

- Demostra que el quadrat d'un parell és parell

Dem: k parell $\Rightarrow k = 2n \Rightarrow k^2 = (2n)^2 = 4n^2 \Rightarrow 2 \underbrace{(2n^2)}_m \Rightarrow 2m$ parell.

1.1. PROPOSICIONS

Una proposició és un enunciat que pot ser cert o fals (1, v / 0, f)

ex: $(a+3)^2 = a^2 + 6a + 9$ per a qualsevol valor de a real.

* Lletres proposicionals $\rightarrow p, q, r \dots$

* Conectius $\rightarrow \wedge$ (i, conjunció) / \vee (o) / \rightarrow (llavors) / \leftrightarrow (si només si) / \neg (no)

Connectiu \neg		ex: $p : 3+3=6$ cert		$\neg p : 3+3 \neq 6$ fals	
P	$\neg p$				
1	0				
0	1	$\neg p$ té el mateix valor que p .			

P	$\neg p$	$\neg\neg p$
1	0	1
0	1	0

Connectiu $\wedge, \vee, \rightarrow, \leftrightarrow$

		\neg consequent			
antecedent		p	q	$p \wedge q$	$p \vee q$
1	1	1	1	1	1
1	0	0	1	0	1
0	1	0	1	1	1
0	0	0	0	1	1

* Quan $p \rightarrow q$ si l'antecedent es fals la proposició SEMPRE té un valor cert.

1.2. FÓRMULES LÒGIQUES

Són successions de símbols a partir de les regles següents:

R1 - Les lletres proposicionals són fórmules

R2 - Si ψ i Ψ són fórmules, uavors ($\psi * \Psi$) és fórmula

R3 - Si ψ és fórmula, uavors $\neg\psi$ és fórmula

ex. $\neg(p \rightarrow q)$ R1 - p és fórmula

R1 - q és fórmula

R2 - $(p \rightarrow q)$ és fórmula

R3 - $\neg(p \rightarrow q)$ és fórmula

1.3. EQUIVALENCIA DE FÓRMULES

* ψ, Ψ fórmules on $\psi \equiv \Psi$ vol dir que $\psi ; \Psi$ tenen la mateixa taula de veritat.

ex: $\psi \rightarrow \psi \equiv \neg\psi \vee \psi$

ψ	Ψ	$\psi \rightarrow \Psi$	$\neg\psi$	$\neg\psi \vee \psi$
1	1	1	0	1
1	0	0	0	0
0	1	1	1	1
0	0	1	1	1

Equivalències bàsiques

De Morgan $\rightarrow \neg(\psi \wedge \theta) \equiv \neg\psi \vee \neg\theta$

Commutatives \wedge, \vee , Assosiatives i Distributives

Doble negació $\rightarrow \neg\neg\psi \equiv \psi$

Traducció de la " \rightarrow ". $\psi \rightarrow \theta \equiv \neg\psi \vee \theta$

Traducció de la " \leftrightarrow ": $\psi \leftrightarrow \theta \equiv (\psi \rightarrow \theta) \wedge (\theta \rightarrow \psi)$

* Demostra sense taules de veritat que $(\psi \vee \theta) \rightarrow \psi \equiv (\psi \rightarrow \psi) \wedge (\theta \rightarrow \psi)$

Dem:

$$(\psi \vee \theta) \rightarrow \psi \equiv \neg(\psi \vee \theta) \vee \psi \equiv \text{De morgan} : (\neg\psi \wedge \neg\theta) \vee \psi \equiv \text{distributiva}$$

$$(\neg\psi \vee \psi) \wedge (\neg\theta \vee \psi) \equiv (\psi \rightarrow \psi) \wedge (\theta \rightarrow \psi)$$

TALLER LAB. 17 SEPT

PROFE TALLER: CARLOS SERRA

Ed. 2, Desp. 424

Exercicis sumatoris

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

$$1. \sum_{i=0}^{24} -2 + 2i = -2 + 0 + 2 + 4 + 6 + \dots + 50$$

$$2. \sum_{i=0}^{23} 2i + 1 = 3 + 5 + 7 + \dots + 55$$

$$3. \sum_{i=0}^{25} (-1)^{(i+1)} \cdot 2i = 2 - 4 + 6 - \dots + 50$$

$$4. \sum_{i=0}^{24} (-1)^{(i+1)} (2i+1)^2 = -1^2 + 3^2 - 5^2 + 7^2 - \dots - 49^2$$

$$5. \sum_{i=0}^{15} \frac{2+3i}{(1+4i)^3} = \frac{2}{1^3} + \frac{5}{5^3} + \frac{8}{9^3} + \frac{11}{13^3} + \dots + \frac{47}{61^3}$$

$$6. \sum_{i=0}^{19} 3i - 3 = -3 + 0 + 3 + 6 + 9 + 12 + \dots + 60$$

$$7. \sum_{i=0}^{20} (-1)^i (1+3i)^3 = 1^3 - 4^3 + 7^3 - 10^3 + \dots + 61^3$$

$$8. \sum_{i=0}^9 (-1)^i \frac{1}{(3+4i)} = \frac{1}{3} - \frac{1}{7} + \frac{1}{11} - \frac{1}{15} + \dots - \frac{1}{39}$$

$$9. \sum_{i=0}^{30} (-1)^{(i+1)} \left(\frac{2+2i}{(1+3i)^3} \right) = -\frac{2}{1^3} + \frac{4}{4^3} - \frac{6}{7^3} + \frac{8}{10^3} - \dots - \frac{42}{61^3}$$

PROPIETATS
SUMATORIS

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

$$\sum_{i=m}^n cf(i) = c \sum_{i=m}^n f(i)$$

$$\text{II. a) } \sum_{i=0}^{n+1} a_i - \sum_{i=0}^n a_i =$$

$$\text{b) } \sum_{i=1}^{n+2} a_i - \sum_{i=1}^{n-1} a_i =$$

$$\text{III. Calcula } \sum_{k=1}^n (k+3)^2 \text{ sabent que } \sum_{i=1}^n k = \frac{n(n+1)}{2} \text{ i } \sum_{i=1}^n k^2 = \frac{n(n+1)(2n+1)}{6}$$

$$\sum_{k=1}^n (k+3)^2 = \sum_{k=1}^n (k^2 + 6k + 9) = \sum_{k=1}^n k^2 + \sum_{k=1}^n 6k + \sum_{k=1}^n 9 = \sum_{k=1}^n k^2 + 6 \sum_{k=1}^n k + \sum_{k=1}^n 9 =$$

$$= \frac{n(n+1)(2n+1)}{6} + 6 \cdot \frac{n(n+1)}{2} + 9n = n \left[\frac{(n+1)(2n+1) + 18(n+1) + 54}{6} \right] =$$

$$= n \cdot \left[\frac{2n^2 + n + 2n + 1 + 18n + 18 + 54}{6} \right] = n \cdot \left[\frac{2n^2 + 21n + 73}{6} \right]$$

15. Canvia l'índex dels sumatoris per que comencin en $j=0$.

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

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

1)

* Progressions aritmètiques

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

$$a_i = a_{i-1} + d \rightarrow a_n = a_1 + (n-1)d$$

ex.: $a_n = 5n - 3$ és una progressió aritmètica amb diferència $d = 5$.

$$\text{Suma d'una progressió aritmètica} \rightarrow \sum_{i=m}^n a_i = \frac{(a_m + a_n)(n-m+1)}{2} = \frac{a_m + a_n}{2} \cdot n$$

* Progressions geomètriques

Cada terme a_{i+1} s'obté de l'anterior a_i multiplicat per una quantitat r anomenada raó $a_{i+1} = r a_i \rightarrow a_i = a_{i-1} \cdot r \rightarrow a_n = a_m \cdot r^{n-1}$

ex. $a_n = \frac{3}{4} 2^n$ és una progressió geomètrica amb raó $r = 2$

$$\text{Suma d'una progressió geomètrica amb } r \neq 1 \rightarrow \sum_{i=m}^n a_i = \frac{a_{n+1} - a_m}{r - 1} = \frac{a_n \cdot r - a_m}{r - 1}$$

PRODUCTORIS

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

PROPIETATS
DELS
PRODUCTORIS

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

$$17 \quad \text{calculieu} \quad \frac{\prod_{i=2}^{n+2} a_i}{\prod_{i=2}^n a_i}$$

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

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

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

$$19. \quad \text{Si } A = \prod_{i=n}^m a_i \text{ i } B = \prod_{i=n}^m b_i = \prod_{j=n}^m b_j$$

$$\text{a) } \prod_{i=n}^m a_i b_i = a_n \cdot b_n \circ a_{n+1} \cdot b_{n+1} \dots a_m \cdot b_m = (a_n \dots a_m) (b_n \dots b_m) =$$

$$= \left(\prod_{i=n}^m a_i \right) \left(\prod_{i=n}^m b_i \right) = A \cdot B$$

$$\text{b) } \prod_{i=n}^m \prod_{j=n}^m a_i b_j = \prod_{i=n}^m \left(\prod_{j=n}^m a_i + b_j \right) = \prod_{i=n}^m (a_i b_n \circ a_i b_{n+1} \dots a_i b_m) =$$

$$= \prod_{i=n}^m (a_i^{(m-n+1)} \cdot (b_n \dots b_m)) = \prod_{i=n}^m (a_i)^{m-n+1} \cdot B = (B)^{m-n+1} \prod_{i=n}^m (a_i)^{m-n+1} =$$

$$= (B)^{m-n+1} (a_n)^{m-n+1} \cdot (a_{n+1})^{m-n+1} \cdot (a_m)^{m-n+1} = (B)^{m-n+1} \cdot (a_n \cdot a_{n+1} \cdot a_m)^{m-n+1} =$$

$$= (B)^{m-n+1} (A)^{m-n+1} = (AB)^{m-n+1}$$

LÓGICA i DEMOSTRACIONS

$$5. \quad \psi \leftrightarrow (\psi \leftrightarrow \theta) \equiv (\psi \leftrightarrow \psi) \leftrightarrow \theta$$

$$\text{Si } \psi \leftrightarrow (\psi \leftrightarrow \theta) \equiv \psi \leftrightarrow ((\psi \rightarrow \theta) \wedge (\theta \rightarrow \psi)) \equiv$$

$$[\psi \rightarrow ((\psi \rightarrow \theta) \wedge (\theta \rightarrow \psi))] \wedge [((\psi \rightarrow \theta) \wedge (\theta \rightarrow \psi)) \rightarrow \psi] \equiv$$

$$\neg \psi \vee [(\psi \rightarrow \theta) \wedge (\theta \rightarrow \psi)] \wedge (\neg [(\psi \rightarrow \theta) \wedge (\theta \rightarrow \psi)] \rightarrow \psi) \equiv$$

