.

9. (R) Si B, C són conjunts i $B \subseteq C$, al conjunt $A = P(C)$ definim la relació següent: Donats $x, y \in P(C)$:

$$xRy \Leftrightarrow x \cup B = y \cup B.$$

Demostreu que és una relació d'equivalència. Si $C = \{1, 2, 3, 4\}$ i $B = \{1, 2\}$, calculeu totes les classes de R i el conjunt quocient A/R .

10. (R) A \mathbb{Z} definim la relació següent:

$$\text{Donats } x, y \in \mathbb{Z}, \quad xRy \Leftrightarrow x^2 + 3y = y^2 + 3x.$$

Demostreu que és d'equivalència, calculeu les classes de 0, 1, 2, 3, 4. Calculeu la classe \bar{n} d'un element qualsevol n i el conjunt quocient \mathbb{Z}/R .

11. A \mathbb{R} definim la relació següent:

$$\text{Donats } x, y \in \mathbb{R}, \quad xRy \Leftrightarrow xy > 0 \vee x = y = 0.$$

Demostreu que és d'equivalència, calculeu totes les classes i el conjunt quocient \mathbb{R}/R .

12. (R) Considerem la relació "tenir la mateixa part entera" a \mathbb{R} . Demostreu que és d'equivalència, calculeu les classes de 1.2, π , -1.2 . Descriviu el conjunt quocient.

13. (R) Si $A = \mathbb{Z} \times \mathbb{Z}$, considerem la relació: $(x, y) R (x', y') \Leftrightarrow xy = x'y'$. Demostreu que és d'equivalència, calculeu les classes de (1, 0), (1, 1), (2, 1), (2, 3), $(-2, 4)$. Descriviu el conjunt quocient.

14. (R alguna) Si R és una relació d'equivalència a A i $x, y \in A$, demostreu que són equivalents:

a. $\bar{x} \cap \bar{y} \neq \emptyset$.

b. $\bar{x} \subseteq \bar{y}$.

c. $\bar{x} \cap \bar{y} = \bar{y}$.

d. Existeix $z \in A$ tal que $\bar{x} \cup \bar{y} \subseteq \bar{z}$.

e. Existeix $z \in A$ tal que $\bar{x} \subseteq \bar{z} \subseteq \bar{y}$.

f. Per a tot $z \in A$, si $\bar{z} \subseteq \bar{x}$ llavors $\bar{y} \subseteq \bar{z}$.

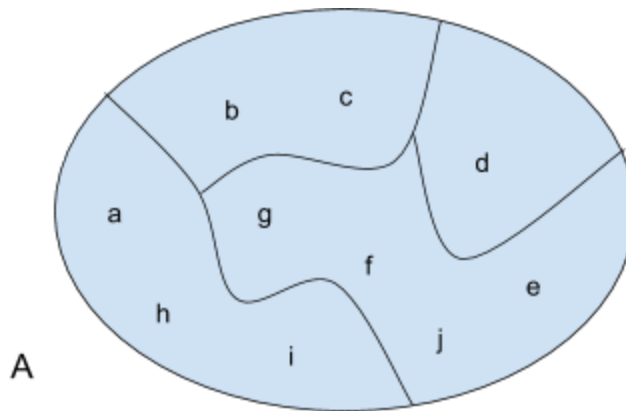
15. Si R és una relació d'equivalència a A i $x, y, z \in A$, demostreu que si

$\bar{z} \subseteq \bar{x} \cap \bar{y}$ llavors $\bar{x} \cup \bar{y} \subseteq \bar{z}$.

16. Demostreu que en una relació d'equivalència no hi ha dues classes diferents, una continguda a l'altre.
17. (R) Demostreu que en una relació d'equivalència es verifica: si $\bar{x} \cap \bar{y} \neq \emptyset$ i $\bar{x} \cap \bar{z} \neq \emptyset$ llavors $\bar{y} \cap \bar{z} \neq \emptyset$.
18. (difícil i llarg) Sigui S una relació a A que és reflexiva i transitiva. Demostreu que la relació R definida per $xRy \Leftrightarrow xSy \wedge ySx$ és d'equivalència. En el conjunt quocient A/R definim la relació binària següent: $\bar{x}T\bar{y} \Leftrightarrow xSy$. Demostreu que està ben definida (no depèn del representant: $xSy, xRx', yRy' \Rightarrow x'Sy'$) i satisfà les propietats reflexiva, antisimètrica i transitiva (és una relació d'ordre parcial).

PARTICIONS

La idea de partició és molt senzilla: tenim un conjunt A i el trenquem (o repartim) en trossos.



En el dibuix hem trencat el conjunt $A = \{a, b, c, d, e, f, g, h, i, j\}$ en 4 trossos: $\{b, c\}$ $\{d\}$ $\{e, f, g, j\}$ $\{a, h, i\}$.

El conjunt format per aquestes 4 parts és una partició de A :

$$\{ \{b, c\}, \{d\}, \{e, f, g, j\}, \{a, h, i\} \}$$

Definició. Una **partició** P de A és un conjunt de subconjunts no buits de A , disjunts 2 a 2 i tal que la seva reunió és el total.

Més precisament: P és una partició de A si :

- $\forall B \in P \quad B \subseteq A$ (de manera equivalent: $P \subseteq P(A)$).
- $\forall B \in P \quad B \neq \emptyset$.
- $\forall B \in P \forall C \in P (B \neq C \rightarrow B \cap C = \emptyset)$.
- Si $P = \{A_1, A_2, \dots, A_n\}$ llavors $A = A_1 \cup A_2 \cup \dots \cup A_n$
($\forall x \in A \exists B \in P \quad x \in B$ si la partició no és finita).

Exemples:

1. $\{\{1\}, \{2, 3\}, \{4\}, \{5, 6, 7\}\}$ és una partició de $\{1, 2, 3, 4, 5, 6, 7\}$
2. $\{\{1, 3, 5\}, \{2, 3\}, \{4\}, \{5, 6, 7\}\}$ **no** és una partició de $\{1, 2, 3, 4, 5, 6, 7\}$
3. $\{\{1\}, \{2, 3\}, \{4\}, \{6, 7\}\}$ **no** és una partició de $\{1, 2, 3, 4, 5, 6, 7\}$

Exercici: Trobeu totes les particions del conjunt $\{1, 2, 3, 4\}$.

Hem vist que si R és una relació d'equivalència a A , llavors A/R és una partició de A .

Si P és una partició de A , cada element x de A pertany a una única “part” (element de P). És a dir, per a cada $x \in A$ hi ha un únic $B \in P$ tal que $x \in B$.

Llavors podem definir una relació R així:

$$xRy \Leftrightarrow x \text{ i } y \text{ pertanyen al mateix } B \in P$$

És fàcil veure que és una relació d'equivalència. Llavors, si $x \in B \in P$ resulta que $\bar{x} = B$. Per tant el conjunt quocient $A/R = P$.

Exercicis:

1. A $\mathbb{R} \times \mathbb{R}$ considerem la relació “estar a la mateixa distància de l'origen”.
 - Proveu que R és una relació d'equivalència.
 - Dibuixeu en el pla la classe del punt $(1, 0)$.
 - Dibuixeu en el pla la classe del punt (a, b) .
 - Doneu el conjunt quocient.
 - Quina partició determina? Dibuixeu les classes.
2. (R) Considerem a $\mathbb{R} \times \mathbb{R}$ la relació següent:

$$(x, y)R(z, t) \Leftrightarrow |x| + |y| = |z| + |t| .$$

- Proveu que R és una relació d'equivalència.
 - Dibuixeu en el pla la classe del punt $(1, 0)$.
 - Dibuixeu en el pla la classe del punt (a, b) .
 - Doneu el conjunt quocient.
 - Quina partició determina? Dibuixeu les classes.
3. A $\mathbb{Z} - \{0\}$ es defineix la relació: dos enters estan relacionats si i només si tenen mateix signe i mateixa paritat o diferent signe i diferent paritat. Demostreu que és una relació d'equivalència i descriviu les classes i el conjunt quocient.
4. (R) Definim la funció $f : \mathbb{R} \times \mathbb{R} \rightarrow \{-1, 0, 1\}$ així:
- $f(x, y) = 1$ si $xy > 0$.
 - $f(x, y) = 0$ si $xy = 0$.
 - $f(x, y) = -1$ si $xy < 0$.
- A $\mathbb{R} \times \mathbb{R}$ definim la relació: $(x, y)R(u, v)$ sii $f(x, y) = f(u, v)$. Demostreu que és una relació d'equivalència i descriviu les classes i el conjunt quocient.

4. FUNCIONS

Una **funció** (o **aplicació**) f consta d'un conjunt "d'origen" A , un conjunt de "destí" B i una "regla" que associa a cada element $x \in A$ **un únic** element $y \in B$.

Més formalment, la "regla" és una relació $R \subseteq A \times B$ que satisfà:

- $\forall x \in A \exists y \in B (x, y) \in R$
- $\forall x \in A \forall y, y' \in B ((x, y) \in R \wedge (x, y') \in R \rightarrow y = y')$

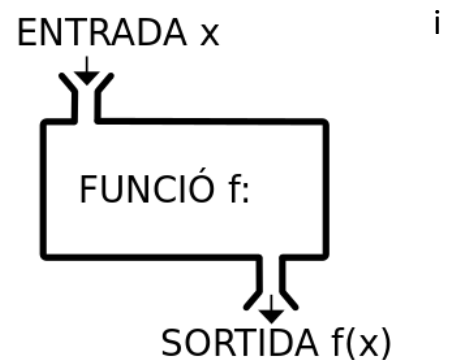
A l'únic $y \in B$ tal que $(x, y) \in R$ li diem **la imatge** de x i el denotem per $f(x)$.

Així, les dues propietats anteriors les podem expressar:

- $\forall x \in A f(x) \in B$
- $\forall x, x' \in A (x = x' \rightarrow f(x) = f(x'))$

Quan aquestes dues condicions es compleixen direm que f **està ben definida**.

Intuïtivament: la "regla" és com una mena de programa, A és el conjunt de les entrades possibles i B és un conjunt que conté totes les sortides possibles (potser és més gran que el conjunt de totes les sortides!). A correspon a una "especificació" de l'entrada del programa: A és el conjunt d'objectes que satisfan la *precondició* del programa. B correspondria a una "especificació" de la sortida: B és el conjunt d'objectes que satisfan la *postcondició* del programa.



Exemple: Les funcions hash. Les funcions hash són funcions que a paraules binàries de longitud arbitrària els hi assignen de manera eficient paraules binàries de longitud fixa. Un dels aspectes importants de les “funcions hash” és que són funcions: si dues entrades tenen hash diferent és que són diferents: (si $h(x) \neq h(y)$ llavors $x \neq y$). Per exemple, *MD5* (Message Digest 5) és una funció que, a cada paraula binària (de qualsevol longitud) li fa correspondre una paraula binària (el seu hash o resum criptogràfic) de 128 bits.

$$\begin{aligned} h : \{0, 1\}^* &\rightarrow \{0, 1\}^{128} \\ m &\rightarrow h(m) \end{aligned}$$

Això serveix per detectar possibles alteracions de la paraula original quan s’envia a través d’un canal de comunicació o s’emmagatzema. Si el missatge/arxiu que hem rebut/emmagatzemat no es correspon amb el seu hash és que ha estat alterat (voluntària o accidentalment). Imaginem que rebem/guardem el missatge/arxiu m juntament amb el seu hash h . Quan rebem/llegim verifiquem $h(m) = h$, i si això no es compleix llavors segur que el missatge/arxiu m és corrupte (ha estat modificat). En aquest punt és essencial que *MD5* sigui una funció: si $h(m_1) \neq h(m_2)$ llavors $m_1 \neq m_2$.

Notació:

$$f : A \rightarrow B, \quad x \rightarrow f(x)$$

Terminologia:

- El conjunt A rep el nom de **domini** o més informalment conjunt d’origen, mentre que a B l’hi direm **codomini** (informalment parlarem de conjunt de destí o arribada). Intentarem evitar la paraula “sortida” perquè es pot referir tant al domini com al codomini.
- $f(x)$ és **la** imatge de x .
- Si $f(x) = y$, x és **una** antiimatge de y , y és **la** imatge de x .
- Quan diem que $f : A \rightarrow B$ **està ben definida** volem dir que es compleixen les dues condicions de la definició: Cada $x \in A$ té una única imatge $f(x)$ i aquesta pertany a B .

Exemples 1:

1. $f: \mathbb{R} \rightarrow \mathbb{R}$ definida per $f(x) = e^x$.
2. $f: \mathbb{Z} \rightarrow \mathbb{N}$ definida per $f(x) = |x|$.
3. $f: \mathbb{Q} \rightarrow \mathbb{Q}$ definida per $f(x) = \frac{3x-5}{4}$.
4. $f: \mathbb{Q} \rightarrow \mathbb{R}$ definida per $f(x) = \frac{3x-5}{4}$.
5. $f: \mathbb{R} \rightarrow \mathbb{R}$ definida per $f(x) = \frac{3x-5}{4}$.
6. $f: \{1, 2, 3\} \rightarrow \{a, b, c, d\}$ definida per $f(1) = d, f(2) = d, f(3) = c$.
7. La identitat en A , que denotem per I_A , és l'aplicació $I_A: A \rightarrow A$ definida per $I_A(x) = x$.
8. $h: \{0, 1\}^* \rightarrow \{0, 1\}$ definida per $h(b_1 b_2 \cdots b_n) = b_1 \oplus b_2 \oplus \cdots \oplus b_n$. Aquí $\{0, 1\}^*$ denota el conjunt de paraules binàries i $b_1 \oplus b_2$ denota el residu de dividir $b_1 + b_2$ per dos. Observeu que $b_1 \oplus b_2 \oplus \cdots \oplus b_n$ és un *bit de paritat*: val 0 quan $b_1 + b_2 + \cdots + b_n$ és parell i val 1 quan $b_1 + b_2 + \cdots + b_n$ és senar.

Observacions importants:

1. Tot element $x \in A$ té **una única** imatge que denotem per $f(x)$.
2. Si $y \in B$, les antiimatges de y són els $x \in A$ tals que $f(x) = y$. Podem pensar que són les solucions $x \in A$ de l'equació $f(x) = y$. En aquesta equació la incògnita és x (la y és un "paràmetre"). Els elements $y \in B$ poden no tenir cap antiimatge, poden tenir-ne una de sola o tenir-ne moltes, depenent de y .

Exemples 2:

1. La funció $f: \mathbb{R} \rightarrow \mathbb{R}$ definida per $f(x) = \sin(x)$. L'element $y = -2$ no té antiimatge, mentre que $y = 0$ té infinites antiimatges.
2. La funció $f: \mathbb{R} \rightarrow \mathbb{R}$ definida per $f(x) = x^2$. L'element $y = -2$ no té antiimatge. L'element $y = 2$ té dues antiimatges, mentre que $y = 0$ té una única antiimatge.

Igualtat entre aplicacions

Dues aplicacions són iguals quan tenen el mateix domini, el mateix codomini i la mateixa "regla". Si el domini o el codomini són diferents, les aplicacions són

automàticament diferents.