...

$$7. \quad \psi \rightarrow (\psi \vee \theta) \equiv (\psi \wedge \neg \psi) \rightarrow \theta$$

$$\text{Si } \psi \rightarrow (\psi \vee \theta) \equiv \neg \psi \vee (\psi \vee \theta) \equiv (\neg \psi \vee \psi) \vee \theta \equiv \neg (\neg \psi \vee \psi) \vee \theta \equiv$$

$$\neg (\neg \psi \wedge \neg \psi) \vee \theta \equiv \neg (\psi \wedge \neg \psi) \vee \theta \equiv (\psi \wedge \neg \psi) \rightarrow \theta$$

$$9. \quad \neg (\psi \leftrightarrow \psi) \equiv \neg \psi \leftrightarrow \psi$$

$$\neg ((\psi \rightarrow \psi) \wedge (\psi \rightarrow \psi)) \equiv \neg (\psi \rightarrow \psi) \vee \neg (\psi \rightarrow \psi) \equiv \neg (\neg \psi \vee \psi) \vee \neg (\neg \psi \vee \psi) \equiv$$

$$(\psi \wedge \neg \psi) \vee (\psi \wedge \neg \psi) \equiv [((\psi \wedge \neg \psi) \vee \psi) \wedge ((\psi \wedge \neg \psi) \vee \neg \psi)] \equiv$$

$$[(\psi \wedge \psi) \wedge (\neg \psi \vee \psi)] \wedge [(\psi \vee \neg \psi) \wedge (\neg \psi \vee \neg \psi)] \equiv (\neg \psi \vee \psi) \wedge (\neg \psi \vee \neg \psi) \equiv$$

$$(\neg \psi \rightarrow \psi) \wedge (\psi \rightarrow \neg \psi) \equiv (\neg \psi \rightarrow \psi)$$

- TAUTOLOGIA
- CONTRADICCIÓ

14. LÒGICA DE PREDICATS

Univers de discurs
 Predicat: $P(x) \rightarrow M = \mathbb{Z}$ → $P(2)$ falsa
 "x és senar"

FÒRMULES DE PREDICAT

Conjunt de seqüències de fòrmules atòmiques, connectius i quantificadors.
 seguit de regles següents:

- R1: Les atòmiques són fòrmules
- R2: Si α és fórmula, $\neg\alpha$ també
- R3: Si α, β són fòrmules, $\alpha \ast \beta$ també
- R4: Si ψ és fórmula i x és una variable llavors $\forall x \psi, \exists x \psi$ també són fòrmules.

$\left\{ \begin{array}{l} \forall \text{ per a qualsevol } (\text{ex: } \forall x \psi \text{ per a qualsevol } x \in U \text{ } \psi \text{ és certa}) \\ \exists \text{ existeix } (\text{ex } \exists x \psi \text{ existeix } x \in U \text{ tq } \psi \text{ és certa}) \end{array} \right.$

ex: $\forall x (x \text{ és senar})$

Dem: fals, ja que $x=2$ no és senar \square

$\exists x (x \text{ és senar})$

Dem: cert, ja que $x=3$ és senar \square

$$U = \{a, b, c\} \quad \left| \begin{array}{l} \forall x P(x) \text{ cert; } P(a) \wedge P(b) \wedge P(c) \text{ és 1. fals; } \neg P(a) \vee \neg P(b) \vee \neg P(c) \text{ és 1. fals; } \\ \exists x P(x) \text{ cert; } P(a) \vee P(b) \vee P(c) \text{ és 1. fals; } \neg P(a) \wedge \neg P(b) \wedge \neg P(c) \text{ és 1. fals; } \end{array} \right.$$

NOMA: $\forall x P(x)$ es pot escriure $\forall x (x \in U \rightarrow P(x))$ o també $\forall x \in U P(x)$.
 $\exists x P(x)$ es pot escriure $\exists x (x \in U \wedge P(x))$

ex: $\exists x (\underbrace{x^2 < 0}_{\text{fals}} \rightarrow x=8)$ per tant és cert \square

$\exists x \in \mathbb{Z} \text{ tq } x^2 + 3 = 9 ; x = \pm \sqrt{6} \notin \mathbb{Z}$, per tant és fals \square

ex: Donat un real qualsevol sempre es pot trovar un natural més gran:

$\forall x \in \mathbb{R} \exists y \in \mathbb{N} \text{ tq } y > x$ Això es cert; Demostrena-ho:

Sigui $x \in \mathbb{R}$ qualsevol. Basta considerar $\max \{ \lfloor x \rfloor + 1, 0 \}$
 o bé $\lfloor x \rfloor + 1$. \square

Equivalències de fórmules

$$\begin{aligned} \neg \forall x \psi &\equiv \exists x \neg \psi ; \quad \neg \exists x \psi \equiv \forall x \neg \psi \\ \neg \forall y \forall x \psi &\equiv \forall y \neg \forall x \psi ; \quad \exists x \exists y \psi \equiv \exists y \exists x \psi \\ \star \forall x (\psi \wedge \psi) &\equiv \forall x \psi \wedge \forall x \psi ; \quad \exists x (\psi \vee \psi) \equiv \exists x \psi \vee \exists x \psi \star \\ \hookrightarrow \forall x (\psi \vee \psi) &\rightarrow \text{fals!} \quad \hookrightarrow \exists x (\psi \wedge \psi) \rightarrow \text{fals} \end{aligned}$$

Demostra que és fals $\forall x (\psi \vee \psi)$:

$$U = \mathbb{R}$$

$$\begin{array}{ll} \psi : x \geq 0 & \forall x (\psi \vee \psi) \text{ cert en canvi } \forall x \psi \vee \forall x \psi \text{ és fals} \\ \psi : x < 0 & \end{array}$$

Demostra que $\exists x (\psi \wedge \psi)$ és fals:

Demostra que $\forall x \exists y \psi \not\equiv \exists y \forall x \psi$:

$$p.17 \text{ ex. } 18 \quad \neg \exists x (C(x) \wedge N(x)) \equiv \forall x (C(x) \rightarrow \neg N(x))$$

$$\begin{array}{c} \text{Dem: } \neg \exists x (C(x) \wedge N(x)) \equiv \forall x \neg (C(x) \wedge N(x)) \equiv \forall x (\neg C(x) \vee \neg N(x)) \equiv \forall x (C(x) \rightarrow \neg N(x)) \\ \uparrow \quad \uparrow \quad \uparrow \\ \neg \exists x \psi \equiv \forall x \neg \psi \quad \neg (P \wedge Q) \equiv \neg P \vee \neg Q \quad \neg P \vee \neg Q \equiv P \rightarrow Q \end{array}$$

p.17 ex. 19 i p.18 ex. 25 i 26.

1.5. FORMALITZACIÓ

- * $\forall x (A(x) \rightarrow B(x))$: tots els individus de tipus A que tenen la propietat A tenen tmb B.
 $\forall x P(x)$ és $\forall x (x \in U \rightarrow P(x))$
- * $\exists x (A(x) \wedge B(x))$: hi han individus de tipus A que tenen la propietat B.
 $\exists x P(x)$ és $\exists x (x \in U \wedge P(x))$

p. 19. ex 27.

27. En aquest exercici el domini és el conjunt dels enters. A més de les variables, connectives i quantificadors, podeu utilitzar només els símbols següents:
 i. $<$, $,$, $=$, $+$, 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. Cap nombre primer és un quadrat.
 d. (R) Tot enter múltiple de 3 i de 5 és múltiple de 15.
 e. 2 és primer i és parell.
 f. Tot quadrat parell és múltiple de 4.

$$* \exists t \ x = y$$

a) 1 no és primer

$$\neg P(1)$$

$$b) \forall x [6/x \rightarrow (3/x \wedge 2/x)]$$

Dem: sigui x un enter qualsevol i sigui $6/x$. Per tant
 $\exists t \ x = 6t \quad 6t = 2(3t) \text{ i } 6t = 3(2t) \quad \square$

QUANTIFICADORS BARREJATS

$$\begin{aligned} \forall x \exists y \not\equiv \exists y \forall x \psi &\text{ en canvi } \forall x \forall y \psi \equiv \forall y \forall x \psi \\ \exists x \exists y \psi &\equiv \exists y \exists x \psi \end{aligned}$$

$\forall x \exists y \ x = 3y \rightarrow$ Dem: sigui x un real qualsevol, basta prendre $y = x/3 \in \mathbb{R}$.

1.6. DEMOSTRACIONS

És una justificació de la veritat d'un enunciat seguint unes regles força precises.

DEMOSTRACIÓ DIRECTA

$P \Rightarrow Q$ "P implica Q" significa que si P és cert Q també.

ex: Tot nombre parat té quadrat parat
sigui $n \in \mathbb{Z}$ un enter qualsevol $n \Rightarrow n^2$

$P \Leftrightarrow Q$ "Si P és certa Q també"

ex: La suma de dos enters consecutius és senar

x enter $\Rightarrow x + (x+1)$ senar

$\exists n \in \mathbb{Z} \forall x (x \in \mathbb{Z} \rightarrow x + (x+1) = 2n+1)$

Dem: $x + (x+1) = 2x+1$ senar per tant c.v.d.

ex: Demostra que $x > 1 \Rightarrow \frac{1}{x-1} + \frac{1}{x+1} > 0$

Dem. $\frac{1}{x-1} + \frac{1}{x+1} > 0 \Rightarrow \frac{2x > 0}{(x-1)(x+1) > 0}$ ja que $x > 1$ c.v.d.