Si tenim dues aplicacions amb el mateix domini i mateix codomini llavors n'hi ha prou que tinguin la mateixa "regla":

| |
|---|
| Donades $f, g : A \rightarrow B$ $f = g$ si i només si $\forall x \in A \ f(x) = g(x)$ |
|---|

Exemples 3:

- Les funcions $f : \mathbb{R} \rightarrow \mathbb{R}$ definida per $f(x) = x^2 + 1$, $g : \mathbb{Z} \rightarrow \mathbb{Z}$ definida per $g(x) = x^2 + 1$ i $h : \mathbb{Z} \rightarrow \mathbb{R}$ definida per $h(x) = x^2 + 1$ són totes tres diferents.
- Les funcions $f, g : \{1, 2\} \rightarrow \mathbb{Z}$ definides per $f(x) = x^2$ i $g(x) = 3x - 2$ són iguals (són la mateixa funció!).

Propietats importants que *poden tenir* les aplicacions $f : A \rightarrow B$

| | |
|-------------------|---|
| Injectiva | $\forall x, x' \in A \ (f(x) = f(x') \rightarrow x = x')$ |
| Exhaustiva | $\forall y \in B \ \exists x \in A \ f(x) = y$ |
| Bijectiva | Injectiva i exhaustiva |

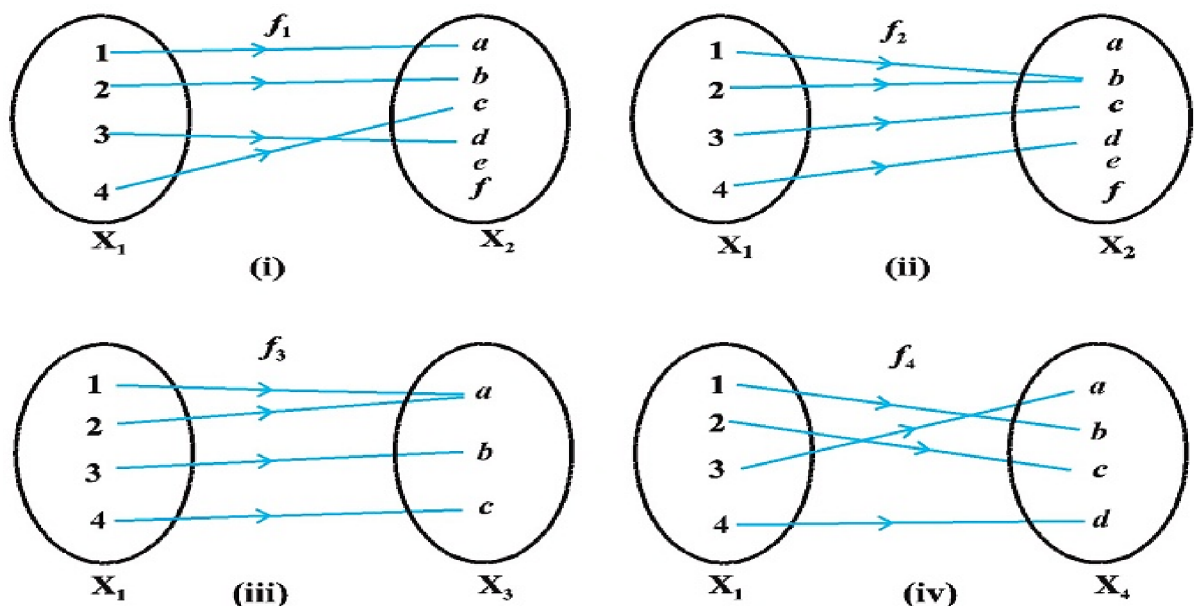


Fig 1.2 (i) to (iv)

Notem que:

Donada $f : A \rightarrow B$:

- f és injectiva \Leftrightarrow tot $y \in B$ té com a molt una antiimatge.
 - f és exhaustiva \Leftrightarrow tot $y \in B$ té com a mínim una antiimatge.
 - f és bijectiva \Leftrightarrow tot $y \in B$ té una única antiimatge.
-

Exemples:

1. En els Exemples 1: la 1 és injectiva i no exhaustiva, 2 és exhaustiva i no injectiva, 3 és bijectiva, 4 és injectiva i no exhaustiva, 5 és bijectiva, 6 és no injectiva i no exhaustiva. 7 és bijectiva.
2. $f : \mathbb{Z} \rightarrow \mathbb{N}$ definida per $f(x) = 2x - 1$, si $x > 0$, $f(x) = -2x$, si $x \leq 0$ és bijectiva.
3. La identitat I_A és bijectiva.

Exercicis:

1. Estudieu la injectivitat, exhaustivitat i bijectivitat de les funcions definides per $f(x) = |x|$, segons f va de \mathbb{Z}, \mathbb{N} en \mathbb{Z}, \mathbb{N} (hi ha 4 funcions diferents).
2. (R) Determineu si les funcions de \mathbb{Z} en \mathbb{Z} següents són injectives, exhaustives i/o bijectives.
 - a. $n \rightarrow n - 1$.
 - b. $n \rightarrow n^2 + 1$.
 - c. $n \rightarrow n^3$.
 - d. $n \rightarrow E(n/2)$.

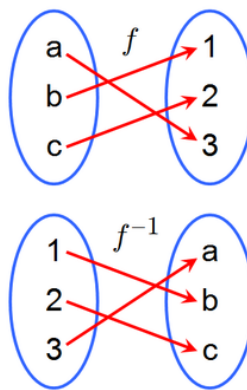
Aquí E indica la funció part entera inferior.

3. Considerem l'aplicació $f : \mathbb{N} \rightarrow \mathbb{N}$ definida per $f(n) = n + 1$ si n és parell; $f(n) = 2n$ si n és senar. Demostreu que f és injectiva però no és exhaustiva.
4. (R) Sabem que $f : \mathbb{N} \rightarrow \mathbb{N}$ és injectiva. Considerem l'aplicació $g : \mathbb{N} \rightarrow \mathbb{N}$ definida per $g(x) = 2f(x) + 3$. Demostreu que g és injectiva.
5. Siguin A, B conjunts on B no és buit. Demostreu que l'aplicació $f : A \times B \rightarrow A$ definida per $f(x, y) = x$ és exhaustiva.
6. Siguin A, B conjunts i $b \in B$. Demostreu que l'aplicació $f : A \rightarrow A \times B$

definida per $f(x) = (x, b)$ és injectiva.

7. (R) Sabem que $f: \mathbb{Z} \rightarrow \mathbb{Z}$ és exhaustiva. Considerem l'aplicació $g: \mathbb{Z} \rightarrow \mathbb{Z}$ definida per $g(x) = f(x+1) - 3$. Demostreu que g és exhaustiva.
8. Sabem que $f: \mathbb{Z} \rightarrow \mathbb{N}$ és injectiva. Considerem l'aplicació $g: \mathbb{Z} \rightarrow \mathbb{N}$ definida per $g(x) = 3f(x)^2 + 1$. Demostreu que g és injectiva però no exhaustiva.
9. Sabem que $f: \mathbb{Z} \rightarrow \mathbb{N}$ és exhaustiva. Considerem l'aplicació $g: \mathbb{Z} \rightarrow \mathbb{N}$ definida per $g(x) = E(f(x)/2)$. Demostreu que g és exhaustiva però no injectiva. Aquí E indica la funció part entera inferior.

Funció inversa



Intuitivament, la “inversa” d’una funció és “la mateixa aplicació però en sentit invers”(les mateixes “fletxes” amb el sentit canviat). Això té un problema: si un element $y \in B$ no té antiimatge, no li podem fer “correspondre” cap element $x \in A$. Per aquesta raó necessitem que l’aplicació sigui exhaustiva. De la mateixa manera, si un element $y \in B$ té moltes antiimatges, li haurem de fer “correspondre” molts elements $x \in A$. Així també necessitem que l’aplicació sigui injectiva. Tot plegat: per poder fer la “inversa” d’una aplicació, aquesta ha de ser bijectiva.

Definició. Si $f: A \rightarrow B$ és bijectiva, sabem que tot element $y \in B$ té una única antiimatge. Llavors la **funció inversa** de f , que denotem per f^{-1} , és l’aplicació que va de B a A i que a tot $y \in B$ l’hi fa correspondre la seva única antiimatge.

| |
|--|
| $f : A \rightarrow B$ <u>bijectiva</u> |
| $f^{-1} : B \rightarrow A$ $f^{-1}(y) :=$ l'única antiimatge de $y =$ l'únic $x \in A$ tal que $f(x) = y$ |

Notem que:

- Cal que f sigui bijectiva, sinó la inversa no existeix.
- $f^{-1}(y) = x \Leftrightarrow f(x) = y$

Exercicis. Demostreu que estan ben definides, són bijectives i calculeu la inversa de:

1. $f : \mathbb{Q} \rightarrow \mathbb{Q}$, definida per $f(x) = \frac{3x-5}{4}$.
2. $f : [5/3, \infty) \rightarrow [0, \infty)$ definida per $f(x) = \sqrt{\frac{3x-5}{4}}$.
3. $f : \mathbb{R} - \{1/3\} \rightarrow \mathbb{R} - \{2/3\}$ definida per $f(x) = \frac{2x+5}{3x-1}$.
4. (R) $f : \mathbb{Z} \rightarrow \mathbb{N}$ definida per $f(x) = 2x - 1$, si $x > 0$, $f(x) = -2x$, si $x \leq 0$.
5. $f : (-\infty, 3) \rightarrow \mathbb{R}$ definida per $f(x) = \ln(6 - 2x)$.
6. $f : \mathbb{R} \rightarrow (1, \infty)$ definida per $f(x) = 2e^{x-1} + 1$.
7. $f : [-\pi/2, \pi/2] \rightarrow [-1, 1]$ definida per $f(x) = \sin(x)$.
8. $f : [10, 11] \rightarrow [10, 11]$ definida per $f(x) = \cos(\pi x - 10\pi)/2 + 21/2$.
9. (R) $f : X \rightarrow X$, on $X = \{1, 2, 3, 4, \dots, 99, 100\}$ i f definida per $f(x) = 2x$, si $1 \leq x \leq 50$, $f(x) = 2(x - 51) + 1$, si $51 \leq x \leq 100$.

Propietat:

Si f és bijectiva llavors f^{-1} també és bijectiva i $(f^{-1})^{-1} = f$.

Imatge i antiimatge d'un conjunt

Donats $f : A \rightarrow B$, $X \subseteq A$, $Y \subseteq B$ definim:

- El conjunt **imatge de** X :

$$f(X) = \{y \in B \mid \exists x \in X f(x) = y\} = \{f(x) \mid x \in X\}$$

$$y \in f(X) \Leftrightarrow \exists x \in X \ f(x) = y$$

- El conjunt **antiimatge** de Y :

$$f^{-1}(Y) = \{x \in A \mid f(x) \in Y\}$$

$$\begin{array}{l} \text{Si } x \in A : \\ x \in f^{-1}(Y) \Leftrightarrow f(x) \in Y \end{array}$$

Notem que:

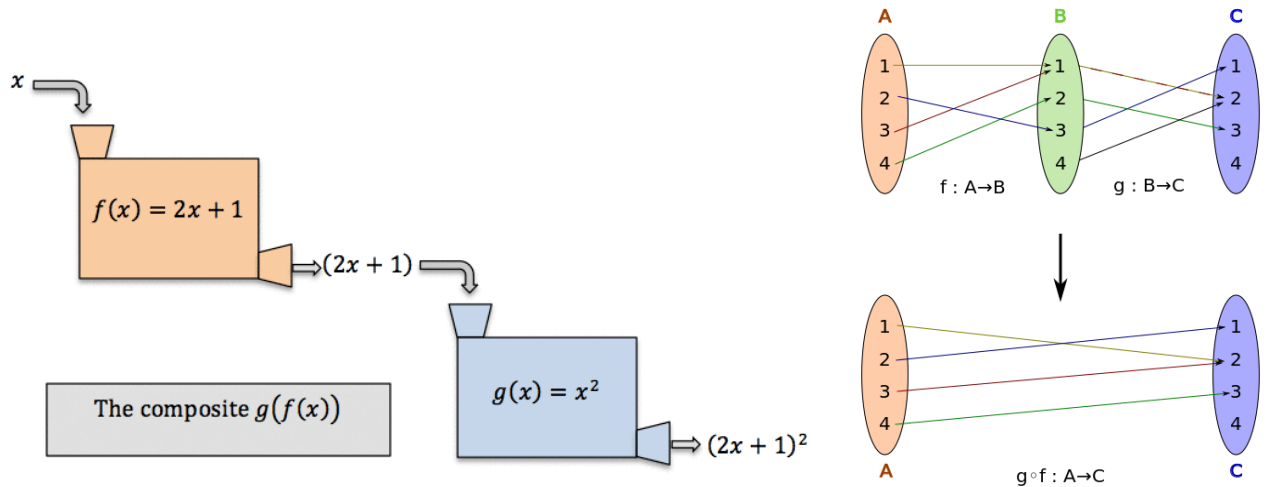
- $f(X)$ és un subconjunt de B (el conjunt de totes les imatges dels elements de X).
- $f^{-1}(Y)$ és un subconjunt de A (el conjunt de totes les antiimatges dels elements de Y).

Exercicis:

1. Sigui $f : \mathbb{Z} \rightarrow \mathbb{Z}$ definida per $f(x) = x^2$.
 - a. Calculeu la imatge dels conjunts següents: $\{-2, -1, 0, 1, 2, 3, 4\}$, \mathbb{N} , \mathbb{Z} , $\{x \in \mathbb{Z} \mid x \text{ és parell}\}$, $\{x \in \mathbb{Z} \mid x < 0\}$.
 - b. Calculeu l'antiimatge de $\{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$, $\{x \in \mathbb{Z} \mid x \text{ és senar}\}$, \mathbb{N} , \mathbb{Z} , $\{x \in \mathbb{Z} \mid x \leq 0\}$, $\{x \in \mathbb{Z} \mid x < 0\}$.
2. Sigui $f : A \rightarrow B$ i siguin $X, Y \subseteq B$. Demostreu que $f^{-1}(X \cup Y) = f^{-1}(X) \cup f^{-1}(Y)$.
3. $f^{-1}(B) = A$.
4. Sigui $f : A \rightarrow B$ i siguin $X, Y \subseteq A$. Demostreu que $f(X \cup Y) = f(X) \cup f(Y)$.
5. Sigui $f : A \rightarrow B$ i sigui $X \subseteq A$. Demostreu que $X \subseteq f^{-1}(f(X))$.
6. Sigui $f : A \rightarrow B$ injectiva i sigui $X \subseteq A$. Demostreu que $f^{-1}(f(X)) = X$.
7. Sigui $f : A \rightarrow B$. Demostreu que f és injectiva \Leftrightarrow per tot $X \subseteq A$ es compleix que $f^{-1}(f(X)) = X$.