DEMOSTRACIÓ PER CONTRA RECÍPROC

Per demostrar $P \Rightarrow Q$, fem $\neg Q \Rightarrow \neg P$

ex: nº parell \Rightarrow nº senar

Dem: contrareciproca, nº senar \Rightarrow nº senar

Sigui n un enter qualsevol

nº senar $\Rightarrow \exists t \in \mathbb{Z} \text{ tq } n = 2t+1 \Rightarrow n^2 = 4t^2 + 4t + 1 \Rightarrow n^2$ senar
 \uparrow
per def de
senar

\uparrow
per def. de
senar

ex: $a, b, c > 0 \in \mathbb{R}$

$c = ab \Rightarrow a \leq \sqrt{c} \text{ o } b \leq \sqrt{c}$

Dem: contrareciproca, $a > \sqrt{c}$; $b > \sqrt{c} \Rightarrow c \neq ab$

en efecte $a > \sqrt{c}$; $b > \sqrt{c} \Rightarrow ab > \sqrt{c}\sqrt{c} = c \Rightarrow ab \neq c$ c.v.d.

\uparrow

$\begin{cases} x > y \\ z > t \end{cases} \Rightarrow xz > yt$
reals positius

DEMOSTRACIÓ REDUCCIÓ A L'ABSURD

Demostrem A : Suposem que A és fals

19 dem. que $\sqrt{2} \notin \mathbb{Q} = \left\{ \frac{a}{b} \mid a, b \in \mathbb{Z}, b \neq 0 \right\}$

fracció

Dem: suposem que $\sqrt{2} \in \mathbb{Q}$, és a dir, $\exists a, b \in \mathbb{Z}, b \neq 0$ tq $\sqrt{2} = \frac{a}{b}$ irreductible
 $\sqrt{2} = \frac{a}{b} \Rightarrow 2 = \frac{a^2}{b^2} \Rightarrow 2b^2 = a^2 \Rightarrow a^2$ és parell $\Rightarrow a$ és parell \Rightarrow
 $\Rightarrow \exists t \in \mathbb{Z} \text{ tq } a = 2t \Rightarrow 2b^2 = 4t^2 \Rightarrow b^2 = 2t^2 \Rightarrow b^2$ és parell $\Rightarrow b$ és parell \Rightarrow
 $\Rightarrow a$ i b parell $\Rightarrow \frac{a}{b}$ és reducible. Per tant contradicció. c.v.d.

21. Si $a, b, c \in \mathbb{Z}$ dem. $a+b$ és parell o $b+c$ és parell o $c+a$ és parell.

Dem (RA) : Suposem $a+b$ senar i $b+c$ senar i $c+a$ senar

$$2a+2b+2c = 2(a+b+c) \Rightarrow 2(a+b+c) \text{ és parell} \Rightarrow a, b, c \text{ senars} \Rightarrow$$

$$\Rightarrow \exists t, x, y \in \mathbb{Z} \text{ tq } a = 2t+1, b = 2x+1, c = 2y+1 \Rightarrow a+b+c = 2(t+x+y)+1 \Rightarrow$$

$\Rightarrow a+b+c$ és senar per tant contradicció

Demostrém A \Rightarrow B : suposem que A és cert i B fals.

33. $x \in \mathbb{Q}$ } $\Rightarrow x+y \notin \mathbb{Q}$ seguin x, y qualsevol
 $y \notin \mathbb{Q}$

Dem (RA) : Suposem que $x \in \mathbb{Q}$, $y \notin \mathbb{Q}$ i $x+y \in \mathbb{Q}$

$$\left\{ x = \frac{a}{b} \mid a, b \in \mathbb{Z} \text{ i } b \neq 0 \right\}, \left\{ x+y = \frac{c}{d} \mid c, d \in \mathbb{Z} \text{ i } d \neq 0 \right\}; y \notin \mathbb{Q}$$

$$y = \frac{c}{d} - \frac{a}{b} = \frac{cb-ad}{db} \text{ és fracció per tant contradicció.}$$

34. $a, b, c \in \mathbb{Z}$ $a+b+c=0$ uawors com a mínim un és parell.

Dem (RA) : $a, b, c \in \mathbb{Z}$, $a+b+c=0$ i a, b, c senars

$\Rightarrow a+b+c=0$ on a, b, c senar i 0 parell per tant absurd.

ALTRES DEMOSTRACIONS

* Prova d'una disjunció $B \vee C$: fem $\neg B \Rightarrow C$

41. Si $n \in \mathbb{Z}$ uawors n senar o n^2 és múltiple de 4.

Dem: Suposem n parell, veiem n^2 és múltiple de 4.

$$(2t)^2 = 4t^2 \text{ és múltiple de 4. c.v.d.}$$

* Disjunció en el conseqüent $A \Rightarrow B \vee C$: fem $A \wedge \neg B \Rightarrow C$

50. $x, y \in \mathbb{R}$. Si $x+y \leq 2$ uawors $x \leq 1$ o $y \leq 1$

Dem: Suposem $x+y \leq 2$ i $x > 1 \Rightarrow y \leq 1$

$$y \leq 2-x < 2-1 = 1; \text{ és a dir } y \leq 1 \text{ c.v.d.}$$

* Disjunció a l'anterior $B \vee C \Rightarrow A \quad \begin{cases} B \Rightarrow A \\ C \Rightarrow A \end{cases}$

63. $n \in \mathbb{Z}$. Si $\frac{n}{4} \quad \text{①} \quad 0 \quad \frac{n}{4} \quad \text{③}$, uawors $\frac{n^2}{4} \quad \text{①}$

Dem: 1) Suposem que $n = 4q+1$ ($q \in \mathbb{Z}$)

$$n^2 = 16q^2 + 8q + 1 = 4(4q^2 + 2q) + 1 \text{ per tant } \frac{n^2}{4} \quad \text{①}$$

2) Suposem que $n = 4q+3$ ($q \in \mathbb{Z}$)

$$n^2 = 16q^2 + 24q + 9 = 4(4q^2 + 6q + 2) + 1 \text{ per tant } \frac{n^2}{4} \quad \text{①}$$

* PROVA PER CASOS

Volem demostrar B . Fem $A_1 \Rightarrow B \dots A_n \Rightarrow B$ inventem n casos.

67. $n \in \mathbb{Z}$. Dem que n^2+n és parell.

Dem: Suposem n parell $\Rightarrow \exists t \in \mathbb{Z} \text{ tq } n = 2t \Rightarrow n^2+n = 4t^2+2t = 2(2t^2+t) \Rightarrow$
 $\Rightarrow n^2+n$ és parell

Suposem n senar $\Rightarrow \exists t \in \mathbb{Z} \text{ tq } n = 2t+1 \Rightarrow n^2+n = (2t+1)^2+(2t+1) =$
 $= 2(2t^2+3t+1) \Rightarrow n^2+n$ parell.

TALLER 02/09

p. 17

$$20. \exists x (P(x) \rightarrow Q(x)) \equiv \forall x P(x) \rightarrow \exists x Q(x)$$

$\exists x (P(x) \rightarrow Q(x)) \Rightarrow$ traducció de la fletxa, $\exists x (\neg P(x) \vee Q(x))$
 $\Rightarrow \exists x \neg P(x) \vee \exists x Q(x) \Rightarrow \neg \forall x P(x) \vee \exists x Q(x) \Rightarrow$ traducció fletxa $\neg \forall x P(x) \rightarrow \exists x Q(x)$
 pertant $\exists x (P(x) \rightarrow Q(x)) \equiv \forall x P(x) \rightarrow \exists x Q(x)$

$$21. \neg \forall x (P(x) \leftrightarrow Q(x)) \equiv \exists x (P(x) \wedge \neg Q(x)) \vee \exists x (Q(x) \wedge \neg P(x))$$

$\neg \forall x (P(x) \leftrightarrow Q(x)) \Rightarrow \exists x \neg (P(x) \leftrightarrow Q(x)) \Rightarrow$ traducció doble fletxa,

$\exists x [(P(x) \wedge \neg Q(x)) \vee (Q(x) \wedge \neg P(x))] \Rightarrow$ distributiva,

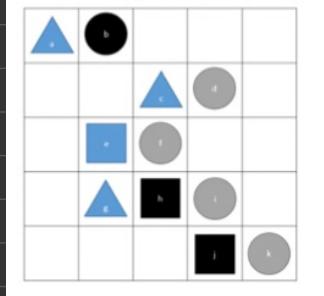
$$\exists x (P(x) \wedge \neg Q(x)) \vee \exists x (Q(x) \wedge \neg P(x)).$$

Pertant $\neg \forall x (P(x) \leftrightarrow Q(x)) \equiv \exists x (P(x) \wedge \neg Q(x)) \vee \exists x (Q(x) \wedge \neg P(x))$.

22. Demostra que $\exists x (P(x) \rightarrow \forall y P(y))$ sempre és certa (sigui qui sigui P).

$\exists x (P(x) \rightarrow \forall y P(y)) \Rightarrow$ traducció de la fletxa $\exists x (\neg P(x) \vee \forall y P(y)) \equiv 1$
 per tant arribem a una tautologia.

25.



$T(x)$: 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

f) $\forall x (C(x) \rightarrow E(x, d))$

l) $\exists x (T(x) \wedge \neg G(x))$

g) $\exists x B(x)$

m) $\forall x (Q(x) \rightarrow \neg K(x, b))$

h) $\forall x (Q(x) \rightarrow N(x))$

n) $\exists x (C(x) \rightarrow B(x))$

i) $\forall x (T(x) \rightarrow E(x, d))$

o) $\forall x (C(x) \rightarrow S(x, d))$

j) $\exists x (T(x) \rightarrow E(x, d))$

p) $\forall x [C(x) \rightarrow (E(x, a) \vee S(x, b))]$

k) $\exists x [T(x) \wedge (S(x, a) \wedge \neg E(x, a))]$

28. a) $\exists n \in \mathbb{Z} (n \cdot x = y)$
- b) $\exists n \in \mathbb{Z} (n \cdot n = x)$ ↗ es correcto pero muy largo.
- c) $\exists n, m \in \mathbb{Z} (\neg(n=1) \wedge \neg(m=1) \wedge \neg(n=x) \wedge \neg(m=x) \wedge \neg(n \cdot m = x))$
 $(\exists n, m \in \mathbb{Z}, x = n \cdot m) \rightarrow ((n=1 \wedge m=x) \vee (n=x \wedge m=1)) \in P(x)$
- d) $\forall x \in \mathbb{Z} [P(x) \wedge (\exists n \in \mathbb{Z} (x = 2n)) \rightarrow x = 2]$
- e) $\forall x \in \mathbb{Z} [P(x) \rightarrow \exists y \in \mathbb{Z} (P(y) \wedge (y > x))]$
- f) $\forall y \forall z (z = y \cdot z \rightarrow (y = 1 \vee y = -1 \vee z = 1 \vee z = -1)) \wedge$
 $\forall x (\forall y \forall z (x = y \cdot z \rightarrow (y = 1 \vee y = -1 \vee z = 1 \vee z = -1)) \rightarrow (x = 2 \vee x > 2))$
-