8. (R) Sigui $f: \mathbb{Z} \rightarrow \mathbb{Z}$ definida per $f(x) = x$ si x és parell, $f(x) = x + 1$ si x és senar.
- Calculeu la imatge dels conjunts següents: $\{-2, -1, 0, 1, 2, 3, 4\}$, \mathbb{N} , \mathbb{Z} , $\{x \in \mathbb{Z} \mid x \text{ és parell}\}$, $\{x \in \mathbb{Z} \mid x < 0\}$.
 - Calculeu l'antiimatge de $\{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$, $\{x \in \mathbb{Z} \mid x \text{ és senar}\}$, \mathbb{N} , \mathbb{Z} , $\{x \in \mathbb{Z} \mid x \leq 0\}$, $\{x \in \mathbb{Z} \mid x < 0\}$.
9. Sigui $g: \mathbb{R} \rightarrow \mathbb{R}$ l'aplicació definida per $g(x) = E(x)$. Calculeu:
- $g^{-1}(\{0\})$
 - $g^{-1}(\{-1, 0, 1\})$
 - $g^{-1}(\{x \in \mathbb{R} \mid 0 < x < 1\})$
10. (R) Sigui $f: A \rightarrow B$ i siguin $X, Y \subseteq B$. Demostreu que $f^{-1}(X \cap Y) = f^{-1}(X) \cap f^{-1}(Y)$.
11. Sigui $f: A \rightarrow B$ i siguin $X, Y \subseteq A$. Demostreu que $f(X \cap Y) \subseteq f(X) \cap f(Y)$.
12. (R) Doneu exemples de $f: A \rightarrow B$ i $X, Y \subseteq A$ tals que $f(X \cap Y) \neq f(X) \cap f(Y)$.
13. (R) Sigui $f: A \rightarrow B$ injectiva i siguin $X, Y \subseteq A$. Demostreu que $f(X \cap Y) = f(X) \cap f(Y)$.
14. Sigui $f: A \rightarrow B$ satisfent que per a tot $X, Y \subseteq A$ es compleix que $f(X \cap Y) = f(X) \cap f(Y)$. Demostreu que f és injectiva.
15. Sigui $f: A \rightarrow B$. Demostreu que $f(A) = B \Leftrightarrow f$ és exhaustiva.
16. Sigui $f: A \rightarrow B$ i $Y \subseteq B$. Demostreu que $f(f^{-1}(Y)) \subseteq Y$.
17. (R) Demostreu que si $f: A \rightarrow B$ és exhaustiva i $Y \subseteq B$ llavors $f(f^{-1}(Y)) = Y$.
18. Sigui $f: A \rightarrow B$. Demostreu que f és exhaustiva \Leftrightarrow per tot $Y \subseteq B$ es compleix que $f(f^{-1}(Y)) = Y$.
19. Sigui $f: A \rightarrow B$. Demostreu que són equivalents:
- f és injectiva.
 - per tot $X, Y \subseteq A$ es compleix que $f(X \cap Y) = f(X) \cap f(Y)$.
 - per tot $X, Y \subseteq A$, si $X \cap Y = \emptyset$ llavors $f(X) \cap f(Y) = \emptyset$.

Composició d'aplicacions



Donades $f: A \rightarrow B$ i $g: B \rightarrow C$ definim la composició de f amb g , que anomenarem f **composada amb** g i que denotem per $g \circ f$, així:

$$g \circ f: A \rightarrow C, \quad (g \circ f)(x) = g(f(x))$$

Notem que:

- No sempre es pot compondre, només quan el codomini de la primera aplicació és el mateix que (o està contingut a) el domini de la segona.
- Diem f composada amb g , però ho denotem $g \circ f$.

Exercicis/Exemples. Calculeu les composades $g \circ f$ en els casos següents. Es pot calcular $f \circ g$?

1. $f: \mathbb{R} \rightarrow \mathbb{R}$ definida per $f(x) = e^x$, $g: \mathbb{R} \rightarrow \mathbb{R}$ definida per $g(x) = 2x$.
2. $f: \mathbb{Z} \rightarrow \mathbb{N}$ definida per $f(x) = x \bmod 5$, $g: \mathbb{N} \rightarrow \mathbb{R}$ definida $g(x) = \ln(x + 1)$.
3. $f: \mathbb{Z} \rightarrow \mathbb{Z}$ definida per $f(x) = x^3 - 11$, $g: \mathbb{Z} \rightarrow \mathbb{N}$ definida per $g(x) = 2x - 1$, si $x > 0$, $g(x) = -2x$, si $x \leq 0$.

Exemple: Els algoritmes de xifrat/desxifrat criptogràfic RSA consten de dues aplicacions $f: \mathbb{Z}_n \rightarrow \mathbb{Z}_n$ i $g: \mathbb{Z}_n \rightarrow \mathbb{Z}_n$ tals que $g \circ f = I_{\mathbb{Z}_n}$. f és l'algorisme de xifrat i g és l'algorisme de desxifrat. Aquí \mathbb{Z}_n és el conjunt quocient de \mathbb{Z} per la relació d'equivalència *tenir el mateix residu mòdul* n .

Propietats:

1. Associativa: si $f : A \rightarrow B$, $g : B \rightarrow C$, $h : C \rightarrow D$ llavors $h \circ (g \circ f) = (h \circ g) \circ f$.
2. Si $f : A \rightarrow B$, llavors $I_B \circ f = f \circ I_A = f$.

Propietats de la composició, injectivitat i exhaustivitat:

3. La composició d'aplicacions injectives és injectiva.
4. Si $g \circ f$ és injectiva llavors f és injectiva.
5. La composició d'aplicacions exhaustives és exhaustiva.
6. Si $g \circ f$ és exhaustiva llavors g és exhaustiva.
7. La composició d'aplicacions bijectives és bijectiva.
8. Si $g \circ f$ és bijectiva llavors f és injectiva i g és exhaustiva.

Propietats de la composició i la inversa:

9. Si $f : A \rightarrow B$ és bijectiva, llavors $f^{-1} \circ f = I_A$ i $f \circ f^{-1} = I_B$.
10. Si $f : A \rightarrow B$ $g : B \rightarrow A$ satisfan $g \circ f = I_A$ i $f \circ g = I_B$, llavors les dues són bijectives i cada una és la inversa de l'altre: $g = f^{-1}$ i $f = g^{-1}$.

Demo de 10: que f i g són bijectives surt de 4. i 6. Veiem ara que $f = g^{-1}$. Sigui $x \in A$ qualsevol, hem de veure que $g^{-1}(x) = f(x)$. És a dir, hem de veure que $g(f(x)) = x$. Això és cert perquè $g \circ f = I_A$. \square

Exemples:

1. Les aplicacions $\exp : \mathbb{R} \rightarrow (0, \infty)$ i $\ln : (0, \infty) \rightarrow \mathbb{R}$ són bijectives i cada una és la inversa de l'altre.
2. Les aplicacions $\sin : (-\pi/2, \pi/2] \rightarrow [-1, 1]$ i $\arcsin : [-1, 1] \rightarrow [-\pi/2, \pi/2]$ són bijectives i cada una és la inversa de l'altre.
3. Les aplicacions $[0, \infty) \rightarrow [0, \infty)$, $x \rightarrow x^2$ i $[0, \infty) \rightarrow [0, \infty)$, $x \rightarrow \sqrt{x}$ són bijectives i cada una és la inversa de l'altre.
4. Les aplicacions $f : \mathbb{Z} \rightarrow \mathbb{N}$ i $g : \mathbb{N} \rightarrow \mathbb{Z}$ definides per $f(x) = 2x - 1$, si $x > 0$, $f(x) = -2x$, si $x \leq 0$, $g(x) = -x/2$, si x és parell, $f(x) = \frac{x+1}{2}$, si x és senar, són bijectives i cada una és la inversa de l'altre.

Exercicis:

1. Sigui $f: \mathbb{N} \rightarrow \mathbb{N}$ definida per $f(x) = x + 1$, si x és parell, $f(x) = 2x$, altrament. Calculeu $f \circ f$ i proveu que f és injectiva.
2. Demostreu les propietats 1. 3. 6. anteriors.
3. Siguin $f: A \rightarrow B$, $g: B \rightarrow B$ amb g exhaustiva i satisfent $g \circ f = f$. Demostreu que $g = I_B$.
4. Si $f \circ h = g \circ h$ i h és exhaustiva llavors $f = g$.
5. (R) Sigui $f: \mathbb{N} \rightarrow \mathbb{N}$ definida per $f(x) = x$, si x és parell, $f(x) = x + 1$, altrament. Demostreu que $f \circ f = f$.
6. Demostreu les propietats 2., 4.(R), 5., 7., 8.(R), i 9. anteriors.
7. Si $f: A \rightarrow B$ és bijectiva i $g: B \rightarrow C$ és bijectiva llavors $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$
8. $f: A \rightarrow B$ és bijectiva \Leftrightarrow existeix $g: B \rightarrow A$ tal que $g \circ f = I_A$ i $f \circ g = I_B$. En aquest cas cada una és la inversa de l'altre: $g = f^{-1}$ i $f = g^{-1}$
9. Sigui $f: A \rightarrow B$ $g: B \rightarrow C$ tals que $g \circ f$ és bijectiva. Demostreu que són equivalents:
 - a. f és exhaustiva.
 - b. f és bijectiva.
 - c. g és injectiva.
 - d. g és bijectiva.
10. Si $f: A \rightarrow A$ satisfà $f \circ f = I_A$, què podem dir de f ?
11. Sigui $f: \mathbb{Z} \rightarrow \mathbb{Z}$ definida per $f(x) = x + 1$, si x és parell $f(x) = x - 1$, si x és senar. Calculeu $f \circ f$. Demostreu que f és bijectiva i calculeu la seva inversa.
12. (difícil) Sigui $f: A \rightarrow A$ satisfà $f \circ f = f$. Demostreu que són equivalents:
 - a. f és injectiva.
 - b. f és exhaustiva.
 - c. f és bijectiva.
 - d. $f = I_A$.
13. Si $g \circ f$ és injectiva i f és exhaustiva llavors g és injectiva.
14. Si $g \circ f$ és exhaustiva i g és injectiva llavors f és exhaustiva.
15. Si $h \circ f = h \circ g$ i h és injectiva llavors $f = g$.
16. Siguin $f: A \rightarrow A$, $g: A \rightarrow B$ amb g injectiva i satisfent $g \circ f = g$. Demostreu

que $f = I_A$.

17. (R) Sigui $f : A \rightarrow B$. Demostreu que són equivalents:

a. f és injectiva

b. Existeix $g : B \rightarrow A$ tal que $g \circ f = I_A$.

RECEPTES: Demostracions amb funcions



Demostració que $f : A \rightarrow B$ és injectiva

Siguin $x, x' \in A$ qualssevol: $f(x) = f(x') \Rightarrow \dots \Rightarrow x = x'$.

Demostració que $f : A \rightarrow B$ NO és injectiva:

Donar $x, x' \in A$ satisfent $x \neq x'$, $f(x) = f(x')$. (un contraexemple)

Demostració que $f : A \rightarrow B$ és exhaustiva

Sigui $y \in B$ qualsevol. Hem de donar algun $x \in A$ tal que $f(x) = y$.

Demostració que $f : A \rightarrow B$ NO és exhaustiva

Hem de donar $y \in B$ que no tingui cap antiimatge (per al qual "l'equació" $f(x) = y$ no té cap solució $x \in A$).

Demostració que $f : A \rightarrow B$ és bijectiva:

1a manera: f és injectiva i exhaustiva.

2a manera: (encara millor): Sigui $y \in B$ qualssevol. Hem de veure que hi ha un únic $x \in A$ tal que $f(x) = y$.

Demostració que les aplicacions $f, g : A \rightarrow B$ son iguals ($f = g$)

Donat $x \in A$, hem de veure $f(x) = g(x)$

5 i 6. ARITMÈTICA

Treballem en els enters \mathbb{Z} . Si no es diu el contrari, tots els nombres que apareixen són enters.

5. DIVISIBILITAT

Donats dos enters a, b definim:

$$a \mid b \Leftrightarrow \text{existeix un enter } q \text{ tal que } b = aq$$

$a \mid b$ es llegeix a **divideix** b . També diem que a **és un divisor de** b o que b **és un múltiple de** a .

Exemples:

1. $2 \mid 6$, $6 \mid 6$, $6 \mid -12$, $-4 \mid 12$.
2. $1 \mid 0$ $1 \mid 1$ $1 \mid 2$ $1 \mid 3$ $1 \mid a$ per a tot a .
3. $0 \mid 0$ $1 \mid 0$ $2 \mid 0$ $3 \mid 0$ $a \mid 0$ per a tot a .

Notem que:

1. No és exactament el mateix $a \mid b$ que $b/a \in \mathbb{Z}$.
2. Si $a \neq 0$ sí que és equivalent: $a \mid b \Leftrightarrow b/a \in \mathbb{Z}$.
3. $a \mid b \Leftrightarrow (a = b = 0) \vee (a \neq 0 \wedge b/a \in \mathbb{Z})$.

Propietats: Per a tot a, b, c, u, v enters:

1. $1 \mid a$.
2. $a \mid 0$.

3. Reflexiva: $a \mid a$.
 4. Transitiva: $a \mid b, b \mid c \Rightarrow a \mid c$.
 5. $a \mid b \Rightarrow ac \mid bc$.
 6. Simplificació: Si $c \neq 0$, $ac \mid bc \Rightarrow a \mid b$.
 7. $a \mid b \Rightarrow a \mid bc$.
 8. No depèn del signe:

$$a \mid b \Leftrightarrow a \mid -b \Leftrightarrow -a \mid b \Leftrightarrow -a \mid -b \Leftrightarrow |a| \mid |b|.$$
 9. Si $b \neq 0$, $a \mid b \Rightarrow |a| \leq |b|$.
 10. $a \mid b, b \mid a \Rightarrow |a| = |b|$.
 11. **Linealitat:** $a \mid b, a \mid c \Rightarrow a \mid ub + vc$.
-

Demostració de 9. $b = aq$ amb q enter. Com que $b \neq 0$, també $q \neq 0$ i per tant $1 \leq |q|$. Multiplicant per $|a|$ queda $|a| \leq |a||q| = |b|$. \square

Exemple: Volem trobar tots els enters divisors de 6 i 15 alhora. Si $a \mid 15$ i $a \mid 6$, per linealitat, $a \mid 15 - 2 \cdot 6 = 3$. Recíprocament, si $a \mid 3$ per la propietat 7, $a \mid 3 \cdot 5 = 15$ i $a \mid 3 \cdot 2 = 6$. Així, els divisors comuns de 6 i 15 són els enters a tals que $a \mid 3$, és a dir, $\pm 1, \pm 3$

Exercicis.

1. Demostreu totes les propietats 1., 3., 5., 6., 11. anteriors.
2. Demostreu totes les propietats 2., 4.(R), 7., 8., 10. anteriors.
3. Demostreu que si $a \mid a'$ i $b \mid b'$ llavors $ab \mid a'b'$.
4. Demostreu que $a \mid b$ implica $a^n \mid b^n$.
5. (R) Demostreu que si $a \mid (b - 1)$ i $a \mid (c - 1)$ llavors $a \mid (bc - 1)$.
6. A \mathbb{Z} definim la relació següent. Donats a, b enters:

$$aRb \Leftrightarrow a \mid b^n, b \mid a^n \text{ per a un cert } n \geq 1.$$
Demostreu que és una relació d'equivalència.
7. (difícil) Siguin a, b enters no nuls. Demostreu que són equivalents:
 - a. Per a tot $n \geq 0$, $e \mid ca^n + db^n$.
 - b. $e \mid c + d$, $e \mid ca + db$.
 - c. $e \mid c + d$, $e \mid c(a - b)$.

8. Demostreu que si $(a + b + c) \mid abc$ llavors $(a + b + c) \mid a^3 + b^3 + c^3$. (Pista: calculeu $(a + b + c)(a^2 + b^2 + c^2 - ab - ac - bc)$).

Nombres primers

Definició: Donat un nombre enter p :

p és **primer** $\Leftrightarrow p \geq 2$ i els únics divisors positius de p són 1 i p

Notem que:

1. Els primers són positius i el 1 no és primer!
2. Si $n \geq 2$, i no és primer (rep el nom de **compost**) llavors $n = rs$ per a uns certs enters r, s amb $2 \leq r < n$, $2 \leq s < n$.
3. Els nombres $1, -1$ no tenen divisors primers.

Exemples:

1. Els primers fins a 50 són: 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47.
2. El primer més gran que es coneix actualment (trobat el desembre de 2018) és: $2^{82,589,933} - 1$ i té 24,862,048 dígits decimals.

Resultats:

1. Tot nombre enter $n \geq 2$ és primer o és un producte de nombres primers.
 2. Tot nombre enter $n \geq 2$ té algun divisor primer p . Si a més n no és primer, podem triar algun divisor primer $p \leq \sqrt{n}$.
 3. Hi ha infinits nombres primers.
-

Test de primalitat: Per verificar que un nombre n és primer, n'hi ha prou amb verificar que no té cap divisor primer $\leq \sqrt{n}$ (per el resultat 2 anterior).

Exemple : És primer el nombre 102941?

Necessitem la llista de tots els primers fins $\sqrt{102941} = 320,8\dots$. La fem fins al 400. Aquesta llista la faren utilitzant un algorisme anomenat **Garbell d'Eratóstenes**. Consisteix en fer una llista dels 400 (en aquest cas) primers enters i agafar el primer enter de la llista no eliminat (inicialment agafarem el 2) i eliminar tots els seus múltiples excepte l'esmentat nombre (que podem marcar com a primer). Pel test de primalitat només caldrà fer-ho fins al 20. En aquest [link](#) es pot veure la seva execució. Ara, provant divisors resulta que.... [Resposta](#)

Demostracions.

1. Per inducció completa, hem de veure que tot $n \geq 2$ és de la forma $n = \prod_{i=1}^k p_i$ amb $k \geq 1$ i cada p_i primer. El cas base, quan $n = 2$ és obvi. Ara fem el pas inductiu. Si n és primer també és obvi. Si $n \geq 2$ no és primer llavors $n = rs$ amb $2 \leq r, s < n$. Per H.I., r i s són de la forma $r = \prod_{i=1}^u p_i$ $s = \prod_{i=1}^v p'_i$. Multiplicant tenim que

$n = rs = \prod_{i=1}^u p_i \cdot \prod_{i=1}^v p'_i$, que és un producte de primers tal com volíem demostrar. \square

2. Com que n és producte de primers, qualsevol d'aquests primers el divideix. Si n no és primer, serà de la forma $n = rs$ amb $2 \leq r, s < n$. Afirmem que $r \leq \sqrt{n}$ o $s \leq \sqrt{n}$. Si no (R.A.), tindríem que $r, s > \sqrt{n}$ i per tant $n = rs > \sqrt{n}\sqrt{n} = n$, contradicció. Ara, si $r \leq \sqrt{n}$ per exemple, prenem un divisor primer p de r . Llavors $p \leq r \leq \sqrt{n}$ i $p|n$ per la transitiva. \square

2a demostració de 2. Com que n és producte de primers, qualsevol d'aquests primers el divideix. Si n no és primer serà de la forma $n = p_1 p_2 p_3 \dots p_k$ amb tots els p_i primers i $k \geq 2$. Si cap dels $p_i \leq \sqrt{n}$, tindrem que cada $p_i > \sqrt{n}$ i multiplicant $n = p_1 p_2 p_3 \dots p_k > \sqrt{n} \sqrt{n} \dots \sqrt{n} = n^{k/2} \geq n$. Contradicció. \square

3. Per Reducció a l'absurd. Si no, siguin $p_1, p_2, p_3, \dots, p_n$ tots els primers. Com que $p_1 p_2 p_3 \dots p_n + 1 \geq 2$, aquest nombre ha de tenir algun divisor primer, posem p_i . De $p_i | p_1 p_2 p_3 \dots p_n + 1$ i $p_i | p_1 p_2 p_3 \dots p_n$, per linealitat tenim que $p_i | 1$. Contradicció. \square

Màxim comú divisor

El màxim comú divisor dels nombres enters a_1, a_2, \dots, a_n és el més gran de tots els divisors comuns de a_1, a_2, \dots, a_n si algun d'aquests nombres no és 0. Els divisors comuns de $0, 0, \dots, 0$ són tots els enters i per tant no hi ha màxim. En aquest cas es pren el 0 com a mcd per definició. El màxim comú divisor de a_1, a_2, \dots, a_n el denotarem per $mcd(a_1, a_2, \dots, a_n)$. Això ho podem expressar així:

Definició:

- $mcd(0, 0, \dots, 0) = 0$
- Si algun $a_i \neq 0$, $mcd(a_1, a_2, \dots, a_n)$ és l'únic enter d que verifica les dues propietats següents:
 - $d \mid a_i$ per a cada i ,
 - Si $d' \mid a_i$ per a cada i llavors $d' \leq d$.

Propietats: Per a qualssevol enters a, b, u tenim que:

1. Si $a \mid b$ llavors $mcd(a, b) = |a|$.
 2. $mcd(a, 0) = |a|$.
 3. Si p és primer i no divideix b , llavors $mcd(p, b) = 1$.
 4. El mcd no depèn del signe:
$$mcd(a, b) = mcd(a, -b) = mcd(-a, b) = mcd(-a, -b).$$
 5. (Teorema d'Euclides): $mcd(a, b) = mcd(a + ub, b)$.
-

Demostracions:

1. Distingim segons $a = 0$ o no. Si $a = 0$, de $0 \mid b$ deduïm que $b = 0$ i per tant es compleix. Ara fem el cas $a \neq 0$. Òbviament $|a|$ és un divisor comú de a, b . Si d és un divisor comú de a, b , de $d \mid a$ deduïm (ja que $a \neq 0$) $|d| \leq |a|$ i llavors $d \leq |d| \leq |a|$. \square

2. Surt de 1. \square
3. Els únics divisors positius de p són $1, p$. Com que p no divideix b , l'únic divisor comú positiu és 1 . \square
4. Ja que la divisibilitat no depèn del signe. \square
5. Posem $d_1 = \text{mcd}(a, b)$, $d_2 = \text{mcd}(a + ub, b)$. Hem de veure $d_1 = d_2$ i per tant n'hi ha prou amb veure que $d_1 \leq d_2$ i $d_2 \leq d_1$. Com que $d_1 | a$ i $d_1 | b$, per linealitat $d_1 | a + ub$. Així d_1 és un divisor comú de $a + ub, b$ i per tant \leq que el seu mcd. Així $d_1 \leq d_2$. Per a l'altra desigualtat, com que $d_2 | a + ub$, $d_2 | b$ i tenint en compte que $a = (a + ub) - ub$, per linealitat deduïm que $d_2 | a$. Com que d_2 divideix b resulta que $d_2 \leq d_1$. \square

Exercicis:

1. Calculeu el $\text{mcd}(a, b)$ en els casos següents:
 - a. $b = 1$.
 - b. $b = a + 1$.
 - c. $b | a$.
 - d. $b = \text{mcd}(a, c)$.
2. Demostreu que $\text{mcd}(2k + 5, 3k + 7) = 1$.
3. Demostreu que $\text{mcd}(n, n + 2) = 2$ si $2 | n$, 1 altrament.
4. Calculeu $\text{mcd}(a + b, a^2 - b^2)$.
5. (R) Calculeu el $\text{mcd}(a, b)$ en els casos següents:
 - a. $b = ca$.
 - b. $b = a^n$ ($n \geq 1$).
 - c. b és primer.
 - d. $b = 2a - 1$.
6. Demostreu que $\text{mcd}(4k + 14, 6k + 20) = 2$.
7. (R) Demostreu que $\text{mcd}(2k + 9, 3k + 15) = 3$ si $3 | k$, 1 altrament.
8. Calculeu $\text{mcd}(32k + 12, 12k + 4)$.
9. Demostreu que $\text{mcd}(\pm 1, b, c, \dots) = 1$.
10. Demostreu que si $b | a$ llavors $\text{mcd}(a, b, c, \dots) = \text{mcd}(b, c, \dots)$.
11. Demostreu que $\text{mcd}(0, b, c, \dots) = \text{mcd}(b, c, \dots)$.
12. Demostreu que $\text{mcd}(a) = |a|$.

13. Demostreu que $\text{mcd}(a, b, c, \dots) = \text{mcd}(a + ub, b, c, \dots)$.

Definició:

$$a \text{ i } b \text{ són primers entre si} \Leftrightarrow \text{mcd}(a, b) = 1$$

També es diu que a i b són **relativament primers**.

Observació: a i b són primers entre si \Leftrightarrow no tenen cap divisor primer comú.

Demostració: Notem $d = \text{mcd}(a, b)$. Si a, b tenen algun divisor primer p comú, llavors $d \geq p \geq 2$. Recíprocament, si $d \geq 2$, llavors d té algun divisor primer p . De $p|d$ i $d|a$ deduïm $p|a$. Anàlogament $p|d$ i per tant p és un divisor primer comú. \square

Divisió euclidiana

Teorema de la divisió euclidiana. Donats a, b enters amb $b \neq 0$, existeixen uns únics enters q, r tals que:

$$\begin{aligned} a &= bq + r \\ 0 &\leq r < |b| \end{aligned}$$

q rep el nom de **quocient** i r de **residu** de la divisió de a per b .

Demostració:

Comencem demostrant l'existència. Si x és un nombre real, notem per $E(x)$ la seva part entera inferior, que compleix: $E(x) \leq x < E(x) + 1$.

Prenem el quocient q i el residu r així:

| |
|--------------------------------|
| $q = \text{sig}(b)E(a/ b)$ |
| $r = a - bq = a - b E(a/ b)$ |

Com que

$$E(a/|b|) \leq a/|b| < E(a/|b|) + 1,$$

multiplicant per $|b|$, obtenim

$$|b|E(a/|b|) \leq a < |b|E(a/|b|) + |b|$$

i restant $|b|E(a/|b|)$:

$$0 \leq r < |b|.$$

Per veure la unicitat prenem dues possibles solucions q, r i q', r' i veiem que són la mateixa, és a dir: $q = q'$ i $r = r'$. Suposem, per comoditat que $r \leq r'$. Comencem veient, per RA, que $r = r'$. En efecte, de $a = bq + r = bq' + r'$, deduïm que $b(q - q') = r' - r$ i per tant $b \mid r' - r$. Si $r \neq r'$ llavors $|b| \leq |r' - r| = r' - r$. Això implica que $r' = |b| + r \geq |b|$, contradicció. Això demostra que $r' = r$. Però llavors $bq + r = bq' + r'$ implica que $bq = bq'$; i com que $b \neq 0$, resulta que $q' = q$. \square

Notem que:

1. a i b poden ser negatius!
2. Si $b \neq 0$ llavors:

$$b \mid a \Leftrightarrow \text{el residu de la divisió de } a \text{ per } b \text{ és zero.}$$

Exemples:

1. Si dividim 16 entre 5 obtenim quocient 3 i residu 1.
2. Si dividim 16 entre -5 obtenim quocient -3 i residu 1.
3. Si dividim -16 entre 5 obtenim quocient -4 i residu 4.
4. Si dividim -16 entre -5 obtenim quocient 4 i residu 4.

Algorisme d'Euclides

Volem calcular $\text{mcd}(a, b)$. Com que el mcd no depèn del signe podem començar suposant que $a \geq b > 0$.

Observació: Pel teorema d'Euclides tenim que

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

on aquí r denota el residu de la divisió euclidiana de a per b .

Aplicant successivament la fórmula

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

per tal de calcular el mcd, com que anem obtenint una successió de nombres ≥ 0 decreixent a, b, r, \dots , en algun moment arribem a 0. El mcd serà l'últim element no nul de la successió (l'últim residu no nul), ja que $\text{mcd}(a, 0) = |a|$.

Exemple: $\text{mcd}(14001, 279) = \text{mcd}(279, 51) = \text{mcd}(51, 24) = \text{mcd}(24, 3) = 3$.

Això ho organitzem en una taula de la manera següent:

| | | | | | | |
|-----|-------|-----|----|----|---|---|
| q | | 50 | 5 | 2 | | |
| r | 14001 | 279 | 51 | 24 | 3 | 0 |

Una mica més sistemàtic. Definim la seqüència de residus $r_0, r_1, r_2, \dots, r_n$ així:

$r_0 = a, \quad r_1 = b, \quad r_i = q_{i+1}r_{i+1} + r_{i+2}, \quad 0 \leq r_{i+2} < r_{i+1}, \quad i = 0 \dots n-2$
on r_n és l'últim residu no nul. Llavors $\text{mcd}(a, b) = r_n$.

| | | | | | | | | |
|-----|-----------|-----------|-------|-------|-----|-----------|-------|---|
| i | 0 | 1 | 2 | 3 | ... | $n-1$ | n | |
| q | | q_1 | q_2 | q_3 | ... | q_{n-1} | | |
| r | $r_0 = a$ | $r_1 = b$ | r_2 | r_3 | ... | r_{n-1} | r_n | 0 |

Identitats de Bézout

| | | | | | | |
|-----|-------|-----|----|----|---|---|
| q | | 50 | 5 | 2 | | |
| r | 14001 | 279 | 51 | 24 | 3 | 0 |

Les divisions de l'exemple anterior les podem posar així:

$$3 = 51 + 24(-2)$$

$$24 = 279 + 51(-5) \Rightarrow 3 = 51 + (279 + 51(-5))(-2) = 279(-2) + 51(11)$$

$$51 = 14001 + 279(-50) \Rightarrow 3 = 279(-2) + (14001 + 279(-50))(11) = \\ = 14001(11) + 279(-552)$$

Hem arribat a l'expressió següent:

$$3 = 14001(11) + 279(-552)$$

Hem aconseguit posar el mcd d'aquests dos nombres com a combinació lineal d'ells. Això ho podem fer sempre. Argumentant correctament el procediment de l'exemple, obtenim una demostració del següent:

Identitats de Bézout. Donats a, b enters qualssevol, existeixen x, y enters tals que

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

Aquesta expressió rep el nom de **Identitat de Bézout**.