Demostra que $A \not\Rightarrow B$: trovant un cas en què A és cert i B és fals.

ex: $x^2 > 1 \Rightarrow x > 1$; $\forall x (x^2 > 1 \rightarrow x > 1)$ fals

Dem: contraexemple $\exists x (x^2 > 1 \wedge x \leq 1)$ cert

Prenem $x = -2$

$$(-2)^2 > 1 \wedge -2 \leq 1$$

Demostra $P \Leftrightarrow Q$ vol dir $\begin{cases} P \Rightarrow Q \text{ directe} \\ Q \Rightarrow P \text{ reciprocal o invers} \end{cases}$

88. n, m són enters

$n \cdot m$ parell $\Leftrightarrow n$ parell $\vee m$ parell

Dem | Contrarecíproc: m senar \wedge n senar $\Rightarrow m \cdot n$ senar
| m parell: $\exists t \in \mathbb{Z} m = 2t$; $2t \cdot n = 2(t+n) \Rightarrow mn$ parell
| n parell: analogament

87. $a, b \in \mathbb{R}$

$$a > \frac{a+b}{2} \stackrel{A}{\equiv} a > b \stackrel{B}{\equiv} b < \frac{a+b}{2} \stackrel{C}{\equiv}$$

Dem. A \Rightarrow B) $a > \frac{a+b}{2} \Rightarrow 2a > a+b \Rightarrow 2a - a > b \Rightarrow a > b$

B \Rightarrow C) $b < \frac{a+b}{2} \Rightarrow 2b < a+b \Rightarrow b < a$

C \Rightarrow A) $b < \frac{a+b}{2} \Rightarrow 2b < a+b \Rightarrow b < a \Rightarrow a + b < 2a \Rightarrow a > \frac{a+b}{2}$

89. a, b racionals, Demostra que $a + b\sqrt{2}$ racional $\Leftrightarrow b = 0$

• $b = 0 \Rightarrow a + b\sqrt{2} = 0$ és racional

• RA suposem $a + b\sqrt{2} = \frac{c}{d}$ ($\exists c, d \in \mathbb{Z}$, $d \neq 0$) i $b \neq 0$

$a + b\sqrt{2} = \frac{c}{d} \Rightarrow b\sqrt{2} = \frac{c}{d} - a = \frac{c-ad}{d} \Rightarrow \sqrt{2} = \frac{c-ad}{db}$ és racional,
absurd ja que $\sqrt{2}$ no és racional.

- TEMA 2: INDUCCIÓ -

1. INDUCCIÓ SIMPLE

És vol demostrar $P(n)$ cert $\forall n \geq n_0$.

* PAS BASE $P(n_0)$ cert

ex: Demostra que $\sum_{i=1}^n \frac{1}{(4i-3)(4i+1)} = \frac{n}{4n+1}$ per a $n \geq 1$.

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

$P(n)$

$$P(1) : \sum_{i=1}^1 \frac{1}{(4i-3)(4i+1)} = \frac{1}{1 \cdot 5} = \frac{1}{5} \quad \left(= \frac{1}{4 \cdot 1 + 1} \right) \text{ per tant cert}$$

* PAS INDUCTIU sigui $n \geq 1$ { Hipòtesi d'inducció : $P(n-1)$ cert
Hipòtesi d'inducció : $P(n)$ cert

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

tesi $P(n) : \sum_{i=1}^n \frac{1}{(4i-3)(4i+1)} = \frac{n}{4n+1}$

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

Propietat associativa de la suma

★ No t'oblidis d'on vols arribar

$$= \frac{1}{4n-3} \left[n-1 + \frac{1}{4n+1} \right] = \frac{1}{4n-3} \left[\frac{n-1(4n+1)+1}{4n+1} \right] = \frac{1}{4n-3} \left[\frac{4n^2-3n}{4n+1} \right] =$$

$$= \frac{4n^2-3n}{(4n-3)(4n+1)} = \frac{n(4n-3)}{(4n-3)(4n+1)} = \frac{n}{4n+1} \quad \text{c.v.d.}$$

* Pel principi d'inducció $P(n)$ és cert $\forall n \geq n_0$.

ex: Demostra $\prod_{i=1}^n \left(1 + \frac{2}{i}\right) = \frac{(n+1)(n+2)}{2}$ per a $n \geq 1$

* PAS BASE $P(1) : \prod_{i=1}^1 \left(1 + \frac{2}{i}\right) \stackrel{?}{=} \frac{2 \cdot 3}{2} ; 3 = 3$ cert.

* PAS INDUCTIU $n > 1$.

Hipòtesi $\prod_{i=1}^{n-1} \left(1 + \frac{2}{i}\right) = \frac{n(n+1)}{2}$

Tesi $\prod_{i=1}^n \left(1 + \frac{2}{i}\right) = \frac{(n+1)(n+2)}{2}$

$$\prod_{i=1}^n \left(1 + \frac{2}{i}\right) = \left[\prod_{i=1}^{n-1} \left(1 + \frac{2}{i}\right) \right] \left(1 + \frac{2}{n}\right) = \frac{n(n+1)}{2} \cdot \left(1 + \frac{2}{n}\right) =$$

$$= \frac{n(n+1)}{2} \cdot \frac{n+2}{n} = \frac{n^3+3n^2+2n}{2n} = \frac{n(n^2+3n+2)}{2n} =$$

$$= \frac{(n+1)(n+2)}{2} \quad \text{c.v.d.}$$

* Pel principi d'inducció $P(n)$ és cert $\forall n \geq n_0$.

ex. Demostra $\sum_{i=2}^n \frac{1}{i^2} < \frac{n-1}{n}$ per a $n \geq 2$.

$$\boxed{\sum_{i=2}^n \frac{1}{i^2}}$$

$P(n)$

* PAS BASE $\sum_{i=2}^2 \frac{1}{i^2} < \frac{2-1}{2} \rightarrow \frac{1}{4} < \frac{1}{2} \Leftrightarrow 2 < 4$ cert.

* PAS INDUCTIU Sigui $n > 2$

$$\text{hipòtesi d'inducció } \sum_{i=2}^{n-1} \frac{1}{i^2} < \frac{n-2}{n-1}$$

$$\text{tesi } \sum_{i=2}^n \frac{1}{i^2} < \frac{n-1}{n}$$

$$\sum_{i=2}^n \frac{1}{i^2} = \sum_{i=2}^{n-1} \frac{1}{i^2} + \frac{1}{n^2} < \frac{n-2}{n-1} + \frac{1}{n^2}$$

★ $A < B$ i $A < C$ uavors basta veure $B \leq C$

$$\text{Si } \frac{n-2}{n-1} + \frac{1}{n^2} \leq \frac{n-1}{n}, \text{ naunem acabat}$$

$$\frac{n^3 - 2n^2 + n - 1}{(n-1)n^2} \leq \frac{n-1}{n}; (n^3 - 2n^2 + n - 1) \cancel{n} \leq (n-1)^2 n^2; n^3 - 2n^2 + n - 1 \leq (n-1)^2 n,$$

$$n^3 - 2n^2 + n - 1 \leq n^3 - 2n^2 + n; -1 \leq 0 \text{ c.v.a.}$$

TALLER 8 D'OCTUBRE

29. $\exists x \in \mathbb{R} (x > 2 \wedge x < 6)$, cert

30. $\forall x \in \mathbb{Z} (x^2 \mid 16 \rightarrow x \mid 8)$, fals

31. $\exists x \in \mathbb{R} (x > 5 \wedge x < 2)$, fals

32. $\forall x \in \mathbb{R} (x > 2 \rightarrow x < 5)$, fals

33. $\exists x \in \mathbb{R} (x^2 - x > 1 \wedge x^2 + x < 1)$, cert

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

36. $\exists y \forall x xy = 0$, si $y = 0$, $\forall x xy = 0$. verdader

37. $\forall x \exists y (xy - 1 = 0)$ verdader

38. $\forall x \exists y (x \neq 0 \rightarrow xy - 1 = 0)$

39. $\exists y \forall x xy = x$ verdader

40. $\exists y \forall x xy = 1$

41. $\forall x \exists y (xy + 2y - 1 = 0)$

14. n enter. Si $5n^2 + 1$ és senar uavors n parell.

Dem. RA, suposem que $5n^2 + 1$ és senar i n senar.

$$\exists k \in \mathbb{Z} \text{ tq } n = 2k - 1 \Rightarrow 5n^2 + 1 = 5(2k-1)^2 + 1 = 5(4k^2 - 4k + 1) + 1;$$

$$20k^2 - 20k + 5 + 1 = 20k^2 - 20k + 6 = \underbrace{2(10k^2 - 10k + 3)}_{2n} \text{ parell} \Rightarrow \text{contradicció per tant c.v.d.}$$

15. n enter. Si n^3 senar uavors n senar

Dem. CONTRADICTION, n parell $\rightarrow n^3$ parell

$$\exists k \in \mathbb{Z} \text{ tq } n = 2k \Rightarrow n^3 = (2k)^3 = 8k^3 = \underbrace{2(4k^3)}_{2n} \text{ parell} \Rightarrow \text{per tant c.v.a.}$$

26. Demosta que $\log_2 3$ és irracional.

Dem. RA, suposem que $\log_2 3$ és racional

$\exists a, b \in \mathbb{Z} \ b \neq 0 \text{ tq } \log_2 3 = \frac{a}{b} \Rightarrow 2^{\frac{a}{b}} = 3 \Rightarrow (2^{\frac{a}{b}})^b = 3^b \Rightarrow 2^a = 3^b$

\Rightarrow per que això sigui cert a, b haureien de ser $= 0$ pertant contradicció cvd. \clubsuit