Una manera de calcular identitats de Bézout més sistemàtica: Definim dues successions recurrents així:

$$x_0 = 1, \quad x_1 = 0, \quad x_i = x_{i-2} - q_{i-1}x_{i-1} \quad \text{per } i = 2 \dots n$$

$$y_0 = 0, \quad y_1 = 1, \quad y_i = y_{i-2} - q_{i-1}y_{i-1} \quad \text{per } i = 2 \dots n$$

Si ho posem a la taula anterior ampliant-la:

| | | | | | | | | |
|-----|---|---|-------|-------|-----|-----------|-------|--|
| i | 0 | 1 | 2 | 3 | ... | $n-1$ | n | |
| x | 1 | 0 | x_2 | x_3 | ... | x_{n-1} | x_n | |

| | | | | | | | | |
|-----|-----------|-----------|-------|-------|-----|-----------|-------|---|
| y | 0 | 1 | y_2 | y_3 | ... | y_{n-1} | y_n | |
| q | | q_1 | q_2 | q_3 | ... | q_{n-1} | | |
| r | $r_0 = a$ | $r_1 = b$ | r_2 | r_3 | ... | r_{n-1} | r_n | 0 |

Aplicat a l'exemple anterior:

| | | | | | | |
|-----|-------|-----|-----|-----|------|---|
| i | 0 | 1 | 2 | 3 | 4 | |
| x | 1 | 0 | 1 | -5 | 11 | |
| y | 0 | 1 | -50 | 251 | -552 | |
| q | | 50 | 5 | 2 | | |
| r | 14001 | 279 | 51 | 24 | 3 | 0 |

$$3 = 14001(11) + 279(-552)$$

Exercicis.

1. Calculeu el mcd i una identitat de Bézout per a les parelles següents: $(-512, 88)$ i $(1234, -221)$.
2. (R algun) Executeu l'algorisme d'Euclides estès per a les parelles de la taula següent:

| | | | | |
|-------|------|-------------|------|------|
| a | b | $mcd(a, b)$ | x | y |
| 5548 | 1727 | 1 | 80 | -257 |
| 3614 | 7752 | 2 | 1435 | -669 |
| 1084 | 4904 | 4 | -95 | 21 |
| 7084 | 3563 | 7 | -85 | 169 |
| -7084 | 3563 | 7 | | |

| | | | | |
|--------|--------|---|--|--|
| 7084 | - 3563 | 7 | | |
| - 7084 | - 3563 | 7 | | |

3. (R) Demostreu que l'aplicació $f : \mathbb{Z} \times \mathbb{Z} \rightarrow \mathbb{Z}$ definida per $f(x, y) = 5548x + 1727y$ és exhaustiva.

Notem que: Les identitats de Bézout no són mai úniques. Sempre podem sumar i restar múltiples de $\frac{ab}{\text{mcd}(a,b)}$:

$$ax + by = a\left(x + t\frac{b}{\text{mcd}(a,b)}\right) + b\left(y - t\frac{a}{\text{mcd}(a,b)}\right).$$

Conseqüències de Bézout

Lema de Gauss. Si $a \mid bc$ i $\text{mcd}(a, b) = 1$ llavors $a \mid c$

Lema Euclides Si p és primer i $p \mid bc$ llavors $p \mid b$ o $p \mid c$

Per inducció és fàcil veure que el lema d'Euclides val amb més factors:

$$\text{Si } p \mid b_1 \cdots b_n \text{ i } p \text{ és primer llavors } p \mid b_1 \text{ o } p \mid b_2 \text{ o } \cdots \text{ o } p \mid b_n$$

Demostracions.

Lema de Gauss. Com que $\text{mcd}(a, b) = 1$, per Bézout sabem que existeixen x, y enters satisfent:

$$1 = ax + by.$$

Multiplicant per c obtenim:

$$c = acx + bcy.$$

Per linealitat, de $a \mid a$ i $a \mid bc$ deduïm que a divideix $acx + bcy = c$. \square

Lema d'Euclides. Hem de veure que si p no divideix b llavors p divideix c . En

efecte: al ser primer, si p no divideix b resulta que $\text{mcd}(p, b) = 1$. Aplicant el lema de Gauss tenim que $p|c$. \square

Descomposició en factors primers.

Unicitat de la descomposició en factors primers.

Tot nombre enter $n \geq 2$ té una descomposició única de la forma següent:

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

on cada p_i és primer i cada $e_i > 0$.

Això vol dir que el k , els p_1, \dots, p_k i els e_1, \dots, e_k són únics (llevat de permutació).

Exemple: $84 = 2^2 3^1 7^1$, $90 = 2^1 3^2 5^1$

Demostració. L'existència ja l'hem fet, la unicitat la fem per inducció completa sobre n .

Suposem que n admet dues factoritzacions $n = p_1^{e_1} p_2^{e_2} \dots p_k^{e_k} = q_1^{f_1} q_2^{f_2} \dots q_r^{f_r}$, on podem suposar que els primers estan ordenats en forma creixent ($p_1 < p_2 < \dots$ i $q_1 < q_2 < \dots$). Com que $e_1 > 0$ resulta que $p_1 | q_1^{f_1} q_2^{f_2} \dots q_r^{f_r}$ i, pel Lema d'Euclides, $p_1 | q_i$ per algun i . Al ser q_i primer tenim que $p_1 = q_i$. Ara, dividint per $p_1 = q_i$ obtenim dues factoritzacions de n/p_1 :

$$n/p_1 = p_1^{e_1-1} p_2^{e_2} \dots p_k^{e_k} = q_1^{f_1} q_2^{f_2} \dots q_i^{f_i-1} \dots q_r^{f_r}.$$

Per Hipòtesi d'inducció aquestes factoritzacions són la mateixa: $k = r$, $i = 1$, $p_1 = q_1, \dots, p_r = q_r$, $e_1 - 1 = f_1 - 1$, $e_2 = f_2, \dots, e_r = f_r$. Per tant, també les dues factoritzacions de n són la mateixa: $k = r$, $i = 1$, $p_1 = q_1, \dots, p_r = q_r$, $e_1 = f_1, e_2 = f_2, \dots, e_r = f_r$. \square

La factorització següent és una variant que inclou els nombres negatius i l'1. També ens permet usar més primers dels estrictament necessaris, encara que això espatlla la unicitat.

Descomposició en factors primers amb signe i exponents possiblement nuls.

Tot nombre enter $n \neq 0$ té una descomposició de la forma següent:

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

on $\varepsilon = \pm 1$, cada p_i és primer i cada $e_i \geq 0$.

Notem que: En aquesta última factorització tant ε com els exponents són únics. Però ni el k ni els p_1, \dots, p_k són únics, ja que sempre podem afegir un nou primer amb l'exponent 0. Per exemple

$$-28 = (-1)2^2 7^1 = (-1)2^2 3^0 5^0 7^1 11^0$$

Gràcies a això sempre podem suposar que apareixen els mateixos primers en la factorització de diversos nombres:

$$84 = 2^2 3^1 5^0 7^1 11^0, \quad -90 = (-1)2^1 3^2 5^1 7^0 11^0, \quad -264 = (-1)2^3 3^1 5^0 7^0 11^1$$

Càlcul del mcd a partir de la factorització i conseqüències

Divisibilitat i càlcul del mcd a partir de la factorització

Si expressem $a = \varepsilon_1 p_1^{e_1} p_2^{e_2} \dots p_k^{e_k}$ i $b = \varepsilon_2 p_1^{f_1} p_2^{f_2} \dots p_k^{f_k}$ amb $e_i, f_i \geq 0$, $\varepsilon_i = \pm 1$ i cada p_i primer llavors tenim:

1. $a \mid b \Leftrightarrow e_i \leq f_i$ per a cada i .
 2. $\text{mcd}(a, b) = p_1^{\min(e_1, f_1)} p_2^{\min(e_2, f_2)} \dots p_k^{\min(e_k, f_k)}$.
 3. La fórmula del mcd també val amb 3 o més nombres agafant el mínim dels diversos exponents.
 4. els divisors positius de a son tots els nombres de la forma $p_1^{g_1} p_2^{g_2} \dots p_k^{g_k}$ amb $0 \leq g_i \leq e_i$.
 5. El nombre de divisors positius de a és $(e_1 + 1)(e_2 + 1) \dots (e_k + 1)$.
-

Demostracions:

1. \Rightarrow) Si $a|b$ resulta $b = ad$, per a un cert $d = \varepsilon_3 p_1^{g_1} p_2^{g_2} \dots p_k^{g_k}$. Llavors $\varepsilon_2 p_1^{f_1} p_2^{f_2} \dots p_k^{f_k} = \varepsilon_1 \varepsilon_3 p_1^{e_1+g_1} p_2^{e_2+g_2} \dots p_k^{e_k+g_k}$. Per la unicitat dels exponents de la descomposició en factor primers tenim que $f_i = e_i + g_i$. Com que $g_i \geq 0$ obtenim $f_i \geq e_i$. \Leftarrow) Recíprocament, si $f_i \geq e_i$ resulta que $b = ad$, amb $d = \varepsilon_1 \varepsilon_2 p_1^{f_1-e_1} p_2^{f_2-e_2} \dots p_k^{f_k-e_k}$. \square
2. Surt de 1. \square
3. Surt de 1. \square
4. Surt de 1. \square
5. Surt de 4. \square

Exemple: $\text{mcd}(84, -90, -264) = 2^1 3^1 5^0 7^0 11^0$.

Exercicis:

1. Trobeu tots els divisors de 600.
2. (R) Si p, q, r són tres nombres primers diferents 2 a 2, calculeu tots els divisors positius de pq^2r^3 .
3. Tenim 1000 rajoles quadrades. De quantes maneres es poden disposar de manera que formin un rectangle?
4. (R) Definim el conjunt $M_a = \{x \in \mathbb{Z} \mid a \mid x\}$.
 - a. Si p, q són primers diferents, demostreu que $M_p \cap M_q = M_{pq}$.
 - b. Val $M_p \cap M_q = M_{pq}$ per a p, q enters qualssevol? Justifiqueu-ho.
5. Aquest exercici és continuació d'un exercici anterior, en el qual es demanava demostrar que la relació en els enters: $aRb \Leftrightarrow a \mid b^n, b \mid a^n$ per a un cert $n \geq 1$, és d'equivalència.
 - a. Demostreu que si $a \neq 0, a \mid b^n$ per a un cert $n \geq 1$ sii tots els factors primers de a ho són de b .
 - b. Descriviu la classe d'un enter a .
 - c. Demostreu que hi ha una bijecció entre $\mathbb{Z} - \{0\}/R$ i el conjunt dels subconjunts finits de nombres primers

Conseqüències de la factorització:

1. **Tot divisor comú de a, b divideix $\text{mcd}(a, b)$.** De fet:

$$d \mid a \text{ i } d \mid b \Leftrightarrow d \mid \text{mcd}(a, b).$$

2. Associativitat mcd:

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

3. $\text{mcd}(ca, cb) = |c| \text{mcd}(a, b).$

4. $\text{mcd}(a/\text{mcd}(a, b), b/\text{mcd}(a, b)) = 1$ **(si $\text{mcd}(a, b)$ no és nul).**

5. Totes les propietats anteriors valen també amb 3 o més enters.
-

Demostracions:

1. Posem $a = \varepsilon_1 p_1^{e_1} p_2^{e_2} \dots p_k^{e_k}$, $b = \varepsilon_2 p_1^{f_1} p_2^{f_2} \dots p_k^{f_k}$, $d = \varepsilon_3 p_1^{g_1} p_2^{g_2} \dots p_k^{g_k}$.

Llavors: $d \mid a$ i $d \mid b \Leftrightarrow$ per a cada i $g_i \leq e_i$ i $g_i \leq f_i \Leftrightarrow$ per a cada i $g_i \leq \min(e_i, f_i) \Leftrightarrow d \mid \text{mcd}(a, b)$. \square

2. Surt de l'associativitat del mínim:

$$\min(\min(e, f), g) = \min(e, \min(f, g)) = \min(e, f, g). \quad \square$$

3. Surt de $\min(g + e, g + f) = g + \min(e, f)$. \square

4. Si posem $c = \text{mcd}(a, b)$ i apliquem 3: $c = \text{mcd}(a, b) = \text{mcd}(c a/c, c b/c) = c \text{mcd}(a/c, b/c)$. Com que $c \neq 0$, simplificant obtenim $1 = \text{mcd}(a/c, b/c)$. \square

5. Es fan igual que en el cas de dos. \square

Nota:

1. El càlcul eficient de $\text{mcd}(a_1, a_2, \dots, a_n)$, es pot fer aplicant l'associativitat del mcd i en cada pas, calcular el mcd de dos nombres mitjançant l'algorisme d'Euclides.

Exercicis:

6. Demostreu que si $a + c = 1$ llavors $\text{mcd}(a, c) = 1$.
7. Si $\text{mcd}(a, b) = p$, on p és primer, raoneu i justifiqueu quins són els possibles valors de:
- a. $\text{mcd}(a^2, b)$.

- b. $\text{mcd}(a^3, b)$.
- c. $\text{mcd}(a^2, b^3)$.
8. Demostreu que $\text{mcd}(a, b) = 1$ i $\text{mcd}(a, c) = 1 \Leftrightarrow \text{mcd}(a, bc) = 1$.
9. (R) Demostreu que si $a^2 = 5b^2$ llavors tant a com b són múltiples de 5.
10. Si $\text{mcd}(a, b) = p^3$, on p és primer, calculeu $\text{mcd}(a^2, b^2)$.
11. Demostreu que si $ab + c = 1$ llavors $\text{mcd}(a, c) = \text{mcd}(b, c) = 1$.
12. (R) Suposem que p és primer. Demostreu que són equivalents:
- $p \mid a$.
 - $\text{mcd}(p, a) = p$.
 - $p \mid a^2$.
 - $p^2 \mid a^3$.
13. Demostreu que si $ab + cd = 1$ llavors $\text{mcd}(a, c) = \text{mcd}(b, c) = \text{mcd}(a, d) = \text{mcd}(b, d) = 1$.
14. Demostreu que si $n \geq 0$, $m > 0$ llavors a^n i $a^m - 1$ són primers entre si.
15. Demostreu que l'aplicació $f: \{0, 1, 2, \dots, 13, 14\} \times \{0, 1, 2, \dots, 12, 13\} \rightarrow \mathbb{Z}$ definida per $f(x, y) = 14x + 15y$ és injectiva.
16. (R) Demostreu que a, b són primers entre si \Leftrightarrow existeixen x, y tals que $1 = ax + by$.
17. Demostreu que si $c \neq 0$ i $a^n \mid b^n c$ per a tot $n \geq 0$ llavors $a \mid b$. Val el recíproc?
18. Suposem que p és primer. Demostreu que són equivalents:
- $p^2 \mid a$.
 - $p^4 \mid a^2$.
 - $p^3 \mid a^2$.
 - $\text{mcd}(p^2, a) = p^2$.
 - $p^2 \mid \text{mcd}(p^2, a)$.
 - $p^2 \mid \text{mcd}(p^3, a)$.
 - $p^2 \mid \text{mcd}(p^{10}, a)$.
19. (difícil) Demostreu que hi ha identitats de Bézout per a tres o més enters: Donats a_1, \dots, a_n existeixen x_1, \dots, x_n tals que $\text{mcd}(a_1, \dots, a_n) = a_1x_1 + a_2x_2 + \dots + a_nx_n$.
20. Demostreu que si $(a + b + c) \mid a^3 + b^3 + c^3$ i $a + b + c$ no és múltiple de 3 llavors $(a + b + c) \mid abc$. Pista: calculeu $(a + b + c)(a^2 + b^2 + c^2 - ab - ac - bc)$

21. (R) (difícil) Donats $n, r \geq 0, m > 0$, demostreu que si a i b són primers entre si llavors a^n i $ua^m + b^r$ són primers entre si. Aquí u és un enter qualsevol.
22. Sigui a enter positiu. Demostreu que si \sqrt{a} és racional llavors a és un quadrat (és igual al quadrat d'un altre nombre enter)
23. (difícil) Donats a_1, \dots, a_n primers entre si dos a dos, demostreu que existeixen x_1, \dots, x_n tals que $1 = \sum_{i=1}^n x_i \prod_{j \neq i} a_j$. Val el recíproc?
24. (difícil) Donats a_1, \dots, a_n enters no tots nuls, considerem el conjunt $A = \{a_1x_1 + a_2x_2 + \dots + a_nx_n : \text{cada } x_i \text{ és enter i } a_1x_1 + a_2x_2 + \dots + a_nx_n > 0\}$. Demostreu que A és no buit i que el mínim de A és $\text{mcd}(a_1, \dots, a_n)$.
25. Demostreu que si a és relativament primer amb cada un dels b_1, \dots, b_n llavors a és relativament primer amb el seu producte $b_1 \cdots b_n$. Val el recíproc?
26. Suposem que p és primer, $n \geq 2$ i r, s són enters tals que $n - 1 < r/s \leq n$. Demostreu que són equivalents:
- $p^n \mid a$.
 - $p^r \mid a^s$.
 - $\text{mcd}(p^n, a) = p^n$.
 - $p^n \mid \text{mcd}(p^n, a)$.
 - $p^n \mid \text{mcd}(p^{n+m}, a)$ ($m \geq 0$).
27. (En aquest exercici introduïm un algorisme molt eficient per calcular el mcd de diversos enters positius) Demostreu que el següent algorisme calcula $\text{mcd}(a_1, a_2, \dots, a_n)$. Comencem reemplaçant cada enter pel seu valor absolut. Apliquem successivament les operacions següents: mentre hi hagi zeros, suprimir-los; mentre hi hagi més d'un enter reemplaçar el més gran dels enters pel residu de la seva divisió entre el menor d'ells. Quan només quedi un sol enter, acabar i respondre aquest enter. (pista: useu exercicis 11., 12. i 13. del tema *Màxim comú divisor*).

Equacions diofàntiques

Les equacions diofàntiques són equacions a coeficients enters de les quals busquem les solucions enteres.

Exemples:

1. $3x + 6y = 5$.
2. $6x - 10y = 4$.

La primera equació no té solució ja que la part esquerra és múltiple de 3 i la dreta no.

De la segona trobem una solució particular usant una identitat de Bézout: multiplicant $6 \cdot 2 - 10 \cdot 1 = 2$ per 2 obtenim que $6 \cdot 4 - 10 \cdot 2 = 4$ i per tant $x_0 = 4$, $y_0 = 2$ és una solució de l'equació.

Ara deduïm quines són totes les solucions usant el *Lema de Gauss*. Si x, y és una solució qualsevol llavors $6x - 10y = 6 \cdot 4 - 10 \cdot 2$. Per tant, $6(x - 4) = 10(y - 2)$ i simplificant per 2:

$$3(x - 4) = 5(y - 2). \quad (*)$$

Com que 3 i 5 són primers entre si i $3 \mid 5(y - 2)$, pel lema de Gauss, $3 \mid (y - 2)$ i per tant $3k = y - 2$. O sigui que

$$y = 2 + 3k.$$

Substituint a (*) queda $3(x - 4) = 15k$. Per tant:

$$x = 4 + 5k.$$

Acabem de veure que totes les solucions x, y tenen la forma:

$$x = 4 + 5k, \quad y = 2 + 3k, \quad \text{per un cert enter } k.$$

Finalment cal verificar que tots els x, y de la forma anterior són solució. Això es fa substituint a l'equació:

$$6(4 + 5k) - 10(2 + 3k) = 4.$$

Si reproduïm els arguments anteriors en un cas qualsevol (amb lletres enlloc de nombres) obtenim el resultat següent.

Resolució d'equacions diofàntiques:

- L'equació diofàntica $ax + by = c$ té solució $\Leftrightarrow \text{mcd}(a, b) \mid c$
- Les solucions particulars s'obtenen (com a l'exemple) multiplicant una identitat de Bézout de (a, b) per $\frac{c}{\text{mcd}(a, b)}$ en ambdós costats.
- Si x_0, y_0 és una solució particular de l'equació anterior, totes les solucions són de la forma

$$x = x_0 + \frac{b}{\text{mcd}(a, b)}t, \quad y = y_0 - \frac{a}{\text{mcd}(a, b)}t,$$

per a un cert enter t .

Exercicis.

1. Digueu si les equacions diofàntiques següents tenen solució. Si en tenen, trobeu totes les solucions.
 - $20x + 8y = 6,$ $20x + 8y = 12,$ $20x - 8y = 12,$
 $-20x + 8y = 12,$ $-20x - 8y = 12.$
2. Trobeu la solució (x, y) de les equacions anteriors que tingui la x positiva mínima.
3. Li demaneu a un amic que multipliqui el dia que va néixer per 12 i el número del mes per 31 i que us digui el resultat de la suma d'aquestes quantitats. El resultat és 500. Esbrineu la data del seu aniversari.
4. Digueu si les equacions diofàntiques següents tenen solució. Si en tenen, trobeu totes les solucions.
 - (R) $512x + 88y = 20,$ $512x + 88y = 40,$ $-512x - 88y = 40$
 $-512x + 88y = 40,$ $512x - 88y = 40.$
 - $1234x + 221y = 20,$ $-1234x + 221y = 40,$ $-1234x - 221y = 40.$
5. Trobeu la solució (x, y) de les equacions anteriors que tingui la y màxima que sigui menor o igual que -3 .
6. (R) Els graus Fahrenheit F i Celsius C estan relacionats per la fórmula: $F = \frac{9}{5}C + 32$. Trobeu totes les solucions enteres d'aquesta equació. Heu de tenir en compte que el zero absolut correspon a $-273.15^\circ C$.
7. Descomponeu de totes les maneres possibles la fracció $230/247$ en suma de

dues fraccions positives de denominadors 19 i 13 .

8. S'ha de començar a jugar un partit de futbol i només disposem de dos rellotges de sorra que mesuren 6 i 11 minuts. És possible mesurar exactament els 45 minuts que ha de durar cada part? Trobeu totes les possibles maneres.

Mínim comú múltiple

El mínim comú múltiple dels nombres enters a_1, a_2, \dots, a_n és el més petit de tots els múltiples comuns **positius** (> 0) de a_1, a_2, \dots, a_n , si n'hi ha. Això passa quan tots els a_i són $\neq 0$. Si algun dels $a_i = 0$ l'únic múltiple comú és 0. El mínim comú múltiple dels nombres enters a_1, a_2, \dots, a_n el denotarem per $mcm(a_1, a_2, \dots, a_n)$.

Definició:

- Si algun $a_i = 0$, $mcm(a_1, a_2, \dots, a_n) = 0$.
- Si tots el $a_i \neq 0$, el $mcm(a_1, a_2, \dots, a_n)$ és l'únic enter m que verifica les dues propietats següents:
 - $m > 0$ i $a_i \mid m$ per a cada i .
 - Si $m' > 0$ i $a_i \mid m'$ per a cada i llavors $m \leq m'$.

Propietats:

1. Si $a \mid b$ llavors $mcm(a, b) = |b|$.
2. El mcm no depèn del signe:
$$mcm(a, b) = mcm(a, -b) = mcm(-a, b) = mcm(-a, -b).$$

Càlcul del mcm a partir de la factorització i conseqüències

Càlcul del mcm a partir de la factorització

Si expressem $a = \varepsilon_1 p_1^{e_1} p_2^{e_2} \dots p_k^{e_k}$ i $b = \varepsilon_2 p_1^{f_1} p_2^{f_2} \dots p_k^{f_k}$ amb $e_i, f_i \geq 0$, $\varepsilon_i = \pm 1$ i cada p_i primer llavors tenim:

$$\text{mcm}(a, b) = p_1^{\max(e_1, f_1)} p_2^{\max(e_2, f_2)} \dots p_k^{\max(e_k, f_k)}.$$

Aquesta fórmula també valen amb 3 o més nombres agafant el màxim dels diversos exponents.

Exemple: $84 = 2^2 3^1 5^0 7^1 11^0$, $-90 = (-1) 2^1 3^2 5^1 7^0 11^0$, $-264 = (-1) 2^3 3^1 5^0 7^0 11^1$
 $\text{mcm}(84, -90, -264) = 2^3 3^2 5^1 7^1 11^1$.

Conseqüències:

1. **Càlcul eficient del mcm:** $\text{mcd}(a, b) \text{ mcm}(a, b) = |ab|$
 2. **Tot múltiple comú de a, b és múltiple de $\text{mcm}(a, b)$.** De fet:
$$a \mid m \text{ i } b \mid m \Leftrightarrow \text{mcm}(a, b) \mid m.$$
 3. **Associativitat mcm:** $\text{mcm}(\text{mcm}(a, b), c) = \text{mcm}(a, \text{mcm}(b, c)) = \text{mcm}(a, b, c)$.
 4. Totes les propietats anteriors valen també amb 3 o més enters excepte la propietat 1.
-

Demostracions:

1. Surt de $\min(e, f) + \max(e, f) = e + f$. \square
2. Posem $a = \varepsilon_1 p_1^{e_1} p_2^{e_2} \dots p_k^{e_k}$, $b = \varepsilon_2 p_1^{f_1} p_2^{f_2} \dots p_k^{f_k}$ i $m = \varepsilon_3 p_1^{g_1} p_2^{g_2} \dots p_k^{g_k}$.
Llavors: $a \mid m$ i $b \mid m \Leftrightarrow e_i \leq g_i$ i $f_i \leq g_i \Leftrightarrow \max(e_i, f_i) \leq g_i \Leftrightarrow \text{mcm}(a, b) \mid m$. \square
3. Surt de l'associativitat del màxim:
$$\max(\max(e, f), g) = \max(e, \max(f, g)) = \max(e, f, g). \quad \square$$

4. Es fan igual que en el cas de dos. Un contraexemple a 1. amb tres nombres:

$$\text{mcd}(2, 2, 1) = 1, \quad \text{mcm}(2, 2, 1) = 2$$

Notes:

1. Tal com ja hem dit, la **propietat 1 no val** amb 3 o més enters en general:

$$\text{mcd}(a_1, a_2, \dots, a_n) \text{ mcm}(a_1, a_2, \dots, a_n) \neq |a_1, a_2, \dots, a_n|$$

Per exemple $\text{mcd}(2, 2, 3) \text{ mcm}(2, 2, 3) = 1 \cdot 6 = 6 \neq 2 \cdot 2 \cdot 3$

2. El càlcul eficient de $\text{mcm}(a_1, a_2, \dots, a_n)$ es fa usant l'associativitat del mcm i en cada pas, calcular el mcm de dos mitjançant la fórmula $\text{mcd}(a, b) \text{ mcm}(a, b) = |ab|$ i l'algoritme d'Euclides. El càlcul de $\text{mcm}(a_1, a_2, \dots, a_n)$, no passa pel de $\text{mcd}(a_1, a_2, \dots, a_n)$!!!

Exercicis:

1. (R) Calculeu totes les parelles possibles de nombres enters (incloent negatius!) que tenen màxim comú divisor 5 i mínim comú múltiple 70.
2. (R) Calculeu els enters positius a, b tals que $a + b = 57$ i $\text{mcm}(a, b) = 680$.
3. Demostreu que si a_1, \dots, a_n són relativament primers entre si dos a dos, llavors $\text{mcm}(a_1, \dots, a_n) = |a_1 \cdots a_n|$.
4. Supposem que p és primer. Demostreu que són equivalents:
 - a. $p \mid a$.
 - b. $\text{mcm}(p, a) = |a|$.
 - c. $p \mid a^2$.
 - d. $p^2 \mid a^3$.
5. (R algunes) Supposem que p és primer. Demostreu que són equivalents:
 - a. $p^2 \mid a$.
 - b. $p^4 \mid a^2$.
 - c. $p^3 \mid a^2$.
 - d. $\text{mcm}(p^2, a) = |a|$.
 - e. $p^2 \mid \text{mcm}(p, a)$.
6. Supposem que p és primer, $n \geq 2$ i r, s són enters tals que $n - 1 < r/s \leq n$. Demostreu que són equivalents:
 - a. $p^n \mid a$.
 - b. $p^r \mid a^s$.

- c. $\text{mcm}(p^n, a) = |a|$.
 - d. $p^n \mid \text{mcm}(p, a)$.
 - e. $p^n \mid \text{mcm}(p^{n-1}, a)$.
7. (difícil) Siguin a_1, a_2, \dots, a_n enters amb $n \geq 3$. Demostreu que $\text{mcd}(a_1, a_2, \dots, a_n) \text{mcm}(a_1, a_2, \dots, a_n) = |a_1, a_2, \dots, a_n| \Leftrightarrow a_1, a_2, \dots, a_n$ són primers entre si dos a dos.

6. CONGRUÈNCIES

La relació binària següent a \mathbb{Z} rep el nom de **congruència**. N'hi ha una per a cada $m \geq 1$. El nombre m rep el nom de **mòdul** de la congruència.

Definició

Donat $m \geq 1$

$$\begin{aligned} a \equiv b \pmod{m} &\Leftrightarrow m \mid b - a \\ &\Leftrightarrow b = a + km \text{ per un cert } k \\ &\Leftrightarrow a \text{ i } b \text{ tenen el mateix residu al dividir per } m \end{aligned}$$

És fàcil veure l'equivalència d'aquestes tres propietats. Ho deixem com a exercici pel lector.

Quan $a \equiv b \pmod{m}$ es diu que a **és congruent amb** b **mòdul** m .

Exemples:

1. $7 \equiv 15 \pmod{4}$, $7 \not\equiv 12 \pmod{4}$
2. $a \equiv b \pmod{1}$
3. $a \equiv 0 \pmod{2} \Leftrightarrow a$ és parell
4. $a \equiv 1 \pmod{2} \Leftrightarrow a$ és senar
5. $a \equiv b \pmod{2} \Leftrightarrow a$ i b tenen la mateixa paritat

Propietat 1. La congruència mòdul m és una relació d'equivalència.

Demostració: Evident, fent servir la tercera caracterització de la congruència.