27 dem. que $\sqrt{6} \notin \mathbb{Q} = \left\{ \frac{a}{b} \mid a, b \in \mathbb{Z}, b \neq 0 \right\}$

fracció

Dem: suposem que $\sqrt{6} \in \mathbb{Q}$, és a dir, $\exists a, b \in \mathbb{Z}, b \neq 0 \text{ tq } \sqrt{6} = \frac{a}{b}$ irreductible

$\sqrt{6} = \frac{a}{b} \Rightarrow 6 = \frac{a^2}{b^2} \Rightarrow 6b^2 = a^2 \Rightarrow 2(3b^2) = a^2 \Rightarrow a^2 \text{ és parell} \Rightarrow a \text{ és parell} \Rightarrow$

$\Rightarrow \exists t \in \mathbb{Z} \text{ tq } a = 2t \Rightarrow 6b^2 = 4t^2 \Rightarrow 3b^2 = 2t^2 \Rightarrow b^2 \text{ és parell} \Rightarrow b \text{ és parell} \Rightarrow$

$\Rightarrow a \text{ i } b \text{ parell} \Rightarrow \frac{a}{b} \text{ és reducible. Per tant contradicció. c.v.d. } \blacksquare$

$3b^2 = \text{par}; \text{imp. } b^2 = \text{par}$

30. $a+c$ senar o $b-a$ senar o $b+c-1$ senar

$b^2 = \text{par} \Rightarrow b \text{ par}$

Dem. per casos 1) $a+c$ parell $b-a$ parell $b+c-1$ senar

$$\exists n, m \in \mathbb{N} \text{ tq } \begin{cases} a+c = 2n \\ b-a = 2m \end{cases} \Rightarrow b+c = 2(n+m) \Rightarrow b+c-1 = 2(n+m)-1 \text{ senar}$$

2) $a+c$ parell $b+c-1$ parell $b-a$ senar

$$\exists n, m \in \mathbb{N} \text{ tq } \begin{cases} a+c = 2n \\ b+c-1 = 2m \end{cases} \Rightarrow b-a-c+c-1 = -2n+2m \Rightarrow$$

$$\Rightarrow b-a-1 = 2(m-n) \Rightarrow b-a = 2(m-n)+1 \text{ senar}$$

3) $b+c-1$ parell $b-a$ parell $a+c$ senar

$$\exists n, m \in \mathbb{N} \text{ tq } \begin{cases} b+c-1 = 2n \\ b-a = 2m \end{cases} \Rightarrow -b+a+b+c-1 = -2m+2n \Rightarrow$$

$$\Rightarrow a+c-1 = 2(n-m) \Rightarrow a+c = 2(n-m)+1 \text{ senar.}$$

cvd \clubsuit

6. $\underline{3^n < (n+2)!} \quad \forall n \geq \underline{n_0}$

$P(n)$

Demostració:

PAS BASE $P(0)$ cert; $3^0 < 2!$ cert

PAS INDUCCIÓ; sigui $n > 0$

• Hip. Induct. $3^{n-1} < (n+1)!$

• Tensi $3^n < (n+2)!$

$3^n = 3 \cdot 3^{n-1} < 3(n+1)! ;$ Basta veure que $3(n+1)! \leq (n+2)!$

$3 \leq n+2 \Leftrightarrow \underline{1 \leq n}$ cert ja que $n > 0$

$$4. \frac{6^{2n+1} - 6}{P(n)} = 210 \quad \forall n \geq 0$$

Demostració:

PAS BASE: $P(0)$ cert; $6^1 - 6 = 210$ cert ja que $0 = 0 \cdot 210$

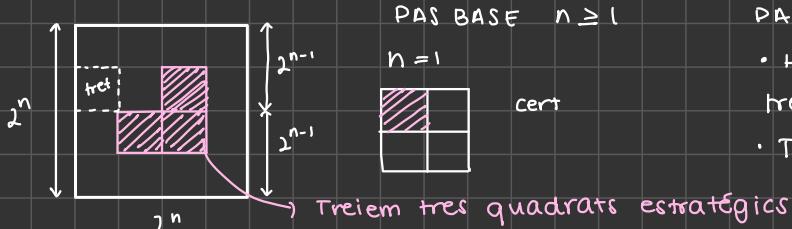
PAS INDUCCIÓ sigui $n > 0$

• Hip. induct $6^{2n-1} - 6 = 210 (= 210k)$

• Ten $6^{2n+1} - 6 = 210$

$$\begin{aligned} 6^{2n+1} - 6 &= 6^2 \cdot 6^{2n-1} - 6 = 36 \cdot 6^{2n-1} - 6 = 35 \cdot 6^{2n-1} + \underbrace{6^{2n-1} - 6}_{210k} \stackrel{\text{Hip. inductiva}}{=} 35 \cdot 6^{2n-1} + 210k = \\ &= \underbrace{35 \cdot 6 \cdot 6^{2n-2}}_{2n-2 \geq 0} + 210k = 210 \cdot [6^{2n-2} + k] = 210 \text{ cvd. } \end{aligned}$$

12. sigui $n \geq 1$



PAS BASE $n \geq 1$

PAS INDUCCIÓ sigui $n > 1$
• Hip. induct: si d'un tauler $2^{n-1} \times 2^{n-1}$ treiem 1 \square .

• Ten: "... $2^n \times 2^n$

A cada un dels 4 taulers apíguem la hip. d'inducció i ja hem acabat.

TALLER 15/10

$$56. \quad a, b, c \in \mathbb{R}, \quad (c = a+b) \rightarrow (2a \leq c) \vee (2b \leq c)$$

∨ al consequent

$$(c = a+b) \wedge (2a > c) \rightarrow 2b \leq c$$

$$a = c - b; \quad 2(c-b) > c; \quad 2c - 2b > c; \quad -2b > -c; \quad 2b \leq c$$

$$57. \quad a, b, c \in \mathbb{Z}, \quad a+c \text{ senar} \quad a+b \text{ senar o } b+c \text{ senar}$$

$$\exists k, k_1, k_2 \text{ tq } (a+c = 2k+1) \rightarrow (a+b = 2k_1+1) \vee (b+c = 2k_2+1)$$

∨ al consequent

$$(a+c = 2k+1) \wedge (a+b = 2k_1) \rightarrow (b+c = 2k_2+1)$$

$$a+c = 2k+1; \quad a = 2k+1-c$$

$$a+b = 2k_1; \quad b = 2k_1 - 2k-1 + c; \quad b = 2(k_1-k) - 1 + c; \quad b - c = 2(k_1 - k) - 1$$

Ex. 2n Parcial 8-1-2021

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

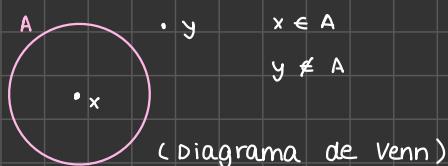
Dem: sigui x qualsevol $1r) \subseteq \neg \text{NO}$

$$x \in (B \cup A) - A \Leftrightarrow x \in B \cup A \wedge x \notin A \Leftrightarrow (x \in B \vee x \in A) \wedge x \notin A \Leftrightarrow$$

$$(x \in B \wedge x \notin A) \vee (x \in A \wedge x \notin A) \Leftrightarrow x \in B \wedge x \notin A \Leftrightarrow x \in B - A \text{ c.v.d}$$

3.1. conjunts

Conjunt A :



* Se puede escribir:

$$A = \{ 3, 4, 5, 6 \}$$

$$A = \{ x \mid x \in \mathbb{Z} \text{ and } 3 \leq x \leq 6 \}$$

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

- PRINCIPI D'EXTENSIONALITAT (= igualtat entre conjunts)

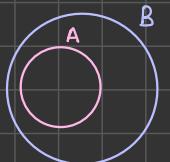
$A = B \Leftrightarrow$ contenen els mateixos elements

$$\Rightarrow \forall x (x \in A \leftrightarrow x \in B)$$

- ## conjunt Buit Ø

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

- ## • Incisió entre conjunts (\subseteq)



$A \subseteq B$; A inclòs a B o A subconjunt de B

$$\forall x (x \in A \rightarrow x \in B)$$

$$A = B \Leftrightarrow A \subseteq B \text{ and } B \subseteq A$$

* Demuestra que $A = \{ x \in \mathbb{R} \mid x \geq 0 \} = \{ x \in \mathbb{R} \mid \exists y \quad x = y^n \} = B$

1. Dem : $A \subseteq B$

sigui x qual sevo

$$x \in A \Rightarrow x \in \mathbb{R} \quad | \quad x \geq 0 \Rightarrow x = (\sqrt{x})^2 \Rightarrow x \in B$$

\uparrow \uparrow \uparrow

def. A existeix \sqrt{x} def. B

2. Dem : $B \in A$

sigui x qual sevol

PROPIETATS

* $A \subseteq A$ (dem.: $\forall x (x \in A \rightarrow x \in A)$ cert.

* $\emptyset \subseteq A$ (dem: $\forall x (x \in \emptyset \rightarrow x \in A)$ cert \square)

* $A \subseteq B$ i $B \subseteq A \Leftrightarrow A = B$ (dem: principi d'extensivitat. cert)

$$* A \subseteq B \wedge B \subseteq C \Rightarrow A \subseteq C \quad (\text{dem: } \forall x (x \in A \rightarrow x \in B) \wedge \forall x (x \in B \rightarrow x \in C), \quad x \in A \Rightarrow x \in B \Rightarrow x \in C)$$

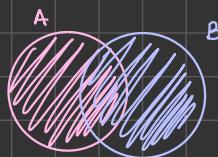
3.2. OPERACIÓNS AMB CONJUNTS

• UNIÓ

Conjunts A i B

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

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



$$\text{ex: } [-1, 3] \cup [0, 8] = [-1, 8]$$

$$\{1, 2, 3\} \cup \{2, 3, 5\} = \{1, 2, 3, 5\}$$

PROPIETATS

* $A \cup A = A$

* $A \cup \emptyset = A$ ($x \in A \vee \emptyset \Leftrightarrow \underbrace{x \in A \vee x \in \emptyset}_{P \vee \emptyset = P} \Leftrightarrow x \in A$)