Classes modulars

La classe de a per la relació de congruència mòdul m es denota per \bar{a} i el conjunt quocient es denota per \mathbb{Z}_m

Exemple: $m = 5$. Com que hi ha 5 residus possibles al dividir per 5, hi haurà cinc classes mòdul 5:

$$\bar{0} = \{x \in \mathbb{Z} : x \equiv 0 \pmod{5}\} = \{5k : k \in \mathbb{Z}\}$$

$$\bar{1} = \{x \in \mathbb{Z} : x \equiv 1 \pmod{5}\} = \{1 + 5k : k \in \mathbb{Z}\}$$

$$\bar{2} = \{x \in \mathbb{Z} : x \equiv 2 \pmod{5}\} = \{2 + 5k : k \in \mathbb{Z}\}$$

$$\bar{3} = \{x \in \mathbb{Z} : x \equiv 3 \pmod{5}\} = \{3 + 5k : k \in \mathbb{Z}\}$$

$$\bar{4} = \{x \in \mathbb{Z} : x \equiv 4 \pmod{5}\} = \{4 + 5k : k \in \mathbb{Z}\}$$

El conjunt quocient és doncs:

$$\mathbb{Z}_5 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}\}$$

Fets:

1. A \mathbb{Z}_m : $\bar{a} = \{x \in \mathbb{Z} : x \equiv a \pmod{m}\} = \{a + km : k \in \mathbb{Z}\}$.
2. $\bar{a} = \bar{b}$ a $\mathbb{Z}_m \Leftrightarrow a \equiv b \pmod{m}$.
3. $\mathbb{Z}_m = \{\bar{0}, \bar{1}, \bar{2}, \dots, \overline{m-1}\}$.

Propietat 2

$$\left| \begin{array}{l} a \equiv a' \pmod{m} \\ b \equiv b' \pmod{m} \end{array} \right| \Rightarrow \left| \begin{array}{l} a + b \equiv a' + b' \pmod{m} \\ ab \equiv a'b' \pmod{m} \end{array} \right|$$

Demostració: Per linealitat:

$$\left| \begin{array}{l} m \mid a' - a \\ m \mid b' - b \end{array} \right. \Rightarrow \left| \begin{array}{l} m \mid (a' - a) + (b' - b) = (a' + b') - (a + b) \\ m \mid b'(a' - a) + a(b' - b) = a'b' - ab \end{array} \right. \quad \square$$

Exemple 1: Quin és el residu de dividir $58 \cdot 79$ mòdul 11? Hi ha dues maneres de fer-ho. La primera consisteix en efectuar la multiplicació $58 \cdot 79 = 4582$ i a continuació calcular el residu de 4582. L'altra consisteix en usar que $58 \cdot 79 \equiv 3 \cdot 2 = 6$. Aquí hem usat que $58 \equiv 3 \pmod{11}$ i $79 \equiv 2 \pmod{11}$ implica que $58 \cdot 79 \equiv 3 \cdot 2 \pmod{11}$. Aquesta segona manera consisteix en “reduir abans de operar”. Això sempre simplifica les operacions.

Exemple 2: Calculem les dues últimes xifres de $2^{1000000}$ a mà. Treballem mòdul 100. Comencem calculant els residus de les primeres potències de 2:

$$\begin{aligned} 2^2 &= 4, & 2^3 &= 8, & 2^4 &= 16, & 2^5 &= 32, & 2^6 &= 64, & 2^7 &= 128 \equiv 28 \pmod{100}, \\ 2^8 &= 2 \cdot 2^7 \equiv 2 \cdot 28 \equiv 56 \pmod{100}, & 2^9 &= 2 \cdot 2^8 \equiv 2 \cdot 56 \equiv 112 \equiv 12 \pmod{100}, \\ 2^{10} &= 2 \cdot 2^9 \equiv 2 \cdot 12 \equiv 24 \pmod{100}, & 2^{11} &= 2 \cdot 2^{10} \equiv 2 \cdot 24 \equiv 48 \pmod{100}, \\ 2^{12} &= 2 \cdot 2^{11} \equiv 2 \cdot 48 \equiv 96 \equiv -4 \pmod{100}, \\ 2^{13} &= 2 \cdot 2^{12} \equiv 2 \cdot (-4) \equiv -8 \pmod{100}, \end{aligned}$$

...

...

$$2^{20} \equiv -24 \pmod{100}, \quad 2^{21} \equiv -48 \pmod{100}, \quad 2^{22} \equiv 4 \pmod{100}.$$

Aquí ens aturem i observem que hem trobat un primer valor que es repeteix:

$$2^{22} \equiv 2^2 \pmod{100}$$

Per tant, també tenim que:

$$2^2 \equiv 2^2 2^{20} \equiv 2^2 2^{20} 2^{20} \equiv 2^2 2^{20} 2^{20} 2^{20} \equiv \dots \equiv 2^{2+20k} \pmod{100}$$

Així, dividint 999998 entre 20 tenim $999998 = 20 \cdot 49999 + 18$, per tant $1000000 = 18 + 2 + 20 \cdot 49999$

$$2^{1000000} \equiv 2^{2+20 \cdot 49999} 2^{18} \equiv 2^2 2^{18} \equiv 2^{20} \equiv -24 \equiv 76$$

Per tant les dues últimes xifres de $2^{1000000}$ són 76.

Altres propietats de les congruències:

1. Si $a \equiv b \pmod{m}$ i $d \mid m$ llavors $a \equiv b \pmod{d}$.

2. Si $k > 0$ llavors:

$$ka \equiv kb \pmod{km} \Leftrightarrow a \equiv b \pmod{m}.$$

3. Si $\text{mcd}(k, m) = 1$ llavors:

$$a \equiv b \pmod{m} \Leftrightarrow ka \equiv kb \pmod{m}.$$

Demostració:

1. $d \mid m$, $m \mid b - a \Rightarrow d \mid b - a$. \square

2. $km \mid kb - ka = k(b - a) \Leftrightarrow m \mid b - a$. \square

3. \Rightarrow Si $m \mid b - a$ òbviament $m \mid k(b - a)$. Recíprocament, Si $m \mid k(b - a)$ i $\text{mcd}(k, m) = 1$, pel Lema de Gauss, $m \mid b - a$. \square

Exemple: Resolem les congruències:

1. $5x \equiv 10 \pmod{9}$

2. $3x \equiv 6 \pmod{9}$

3. $15x \equiv 30 \pmod{9}$

1: Com que $\text{mcd}(5, 9) = 1$, la primera és equivalent a $x \equiv 2 \pmod{9}$ i per tant, les solucions són de la forma $x = 2 + 9k$.

2: La segona, simplificant-la per 3 queda $x \equiv 2 \pmod{3}$ i per tant, les solucions són de la forma $x = 2 + 3k$.

3: La tercera, simplificant-la per 3 queda $5x \equiv 10 \pmod{3}$ Ara, com que 5 i 3 són primers entre si, podem simplificar a l'esquerra per 5: $x \equiv 2 \pmod{3}$. Per tant, les solucions són de la forma $x = 2 + 3k$.

Exercicis: Demostreu que:

1. Demostreu que per a $n \geq 0$, $8^{n+1} - 8 - 56n$ és múltiple de 392 usant congruències i inducció.

2. (R) Sigui p un nombre primer.

a. Si $a^2 \equiv b^2 \pmod{p}$ llavors $a \equiv b \pmod{p}$ o $a \equiv -b \pmod{p}$.

- b. Deduïu que les solucions de la congruència $x^2 \equiv 1 \pmod{p}$ són els enters tals que $x \equiv 1 \pmod{p}$ o $x \equiv -1 \pmod{p}$.
- c. És cert b. si p no és primer?
3. (R) $ka \equiv kb \pmod{m} \Leftrightarrow a \equiv b \pmod{m/\text{mcd}(k,m)}$.
4. (difícil) $a \equiv b \pmod{m} \Leftrightarrow a/\text{mcd}(a,b) \equiv b/\text{mcd}(a,b) \pmod{m/\text{mcd}(a,b,m)}$.
5. $ac \equiv bc \pmod{m} \Rightarrow a^n c \equiv b^n c \pmod{m} \quad (n \geq 1)$.
6. Són equivalents:
- $a^n c \equiv b^n d \pmod{m}$ per a tot $n \geq 0$.
 - $c \equiv d \pmod{m}$, $ac \equiv bd \pmod{m}$.
7. Demostreu que $2 \cdot 5^{2n+1} + 8 \cdot 7^n$ és múltiple de 18 per a tot $n \geq 0$. (Pista: useu inducció i congruències)

Aritmètica modular

Podem definir una aritmètica (operacions de suma i producte) al conjunt \mathbb{Z}_m de la manera següent:

- $\overline{a} + \overline{b} = \overline{a+b}$
- $\overline{a} \cdot \overline{b} = \overline{a \cdot b}$

Això està ben definit gràcies a la propietat 2 de les congruències. Aquesta propietat diu que el resultat “no depèn del representant”. Expressada en termes de classes:

$$\left| \begin{array}{l} \overline{a} = \overline{a'} \\ \overline{b} = \overline{b'} \end{array} \right. \Rightarrow \left| \begin{array}{l} \overline{a+b} = \overline{a'+b'} \\ \overline{ab} = \overline{a'b'} \end{array} \right. \quad \square$$

Amb aquestes operacions és fàcil veure que \mathbb{Z}_m **és un anell**. El neutre de la suma és $\overline{0}$, el neutre del producte és $\overline{1}$ i l'invers per la suma de \overline{a} és $\overline{-a}$.

La propietat 2 que acabem de mencionar diu que el resultat ens permet “triar el representant” que més ens convingui. Sempre és millor “reduir” abans d’operar. Per exemple, a \mathbb{Z}_{3000} :

$$\overline{2990} \overline{2995} = \overline{(-10)} \overline{(-5)} = \overline{50}$$

Exemple: \mathbb{Z}_5 . Podem calcular les taules de la suma i producte.

Taula de la suma a \mathbb{Z}_5 :

| + | $\bar{0}$ | $\bar{1}$ | $\bar{2}$ | $\bar{3}$ | $\bar{4}$ |
|-----------|-----------|-----------|-----------|-----------|-----------|
| $\bar{0}$ | $\bar{0}$ | $\bar{1}$ | $\bar{2}$ | $\bar{3}$ | $\bar{4}$ |
| $\bar{1}$ | $\bar{1}$ | $\bar{2}$ | $\bar{3}$ | $\bar{4}$ | $\bar{0}$ |
| $\bar{2}$ | $\bar{2}$ | $\bar{3}$ | $\bar{4}$ | $\bar{0}$ | $\bar{1}$ |
| $\bar{3}$ | $\bar{3}$ | $\bar{4}$ | $\bar{0}$ | $\bar{1}$ | $\bar{2}$ |
| $\bar{4}$ | $\bar{4}$ | $\bar{0}$ | $\bar{1}$ | $\bar{2}$ | $\bar{3}$ |

Taula del producte a \mathbb{Z}_5 :

| * | $\bar{0}$ | $\bar{1}$ | $\bar{2}$ | $\bar{3}$ | $\bar{4}$ |
|-----------|-----------|-----------|-----------|-----------|-----------|
| $\bar{0}$ | $\bar{0}$ | $\bar{0}$ | $\bar{0}$ | $\bar{0}$ | $\bar{0}$ |
| $\bar{1}$ | $\bar{0}$ | $\bar{1}$ | $\bar{2}$ | $\bar{3}$ | $\bar{4}$ |
| $\bar{2}$ | $\bar{0}$ | $\bar{2}$ | $\bar{4}$ | $\bar{1}$ | $\bar{3}$ |
| $\bar{3}$ | $\bar{0}$ | $\bar{3}$ | $\bar{1}$ | $\bar{4}$ | $\bar{2}$ |
| $\bar{4}$ | $\bar{0}$ | $\bar{4}$ | $\bar{3}$ | $\bar{2}$ | $\bar{1}$ |

Observem que tant $\bar{1}, \bar{2}, \bar{3}$ com $\bar{4}$ tenen invers respecte al producte. És a dir, tot element no nul té invers. Quan això passa diem que l'anell és un **cos**. Així \mathbb{Z}_5 és cos.

Ara calculem la taula del producte a \mathbb{Z}_6 :

| * | $\bar{0}$ | $\bar{1}$ | $\bar{2}$ | $\bar{3}$ | $\bar{4}$ | $\bar{5}$ |
|-----------|-----------|-----------|-----------|-----------|-----------|-----------|
| $\bar{0}$ | $\bar{0}$ | $\bar{0}$ | $\bar{0}$ | $\bar{0}$ | $\bar{0}$ | $\bar{0}$ |
| $\bar{1}$ | $\bar{0}$ | $\bar{1}$ | $\bar{2}$ | $\bar{3}$ | $\bar{4}$ | $\bar{5}$ |
| $\bar{2}$ | $\bar{0}$ | $\bar{2}$ | $\bar{4}$ | $\bar{0}$ | $\bar{2}$ | $\bar{4}$ |
| $\bar{3}$ | $\bar{0}$ | $\bar{3}$ | $\bar{0}$ | $\bar{3}$ | $\bar{0}$ | $\bar{3}$ |
| $\bar{4}$ | $\bar{0}$ | $\bar{4}$ | $\bar{2}$ | $\bar{0}$ | $\bar{4}$ | $\bar{2}$ |
| $\bar{5}$ | $\bar{0}$ | $\bar{5}$ | $\bar{4}$ | $\bar{3}$ | $\bar{2}$ | $\bar{1}$ |

Ara observem que les úniques classes que tenen invers són $\bar{1}$ i $\bar{5}$.

Exercicis:

1. Demostreu que per a tot $m, n \geq 0$ $5^n + 2 \cdot 3^m + 1$ és múltiple de 4.
2. Demostreu que per a tot $n \geq 0$ $19^n + 3^{2n+2}$ acaba en 0 usant classes modulars.
3. Demostreu que n és congruent mòdul 3 amb la suma dels seus dígit.
4. Demostreu els criteris de divisibilitat següents:
 - a. n és múltiple de 4 sii el nombre format pels dos últims dígit de n és múltiple de 4.
 - b. (R) n és múltiple de 5 sii acaba en 0 o en 5.
 - c. (R) n és múltiple de 9 sii la suma dels dígit de n és múltiple de 9.
 - d. n és múltiple de 11 sii la suma dels dígit de n que ocupen un lloc parell menys la suma dels que ocupen un lloc senar és múltiple de 11.
5. Quines xifres s'han de posar en el lloc de a, b perquè el nombre $4a8b$ sigui divisible per 2, 3, 5, 11?
6. Quina xifra s'ha de posar en el lloc de z perquè el nombre $9z86$ en dividir-lo per 11 tingui residu 5?
7. (R) Proveu que no hi ha cap n tal que $5n + 3$ és un quadrat.
8. Sigui $A_n = 2^n + 2^{2n} + 2^{3n}$.

- a. Demostreu que per a tot $n \geq 0$ el nombre $A_{n+3} - A_n$ és múltiple de 7.
- b. Calculeu el residu de dividir A_{2019} per 7.
9. (R) Demostreu que per a tot $n \geq 0$ el nombre $3^{2n+2} - 8n - 9$ és múltiple de 64 usant classes modulars i inducció.

Invers modular

Buscar un invers de \bar{a} a \mathbb{Z}_m és buscar un enter x tal que $\bar{a} \cdot \bar{x} = \bar{1}$. O de manera equivalent, un enter x tal que $ax \equiv 1 \pmod{m}$. Això últim vol dir que $1 = ax + my$ per a un cert y enter. Tot plegat ens diu que \bar{a} té invers a $\mathbb{Z}_m \Leftrightarrow$ l'equació diofàntica $ax + my = 1$ té solució. Però això passa si i només si $\text{mcd}(a, m) = 1$. Observem que l'invers es troba a partir d'una identitat de Bézout per a m, a . Acabem de demostrar que:

Existència d'inversos modulars. \bar{a} té invers a $\mathbb{Z}_m \Leftrightarrow \text{mcd}(a, m) = 1$

Exemple: Tenen inversos mòdul 9 el 5 i el 6? Calculeu-los si en tenen.

Ara trobem l'invers modular de $\overline{227}$ a \mathbb{Z}_{2292} . Observeu que el valor de la x no ens importa i no l'hem calculat.

| | | | | | |
|-----|------|-----|-----|-----|------|
| x | 1 | 0 | | | x |
| y | 0 | 1 | -10 | 101 | -313 |
| q | | 10 | 10 | 3 | |
| r | 2292 | 227 | 22 | 7 | 1 |

$1 = 2292x + 227(-313) \Rightarrow \bar{1} = \overline{2292x} + \overline{227} \cdot \overline{(-313)} \Rightarrow \bar{1} = \overline{0x} + \overline{227} \cdot \overline{-313}$
 $\Rightarrow \bar{1} = \overline{227} \cdot \overline{-313}$ i per tant l'invers de $\overline{227}$ a \mathbb{Z}_{2292} és $\overline{-313} = \overline{1979}$. Això es pot escriure així:

$$\overline{227}^{-1} = \overline{1979}$$

Exercici: Calculeu, si en tenen, els inversos modulars de $\overline{50}$, $\overline{39}$ a \mathbb{Z}_{1210} .

Exemple: L'equació $\overline{5}\overline{x} = \overline{5}$ a \mathbb{Z}_9 . Com que $\overline{5}$ té invers, és equivalent a $\overline{x} = \overline{1}$ (\Rightarrow multiplicant per l'invers de $\overline{5}$, \Leftarrow multiplicant per $\overline{5}$). Això vol dir que $\overline{x} = \overline{1}$ és l'única solució. No cal calcular l'invers. Però és molt important saber que existeix. Per exemple, a \mathbb{Z}_9 , l'equació $\overline{6}\overline{x} = \overline{6}$ té com a solució $\overline{x} = \overline{1}$ (aquí només val \Leftarrow multiplicant per $\overline{6}$). Com que no sabem si val \Rightarrow ($\overline{6}$ no té invers), no podem assegurar que $\overline{x} = \overline{1}$ és la única solució. De fet, és fàcil veure que n'hi ha dues més: $\overline{x} = \overline{4}$ i $\overline{x} = \overline{7}$. En aquest cas, el millor és simplificar la congruència: $6x \equiv 6 \pmod{9} \Leftrightarrow 2x \equiv 2 \pmod{3}$ i aquesta té una única solució mòdul 3: $x \equiv 1 \pmod{3}$. Això es transforma en tres classes mòdul 9: $x \equiv 1 \pmod{9}$, $x \equiv 4 \pmod{9}$, $x \equiv 7 \pmod{9}$.

Exercicis:

1. Resoleu l'equació $\overline{5}\overline{x} - \overline{3} = \overline{29}$ a \mathbb{Z}_{13} .
2. Resoleu el sistema $\overline{4}\overline{x} + \overline{7}\overline{y} = \overline{22}$, $\overline{3}\overline{x} + \overline{3}\overline{y} = \overline{y} + \overline{16}$ a \mathbb{Z}_{11} (Sol: $\overline{x} = \overline{1}$, $\overline{y} = \overline{1}$).
3. Resoleu les congruències següents:
 - a. $3x \equiv 5 \pmod{8}$.
 - b. $2x \equiv 4 \pmod{8}$.
 - c. $6x \equiv 4 \pmod{8}$.
 - d. $2x \equiv 5 \pmod{8}$.
4. Demostreu que el producte de dues classes invertibles de \mathbb{Z}_n és invertible. Qui és l'invers del producte?
5. (R) Resoleu el sistema $\overline{3}\overline{x} + \overline{5}\overline{y} = \overline{4}$, $\overline{4}\overline{x} - \overline{2}\overline{y} = \overline{2}$ a \mathbb{Z}_{11} (Sol: $\overline{x} = \overline{10}$, $\overline{y} = \overline{8}$).
6. Demostreu que $ax \equiv b \pmod{m}$ té solució $\Leftrightarrow \text{mcd}(a, m) \mid b$.
7. Demostreu que l'invers modular, si existeix, és únic (Pista: heu de demostrar que si \overline{b} i \overline{c} són inversos modulars de \overline{a} llavors $\overline{b} = \overline{c}$).
8. (R) Resoleu les congruències següents:
 - a. $22x \equiv 9 \pmod{15}$.
 - b. $21x \equiv 9 \pmod{15}$.

- c. $21x \equiv 10 \pmod{9}$.
9. Sigui $n \geq 1$. Demostreu si a, n són primers entre si, l'aplicació $f: \mathbb{Z}_n \rightarrow \mathbb{Z}_n$ donada per $f(\bar{x}) = \bar{a} \cdot \bar{x}$ és bijectiva i doneu la inversa.
10. Considerem l'aplicació $f: \mathbb{Z}_{29} \rightarrow \mathbb{Z}_{29}$ donada per $f(\bar{x}) = \overline{22} \cdot \bar{x} + \overline{7}$.
- Demostreu que l'aplicació f és bijectiva i doneu la inversa.
 - Considerem l'alfabet de 29 símbols indicat a continuació.

| | | | | | |
|-------|-------|--------|--------|--------|------------|
| A 0 | F 5 | K 10 | P 15 | U 20 | Z 25 |
| B 1 | G 6 | L 11 | Q 16 | V 21 | 26 (espai) |
| C 2 | H 7 | M 12 | R 17 | W 22 | . 27 |
| D 3 | I 8 | N 13 | S 18 | X 23 | , 28 |
| E 4 | J 9 | O 14 | T 19 | Y 24 | |

Codifiquem les paraules usant l'aplicació anterior. Per exemple, 'AVUI', que correspon a 0 21 20 8, es codifica en 7 5 12 9, que correspon a 'HF MJ'. El resultat d'una codificació ha estat el missatge 'KZRT, AI'. Quin és el missatge original?

Un cos és un anell on, llevat del 0 (el neutre de la suma), tot element és invertible respecte la multiplicació.

Quan \mathbb{Z}_m és cos. \mathbb{Z}_m és un cos $\Leftrightarrow m$ és primer

Demostració: \mathbb{Z}_m és un cos \Leftrightarrow tot $\bar{k} \neq \bar{0}$ té invers a \mathbb{Z}_m \Leftrightarrow per a tot enter $1 \leq k \leq m-1$, k i m són primers entre si $\Leftrightarrow m$ és primer. \square

Sistemes de congruències.

Si tenim un sistema de dues congruències:

$$x \equiv a_1 \pmod{m_1}, \quad x \equiv a_2 \pmod{m_2},$$

i x és una solució llavors $x = a_1 + m_1y = a_2 + m_2z$ per a uns certs y, z enters. Per tant

$$m_1y - m_2z = a_2 - a_1 \quad (*)$$

i l'equació diofàntica $(*)$ en les variables y, z té solució. Recíprocament, si y, z és una solució de l'equació diofàntica $(*)$, fent $x = a_1 + m_1y = a_2 + m_2z$ tenim que x és una solució del sistema xinès. Això ens dona un mètode per resoldre un sistema xinès de dues congruències. A més veiem que el sistema té solució si i només si $\text{mcd}(m_1, m_2) \mid a_2 - a_1$.

En cas de tenir-ne, totes les solucions són de la forma $x = a_1 + m_1y = a_1 + m_1(y_0 + \frac{m_2}{\text{mcd}(m_1, m_2)}t) = a_1 + m_1y_0 + \frac{m_1m_2}{\text{mcd}(m_1, m_2)}t = x_0 + \text{mcm}(m_1, m_2)t$ on x_0 és una solució particular del sistema. És a dir, si el sistema té solució, totes les solucions són de la forma

$$x \equiv x_0 \pmod{\text{mcm}(m_1, m_2)}$$

Exemples: Dieu si tenen solució i resoleu els sistemes següents:

1. $x \equiv 2 \pmod{4}, \quad x \equiv 1 \pmod{6}$
2. $x \equiv 4 \pmod{5}, \quad x \equiv 5 \pmod{6}$

Aquest procediment permet convertir un sistema de dues congruències en una sola (si és que té solució) on ara el nou mòdul és el mcm dels dos mòduls anteriors. Iterant aquest mètode podem saber si un sistema xinès té solució i trobar-les totes, en cas de tenir-ne.

Exercicis: Resoleu els sistemes següents:

3. $x \equiv 2 \pmod{4}, \quad x \equiv 1 \pmod{6} \quad x \equiv 1 \pmod{7}$.
4. $x \equiv 4 \pmod{5}, \quad x \equiv 5 \pmod{6} \quad x \equiv 7 \pmod{8}$.
5. (R) $x \equiv 1 \pmod{4}, \quad x \equiv 5 \pmod{6} \quad x \equiv 7 \pmod{10}$.
6. $x \equiv 1 \pmod{3}, \quad x \equiv 3 \pmod{4} \quad x \equiv 4 \pmod{7} \quad x \equiv 7 \pmod{11}$.
7. Una banda de 13 pirates s'apodera d'una caixa de monedes d'or. Si es

repartissin equitativament, en sobrarien 8. Moren 2 pirates. Si es repartissin ara en sobrarien 3. Desapareixen 3 pirates més. En la repartició, ara en sobrarien 5. Quin és el mínim nombre de monedes d'or?

Última propietat de les congruències.

$$a \equiv b \pmod{m_1}, \dots, a \equiv b \pmod{m_n} \Leftrightarrow a \equiv b \pmod{\text{mcm}(m_1, \dots, m_n)}.$$

Demostració: $m_1 | b - a, \dots, m_n | b - a \Leftrightarrow \text{mcm}(m_1, \dots, m_n) | b - a. \quad \square$

Un exemple.

Considerem el sistema:

$$x \equiv 0 \pmod{3}, \quad x \equiv 1 \pmod{4}, \quad x \equiv 2 \pmod{5}.$$

Com que

$$-3 \equiv 0 \pmod{3}, \quad -3 \equiv 1 \pmod{4}, \quad -3 \equiv 2 \pmod{5},$$

resulta que, per la transitivitat, el sistema el podem reescriure:

$$x \equiv -3 \pmod{3}, \quad x \equiv -3 \pmod{4}, \quad x \equiv -3 \pmod{5}.$$

Ara, aplicant la propietat anterior resulta que això és equivalent a:

$$x \equiv -3 \pmod{\text{mcm}(3, 4, 5)}$$

Per tant, totes les solucions del sistema són:

$$x = -3 + 60t, \quad t \text{ enter}$$

El Teorema petit de Fermat.

El teorema (petit) de Fermat. Si p és primer i no divideix a llavors:
$$a^{p-1} \equiv 1 \pmod{p}.$$

Això es pot expressar en classes a \mathbb{Z}_p de la manera següent:

Si p és primer i \bar{a} és invertible llavors: $\overline{a^{p-1}} = \bar{1}$

Demostració. Primer observem que totes les classes invertibles de \mathbb{Z}_p són $\bar{1}, \bar{2}, \dots, \overline{(p-1)}$. Veiem ara que $\bar{1} \cdot \bar{a}, \bar{2} \cdot \bar{a}, \dots, \overline{(p-1)} \cdot \bar{a}$ són les mateixes classes, potser en un ordre diferent. Primer cada classe $\bar{i} \cdot \bar{a}$ és invertible perquè tant \bar{i} com \bar{a} ho són. Com que n'hi ha el mateix nombre, només cal veure que aquestes últimes són totes diferents 2 a 2: Si $\bar{i} \cdot \bar{a} = \bar{j} \cdot \bar{a}$, multiplicant per l'invers de \bar{a} , obtenim $\bar{i} = \bar{j}$. Per tant, quan les multipliquem totes ha donar el mateix resultat:

$$\bar{1} \cdot \bar{2} \cdot \dots \cdot \overline{(p-1)} = \bar{1} \cdot \bar{a} \cdot \bar{2} \cdot \bar{a} \cdot \dots \cdot \overline{(p-1)} \cdot \bar{a} = \bar{1} \cdot \bar{2} \cdot \dots \cdot \overline{(p-1)} \cdot \overline{a^{p-1}}.$$

Com que $\bar{1}, \bar{2}, \dots, \overline{(p-1)}$ són tots invertibles, podem simplificar-ho i obtenir:

$$\bar{1} = \overline{a^{p-1}}. \quad \square$$

Això ens permet reduir l'exponent a un de menor que el mòdul quan aquest és primer.

Exemple. Calcularem el residu de 43^{3221} mòdul 13. Primer de tot reduïm la base:

$$43^{3221} \equiv 4^{3221} \pmod{13}$$

Com que 4 és primer amb 13, per Fermat tenim que $4^{12} \equiv 1 \pmod{13}$. Com que cada 12 factors "desapareixen", el que farem és agrupar els factors en paquets de 12: fem la divisió euclidiana de 3221 per 12 i obtenim que $3221 = 268 \cdot 12 + 5$. Per tant:

$$4^{3221} \equiv 4^{268 \cdot 12 + 5} \equiv \left(4^{12}\right)^{268} 4^5 \equiv 1^{268} 4^5 \equiv 4^5 \equiv 10 \pmod{13}.$$

Observació.

Si $n, m \geq 1$

$$n \equiv m \pmod{p-1} \Rightarrow a^n \equiv a^m \pmod{p}$$

Demostració: Hi ha dos casos segons p i a son relativament primers o no. En el primer cas, si $n \equiv m \pmod{p-1}$, llavors $n = m + k(p-1)$ i per tant:

$$a^n \equiv a^{m+k(p-1)} \equiv a^m (a^{p-1})^k \equiv a^m 1^k \equiv a^m \pmod{p}.$$

En el segon, com que $n, m \geq 1$ resulta que $p|a^n$, $p|a^m$ i per tant

$$a^n \equiv a^m \equiv 0 \pmod{p} \quad . \quad \square$$

Exemple. Calculem el residu de 4^{3141} mòdul 137 reduint amb Fermat. Com que $3141 \equiv 13 \pmod{136}$ tenim que

$$4^{3141} \equiv 4^{13} \equiv 67108864 \equiv 99 \pmod{137}.$$

Exercicis:

1. Calculeu:

- a. $3^{247} \pmod{17}$.
- b. $19^{1976} \pmod{23}$.
- c. (R) $34773^{4969} \pmod{151}$.
- d. $25^{1025} \pmod{251}$.

2. Calculeu, usant Fermat i la última propietat de les congruències:

- a. $3^{7000} \pmod{6}$.
- b. $11^{1234} \pmod{14}$.
- c. (R) $8^{1235} \pmod{15}$
- d. $50^{810} \pmod{35}$.
- e. $1800^{1800} \pmod{77}$.