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

* ASSOCIATIVA: $A \cup (B \cup C) = (A \cup B) \cup C$ ($x \in A \cup B \vee x \in C \Leftrightarrow (x \in A \vee x \in B) \vee x \in C \Leftrightarrow$ def. unió $x \in A \vee (x \in B \vee x \in C) \Leftrightarrow x \in A \vee (x \in B \cup C) \Leftrightarrow x \in A \cup (B \cup C)$)

$$\Leftrightarrow x \in A \vee (x \in B \vee x \in C) \Leftrightarrow x \in A \vee (x \in B \cup C) \Leftrightarrow x \in A \cup (B \cup C) \quad \text{def. unió}$$

def. unió

ASSOCIATIVA

* $A \subseteq A \cup B$, $B \subseteq A \cup B$

* $A \subseteq B \Leftrightarrow A \cup B = B$ (Ataquem la tesi. $x \in A \cup B \Rightarrow x \in A \vee x \in B \Rightarrow x \in B$)

def. unió

$x \in B \vee x \in B$

$P \vee P = P$

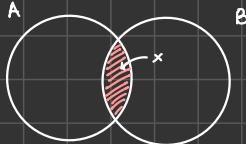
Hipòtesi

* $A \cup B \subseteq C \Leftrightarrow A \subseteq C$, $B \subseteq C$

• INTERSECCIÓ

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

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



$$\text{ex: } [-1, 3] \cap [0, 8] = [0, 3]$$

$$\{1, 2, 3\} \cap \{2, 3, 5\} = \{2, 3\}$$

PROPIETATS

* $A \cap A = A$

* $A \cap \emptyset = \emptyset$

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

* DISTRIBUTIVA: $A \cap (B \cap C) = (A \cap B) \cap C$

* $A \cap B \subseteq A$, $A \cap B \subseteq B$

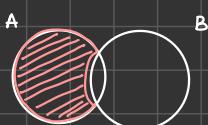
* $A \subseteq B \Leftrightarrow A \cap B = A$

* $C \subseteq A \cap B \Leftrightarrow C \subseteq A \text{ i } C \subseteq B$

• RESTA

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

$$A \subseteq B \Rightarrow A - B = \emptyset$$



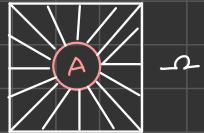
$$\text{ex: } [-1, 3] - [0, 8] = [-1, 0)$$

PROPIETATS

- * $A - A = \emptyset$
 - * $A - \emptyset = A$
 - * $\emptyset - A = \emptyset$
 - * $A - B \subseteq A$
 - * $(A - B) \cap B = \emptyset$
 - * $A \subseteq B \Leftrightarrow A - B = \emptyset$
 - * $C \subseteq A - B \Leftrightarrow C \subseteq A, C \cap B = \emptyset$

• COMPLEMENTI (A^c)

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



ex: $\Omega = \mathbb{R}$

$$[1, 7]^c = (-\infty, 1) \cup [7, +\infty)$$

$$\{3, 4, 5\}^c = \{0, 1, 2, 6, 7, 8, \dots\}$$

PROPIETATS

- * DF MORGAN $(A \cap B)^c = A^c \cup B^c$
 $(A \cup B)^c = A^c \cap B^c$
 - * $A - B = A \cap B^c \leftarrow x = \neg x$
 - * $A \cap A^c = \emptyset$
 $A \cup A^c = \Omega$

3.4. CONJUNT DE LES PARTS D'UN CONJUNT

→ conjunt dels seus subconjunts

ex: $A = \{1, 2\}$

Conjunt de les parts de A: $\{\emptyset, \{1\}, \{2\}, A\}$ = $\mathcal{P}(A)$

$$ex: \quad A = \{1, 2\} \rightarrow \mathcal{P}(A) = \{\emptyset, A\}$$

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

$$A = \emptyset \rightarrow \mathcal{P}(A) = \{\emptyset\}$$

$$\left[\mathcal{P}(A) = \{ x \mid x \subseteq A \} \right]$$

ex. 43

$\varnothing \in \mathcal{P}(A)$ dem: $\varnothing \subseteq A$ cert

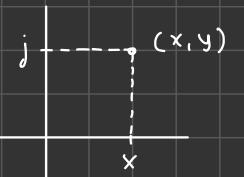
$A \in P(A)$ dem. $A \subseteq A$ cert def

$$A \in P(A) \text{ dem. } A \subseteq A \text{ cert } \stackrel{\text{def}}{P} \stackrel{\text{def}}{\subseteq} A \Leftrightarrow a \in A$$

$$\text{ex 45} \quad P(A \cap B) = P(A) \cap P(B)$$

dern : Sigui x qualsevol $x \in P(A \cap B) \stackrel{\text{def } P}{\Rightarrow} x \subseteq A \cap B \stackrel{\text{def } \subseteq}{\Rightarrow} x \subseteq A \wedge x \subseteq B \stackrel{\text{def } B}{\Rightarrow} x \in P(A) \wedge x \in P(B) \Rightarrow$

$$x \in P(A) \cap P(B)$$



Pla geomètric

$$\mathbb{R}^2 = \mathbb{R} \times \mathbb{R} = \{(x, y) \mid x \in \mathbb{R}, y \in \mathbb{R}\}$$

parell ordenat

PRODUCTE CARTESIÀ $A \times B$

↪ conjunt de parells ordenats

$$[A \times B = \{(a, b) \mid a \in A \wedge b \in B\}]$$

def: x, y elements

(x, y) parell ordenat

$$(x, y) = (z, t) \Leftrightarrow x = z \wedge y = t$$

* $(5, 7) \neq (3, 8)$ ja que $7 \neq 8$

* $(a, b) = (b, a) \Leftrightarrow a = b$ dem: $\Leftrightarrow \bar{e}s (a, a) = (a, a)$

$$\Rightarrow (a, b) = (b, a) \Rightarrow a = b \wedge b = a \Rightarrow a = b$$

ex: $A = \{1, 2\}$

$$B = \{a, b, c\}$$

$$A \times B = \{(1, a), (1, b), (1, c), (2, a), (2, b), (2, c)\}$$

$$\begin{aligned} \text{Card } A = n \\ \text{Card } B = m \end{aligned} \quad \Rightarrow \text{card}(A \times B) = n \cdot m$$

dem: $A \times \emptyset = \emptyset$ suparem que $(a, b) \in A \times \emptyset$ i arribem a un absurd.

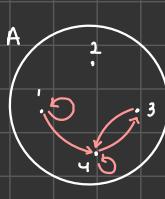
$$(a, b) \in A \times \emptyset \Rightarrow a \in A \wedge b \in \emptyset \stackrel{\text{def. } x}{\Rightarrow} b \in \emptyset \text{ absurd per def. } \emptyset$$

dem: $A \times (B \cap C) = (A \times B) \cap (A \times C)$

$$\star \text{ Sigui } (x, y) \text{ qualsevol, } (x, y) \in A \times (B \cap C) \Leftrightarrow x \in A \wedge y \in (B \cap C) \stackrel{\text{def. } x}{\Leftrightarrow} \stackrel{\text{def. } \cap}{\Leftrightarrow} (x, y) \in (A \times B) \cap (A \times C)$$

$$x \in A \wedge y \in B \wedge y \in C \stackrel{\text{def. } x}{\Leftrightarrow} (x, y) \in A \times B \wedge (x, y) \in A \times C \stackrel{\text{def. } \cap}{\Leftrightarrow} (x, y) \in (A \times B) \cap (A \times C)$$

3.5. RELACIÓ BINÀRIA EN UN CONJUNT A



1R1

1R4

3R4

4R3

4R4

Agofo els parells $\{(1, 1), (1, 4), (3, 4), (4, 3), (4, 4)\}$

$$R = \{(1, 1), (1, 4), (3, 4), (4, 3), (4, 4)\} \subseteq A \times A$$

★ El sentit
de la fletxa, conjunt
és molt important.

Una relació en A ve donada per un subconjunt $R \subseteq A \times A$.

$(x, y) \in R$ ho escribim com $x R y$

$$A = \mathbb{Z}; \quad x R y \Leftrightarrow x^2 = y^2 \quad \text{ex: } 3R3, \quad \cancel{0R4}^{\text{NO}}$$

$$A = \mathbb{R}; \quad x R y \Leftrightarrow |x| = |y| \quad \text{ex: } 7Rx \quad \forall x \in [7, 8)$$

PROPIETATS

- * REFLEXIVA $x R x \quad \forall x \in A$ (dem: $\exists x \in A \quad x R x$)
- * SIMÈTRICA $\forall x, y \in A, x R y \Rightarrow y R x$ (dem: $\exists x, y \in A \quad x R y \wedge y R x$)

- TALLER 22.10 -

ex 33. $\forall n \in \mathbb{N}, n \geq 2 \quad P(n) = n \text{ primo} \vee n = p_1 \cdot p_2 \cdots p_k$

Per inducció completa sobre n .

(1) $P(2)$? Si ja que 2 es primo

(2) $\forall n \in \mathbb{N}, n \geq 3 \quad P(k), 3 \leq k \leq n-1$

$$\hookrightarrow k \text{ primo o } k = p_1 \cdot p_2 \cdots p_m$$

En efecte

$$n \begin{cases} n \text{ primer} \\ n \text{ compost}, n = r \cdot s \end{cases} \Rightarrow n = q_1 \cdots q_t \cdot w_1 \cdots w_m = \text{prod de } n^{\circ} \text{ primers}$$

H.I. es compleix $P(r)$ y $P(s)$

$r = q_1, \dots, q_t, q_1, \dots, q_t$ són n° prim.

$s = w_1, \dots, w_m, w_1, \dots, w_m$ són n° prim.

$3 \leq r \leq n-1$

$3 \leq s \leq n-1$

ex 22. Demosta que $\left(\frac{n}{e}\right)^n < n!$ per a $n > 1$. Pista $\left(1 + \frac{1}{n}\right)^n < e$

$$\text{PAS BASE} \rightarrow P(1) = \left(\frac{1}{e}\right)^1 < 1! \quad , \quad \frac{1}{e} < 1 \quad \text{cert.}$$

PAS INDUCTIU $\rightarrow \forall n \in \mathbb{W}, n \geq 2, P(n-1) \Rightarrow P(n)$

$$\begin{aligned} P(n+1) &= \left(\frac{n+1}{e}\right)^{n+1} \\ \left(\frac{n}{e}\right)^n &= \left(\frac{n-1}{e}\right)^{n-1} \cdot \left(\frac{e}{n-1}\right)^{n-1} \cdot \left(\frac{n}{e}\right)^n = \left(\frac{n-1}{e}\right)^{n-1} \cdot \left(\frac{e}{n-1}\right)^{n-1} \cdot \left(\frac{n}{e}\right)^{n-1} \cdot \frac{n}{e} = \\ &= \left(\frac{n-1}{e}\right)^{n-1} \underbrace{\left(\frac{n}{n-1}\right)^{n-1}}_{\frac{n}{e}} < (n-1)! \frac{n}{e}, \quad e = n \cdot (n-1)! = n! \\ \left(\frac{n}{n-1}\right)^{n-1} &= \left(1 + \frac{1}{n-1}\right)^{n-1} < e \end{aligned}$$

ex 89. $A = \mathbb{Z}$

$$x R y \Leftrightarrow x, y \text{ mateix residu mòdul 4} \quad \begin{matrix} x \mid 4 \\ r \end{matrix} \quad \begin{matrix} y \mid 4 \\ r \end{matrix}$$

Reflex: $x R y \quad \forall x \in \mathbb{Z}$ ja que x mateix residu que x

Sim: $x R y \Rightarrow y R x$

Trans: $\begin{matrix} x R y \\ y R z \end{matrix} \quad \Rightarrow \quad x R z$

ex. 91. B, C conjunts, $B \subseteq C$

$$A = P(C) \quad , \quad \forall x, y \in A \quad , \quad x R y \Leftrightarrow x - B = y - B$$

Reflex: $x R x \quad \forall x \in A$ ja que $x - B = x - B$

$$\text{Sim: } x - B = y - B \Rightarrow y - B = x - B$$

$$\begin{aligned} \text{Trans: } & x - B = y - B \\ & y - B = z - B \end{aligned} \quad \left. \begin{aligned} x - B &= z - B \\ y - B &= z - B \end{aligned} \right\}$$

ex. 93 $A = \mathbb{Z}$, $x R y \Leftrightarrow x^2 - y^2 = x - y \Leftrightarrow x^2 - x = y^2 - y$

$$\text{Reflex: } \forall x, x^2 - x = x^2 - x$$

$$\text{Sim: } x^2 - x = y^2 - y \Rightarrow y^2 - y = x^2 - x$$

$$\begin{aligned} \text{Trans: } & x^2 - x = y^2 - y \\ & y^2 - y = z^2 - z \end{aligned} \quad \left. \begin{aligned} x^2 - x &= y^2 - y \\ y^2 - y &= z^2 - z \end{aligned} \right\}$$

$$\bar{0} = \{x \in \mathbb{Z} \mid x^2 - x = 0^2 - 0\} = \{0, 1\}$$

$$\bar{a} = \{x \in \mathbb{Z} \mid x^2 - x = a^2 - a\} = \{a, 1-a\}$$

RELACIONS D'EQUIVALENCIA

| conjunt A

| Relació R (reflexiva, simètrica, transitiva, equivalència)

EQUIVALENCIA D'UN ELEMENT $a \in A$

$$\bar{a} = \{b \in A \mid b Ra\} \subseteq A$$

$$\{\bar{1}, \bar{2}, \bar{3}\} = \{x \in P(\mathbb{C}) \mid x - \{1, 2\} = \{1, 2, 3\} - \{1, 2\} = \{3\} = \{\{3\}, \{1, 3\}, \{2, 3\}, \{1, 2, 3\}\}$$

• CONJUNT COCIENT \rightarrow el conjunt de totes les classes

$$A/R = \{\bar{a} \mid a \in A\}$$

$$A/R = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}\}$$

ex: $A = \mathbb{R} \times (\mathbb{R} - \{0\})$

$$(x, y) R (x', y') \Leftrightarrow xy' = yx'$$

ex: $A = \mathbb{R} \times P(\{1, 2, 3\})$

$$(x, y) R (x', y') \Leftrightarrow \lfloor x \rfloor = \lfloor x' \rfloor \wedge \text{card } y = \text{card } y'$$

$$(1, 7) R (10, 70) ? \quad \text{Si: } 70 = 70$$

* EQUIVALENCIA DE "a": $\bar{a} = \{x \in A \mid x Ra\} \subseteq A$

CONJUNT QUOCIENT

$$\frac{A}{R} = \{\bar{a} \mid a \in A\} \subseteq P(A)$$



* Les classes donen una partició del conjunt A.

Definició de partició: col·lecció de subconjunts de A no buits disjunts dos a dos de tal manera que la unió de tots és el conjunt A.

- TEMA 4 : funcions (o bé aplicacions) -

CONJUNTS A i B ; $f : A \rightarrow B$

\nwarrow domini
 \downarrow codomini
 \nearrow antimatge de $f(a)$
 $a \rightarrow f(a)$
 \nwarrow la imatge de a

* cada $a \in A$ té una única imatge a B

$$(\forall a \in A \exists b \in B f(a) = b \wedge (\forall c \in B f(c) = c \rightarrow b = c))$$

ex: $f : \mathbb{R} - \{1\} \rightarrow \mathbb{R}$

$$x \rightarrow \frac{x+2}{x-1}$$

Tot relati $x \neq 1$ té una única imatge $f(x) = \frac{x+2}{x-1} \in \mathbb{R}$

ex: $f : \mathbb{Z} \rightarrow \mathbb{Z}$

$$\begin{cases} n \text{ (parell)} \rightarrow n+6 \text{ (parell)} \\ n \text{ (senar)} \rightarrow 2n+5 \text{ (senar)} \end{cases} \Rightarrow$$

ANTIIMATGE(S) DE 1: no en té
 $2n+5=1 \Leftrightarrow n=-2$ no es senar

ANTIIMATGE DE -8: -14 única antimatge
 $n+6=-8 \Leftrightarrow n=-14$ parell

Funcions iguals

$$f = g \quad \begin{cases} f : A \rightarrow B, g : A \rightarrow B \\ f(x) = g(x) \quad \forall x \in A \end{cases}$$

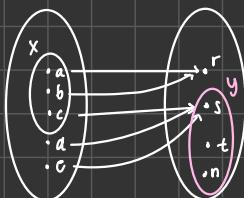
ex: $f : \mathbb{R} \rightarrow \mathbb{R}$

$$x \rightarrow x+1$$

$$g : \mathbb{R} \rightarrow \mathbb{R}, \quad x \rightarrow \frac{(x+1)(x^2+1)}{x^2+1}; \quad f = g.$$

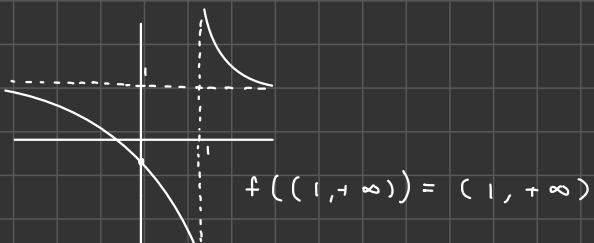
Imatge d'un circuit $x \subseteq A$ (és el conjunt de les imatges dels seus elements)

Antiimatge d'un circuit $y \subseteq B$ (és el conjunt de les antiimatges dels seus elements)



$$f(x) = \{r, s\}$$

$$f^{-1}(y) = \{c, d, e\}$$



Enunciats Aplicacions

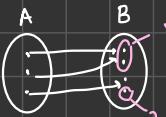
* $f : A \rightarrow B$

$x \rightarrow f(x)$ imatge única

* $f = g$

* $x \subseteq A; f(x) = \{f(x) = \{f(x)\} \mid x \in x\} \subseteq B$

* $y \subseteq B; f^{-1}(y) = \{x \in A \mid f(x) \in y\}$



$$f^{-1}(y) = \{r, s\}$$

$$f^{-1}(z) = \emptyset$$

PROBLEMA TEÓRIC

Demostra que $f^{-1}(x_1 \cap x_2) = f^{-1}(x_1) \cap f^{-1}(x_2)$

$$f : A \rightarrow B$$

$$x_1 \subseteq B, x_2 \subseteq B$$

dem: \subseteq) sigui x qualsevol

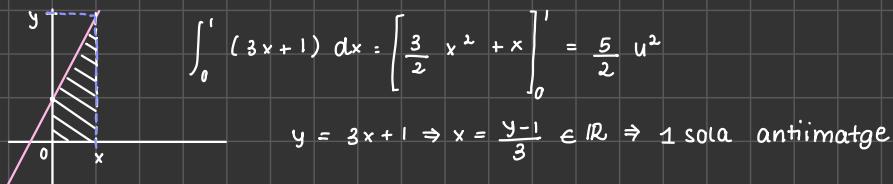
$$\begin{aligned} x \in f^{-1}(x_1 \cap x_2) &\Leftrightarrow f(x) \in x_1 \cap x_2 \Leftrightarrow f(x) \in x_1 \wedge f(x) \in x_2 \Leftrightarrow x \in f^{-1}(x_1) \wedge x \in f^{-1}(x_2) \\ &\text{Def. de } f^{-1}(N) \quad \text{Def. de } f^{-1}(N) \end{aligned}$$

$$\Leftrightarrow x \in f^{-1}(x_1) \cap f^{-1}(x_2) \quad * \text{ les fletxes són reversibles per tant c.v.a.}$$

Def. de \cap

f. injectiva d $\forall x \in B$ té 1 o 0 antíimatges a A?

ex. $f : \mathbb{R} \rightarrow \mathbb{R}$ sigui $y \in B$ qualsevol \Rightarrow cerca d'antíimatges de $y = f(x) = y$ incognita
 $x \mapsto 3x + 1$ el n° x = número d'antíimatges



ex. $g : \mathbb{Z} \rightarrow \mathbb{Z}$
 $f(x) = y \Leftrightarrow x = \frac{y-1}{3} \in \mathbb{Z}$

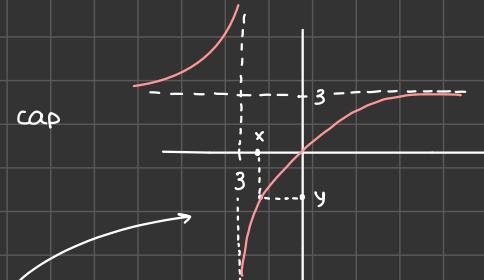
$$\begin{cases} f^{-1}(7) = 2 \\ f^{-1}(4) = 1 \end{cases}$$

En aquest cas g es injectiva perquè cada y té 1 o cap

ex. $f : \mathbb{R} - \{-3\} \rightarrow \mathbb{R}$
 $x \mapsto \frac{3x+1}{x+3}$

Sigui $y \neq 3$. $\frac{3x+1}{x+3} = y \Leftrightarrow 3x+1 = yx+3y \Leftrightarrow x = \frac{3y-1}{3-y} \in \mathbb{R}$

$\begin{cases} \text{si } y \neq 3; 1 \text{ antíimmatge} \\ \text{si } y = 3; 3x+1 = 3x+9; 1 \neq 9 \\ \text{si } x, \text{ cap imatge} \end{cases}$



simbolització injectiva

- $\forall x, x' \in A (f(x) = f(x') \rightarrow x = x')$
 - $\exists x, x' \in A (f(x) = f(x') \wedge x \neq x')$
- REGLA TAKA-TAKA*
- $$\begin{aligned} f(x) = f(x') &\rightarrow x = x' \\ \frac{3x+1}{x+3} = \frac{3x'+1}{x'+3} &\Rightarrow 3x' + 9x + x'^2 + 3 = 3x^2 + 9x' + x'^2 \\ &\Rightarrow 9x - x = 9x' - x \Rightarrow 8x = 8x' \Rightarrow x = x' \end{aligned}$$

f exhaustiva $\forall y \in B$ té 1 o més antíimatges a A.

No existeix $\exists y \in B$ sense $f(x) \neq y \forall x \in A$.

ex. $h : \mathbb{R} - \{-3\} \rightarrow \mathbb{R} - \{3\}$

$x \mapsto \frac{3x+1}{x+3} \rightarrow$ l'únic nombre que no tenia antíimatge (3) l'hem tret. Per tant és exhaustiva.

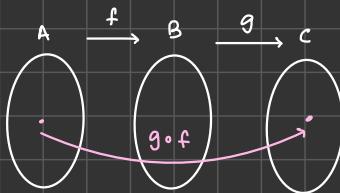
f bijectiva $\forall y \in B$ té una única antíimatge $x \in A$.

ex. $h : \mathbb{R} \rightarrow \mathbb{R}$

$x \mapsto 3x+1 ; \forall y \in B$ té una antíimatge única

4. COMPOSICIÓ DE FUNCIONS

Def : $f: A \rightarrow B$ aplicacions
 $g: B \rightarrow C$



Composició de la funció f amb la funció $g \rightarrow g \circ f$ "f composada amb g" és la aplicació $g \circ f: A \rightarrow C$, $x \rightarrow g(f(x))$

ex : $f: \mathbb{R} \rightarrow \mathbb{R}$; $g: \mathbb{R} \rightarrow \mathbb{R}$
 $x \rightarrow x^2$ $x \rightarrow \sin x$

$g \circ f: \mathbb{R} \rightarrow \mathbb{R}$

$$x \rightarrow g(f(x)) = g(x^2) = \sin x^2$$

$f \circ g: \mathbb{R} \rightarrow \mathbb{R}$

$$x \rightarrow f(g(x)) = f(\sin x) = \sin^2 x$$

ex : $f: \mathbb{N} \rightarrow \mathbb{N}$ $g: \mathbb{N} \rightarrow \mathbb{Z}$
 $n \text{ parell} \rightarrow n+1$ $n \rightarrow n^2$
 $n \text{ senar} \rightarrow 2n$

$$g \circ f: \mathbb{N} \rightarrow \mathbb{Z}$$

$$n \rightarrow g(f(n)) = \begin{cases} n \text{ parell}, g(n+1) = (n+1)^2 \\ n \text{ senar}, g(2n) = 4n^2 \end{cases}$$

$f \circ g \neq$

PROPIETATS

1. Associativa , $A \xrightarrow{f} B \xrightarrow{g} C \xrightarrow{h} D$, $h \circ (g \circ f) = (h \circ g) \circ f \Rightarrow h \circ g \circ f$

Dem : $\forall x \in A$ es té $[h \circ (g \circ f)](x) = [(h \circ g) \circ f](x)$

$$h \circ (g \circ f)(x) \Rightarrow h(g(f(x)))$$

$$(h \circ g) \circ f(x) \Rightarrow h(g(f(x)))$$

2. No commutativa

3. La composició d'injectives és injectiva

Dem : $f: A \rightarrow B$, $g: B \rightarrow C$

$$\left. \begin{array}{l} f \text{ inj.} \\ g \text{ inj.} \end{array} \right\} \Rightarrow g \circ f \text{ inj. } (g \circ f)(x) = (g \circ f)(y) \Rightarrow x = y$$

- TEMA 5: DIVISIBILITAT AMB ENTERS -

* No es pot dividir per una uetra si no saps res d'aquesta (ja que podria ser un "0",

Dibisibilitat: a es dibidible entre b , $a|b \Leftrightarrow \exists c \text{ tq } b = a \cdot c$ * En aquest tema totes les uetres pertanyen a \mathbb{Z} per tant no ho escribim.

PROPIETATS

1. $\forall a \rightarrow a = 1 a$ cvd

ex : $a|ab \rightarrow \text{dem : } ab = a \cdot b$ cvd

2. Linealitat $\frac{a|b}{a|c} \Rightarrow a| \lambda b + \mu c \quad \forall \lambda, \mu$

Dem : $a|b \Rightarrow \exists k \ b = ak \Rightarrow \lambda b = \lambda ak \quad | \quad \lambda b + \mu c = a(\lambda k + \mu)$
 $a|c \Rightarrow \exists h \ c = ah \Rightarrow \mu c = \mu ah$

Pertant $a|\lambda b + \mu c$ cvd

★ TEORIA DEL PETIT FERMAT

$$\bar{1} = \overline{a^{p-1}} \not\equiv_p \text{ p de primer}$$

$$\text{ex: } p = 13, \quad \overline{12348}^{12} = \bar{1} \not\equiv_{13}$$

5.1. MÀXIM COMÚ DIVISOR a_1, \dots, a_n

$$\text{mcd}(12, 32) = 2^2 = 4$$

$\nearrow 2^2 \cdot 3$
 $\searrow 2^5$

Definició :

- * $\text{mcd}(0, \dots, 0) = 0$
- * En cas contrari, $\text{mcd}(a_1, \dots, a_n) = d$ ($\exists a_i \neq 0$)

$$\text{ex: } \text{mcd}(12, 32)$$

$$\begin{aligned} \text{Divisors de } 12: & \pm 1, \pm 2, \pm 3, \pm 4, \pm 6, \pm 12 \\ \text{Divisors de } 32: & \pm 1, \pm 2, \pm 4, \pm 8, \pm 16, \pm 32 \end{aligned} \quad \left. \begin{array}{l} \text{mcd}(12, 32) = 4 \\ \text{mcd}(-12, 32) = 4 \end{array} \right\} \text{mcd}(12, 32) = 4$$

$$\text{mcd}(-12, 32) = 4$$

★ $a|b \wedge b|c \Rightarrow a|c$
dem: trivial.

PROPIETATS

1. mcd no depen del signe (la llista de divisors d'un numero k és la mateixa que un número -k).

2. $a|b \Rightarrow \text{mcd}(a, b) = |a|$ (tot divisor de a és divisor de b)

3. $\text{mcd}(a, 0) = |a|$

4. p primer i p no divisor de $b \Rightarrow \text{mcd}(p, b) = 1$ (o resto)

5. **TEOREMA D'EUCLIDES** $\text{mcd}(a, b) = \text{mcd}(a - mb, b)$ $\forall u$ múltiple de b el mcd es manté!

Dem: $\overbrace{\text{mcd}(a, b)}^{d_1} = \overbrace{\text{mcd}(a, b + au)}^{d_2}$ $\forall u$, volem veure $d_1 \leq d_2$ i $d_2 \leq d_1$

Procedim

$$1) \quad d_2 | a \Rightarrow d_2 | (b + au) - au \Rightarrow d_2 \leq d_1$$

$d_2 | b + au$ inequitat

2) Es fa intercanviant a i b

$$\text{ex: } \text{mcd}(12, 32) = \text{mcd}(12, \underbrace{32 \cdot 2 \cdot 12}_{8}) = \text{mcd}(8, \underbrace{12 - 8}_{4}) = 4.$$

$$\text{ex: } \text{mcd}(n, n+2) = \text{mcd}(n, n+2-n) = \text{mcd}(n, 2) \quad \left. \begin{array}{l} n \text{ parell} = 2 \\ n \text{ senar} = 1 \end{array} \right\}$$

T. EUCLIDES

$$\text{ex: } \text{mcd}(a^2-1, a^3-1) = \text{mcd}(a^2-1, a^3-1 - a(a^2-1)) =$$

$$= \text{mcd}(a-1, a^2-1 - a(a-1)) = \text{mcd}(a-1, a-1) = |a-1|$$

5.2. NOMBRES PRIMERS ENTRE SÍ

Dos nombres són primers entre si si el seu mcd = 1.

✓ $a \text{ i } b$ no tenen factors primers comuns
 (a, b) primers entre si $\Leftrightarrow (a, b) = 1$

exercici: trova tots els enters tals que $a-1 \mid a$

* calculen a

$$\begin{cases} \text{mcd}(a-1, a) = \text{mcd}(a-1, a(a-1)) = \text{mcd}(a-1, 1) = 1 \\ a-1 \mid a \end{cases} \quad \text{T.E}$$

Uanors $a-1 = \pm 1 \Rightarrow a = 0, 2$.

5.3. DIVISIÓ EUCLIDIÀNA

$$\begin{array}{c} \text{dividend} \rightarrow a \mid b \leftarrow \text{divisor} \\ \text{residu} \rightarrow r \mid q \leftarrow \text{quotient} \end{array} \quad \begin{array}{r} 22 \\ 4 \end{array} \mid \begin{array}{r} 6 \\ 3 \end{array} \quad 22 = 6 \cdot 3 + 4 \quad 0 \leq r < b$$

TEOREMA: Donats $a, b \in \mathbb{Z}$ ($b \neq 0$) existeixen $q, r \in \mathbb{Z}$ únics tq $\begin{cases} 1) a = bq + r \\ 2) 0 \leq r < |b| \end{cases}$

$$\begin{array}{r} 22 \\ 4 \end{array} \mid \begin{array}{r} -6 \\ -3 \end{array} \Rightarrow 22 = (-6) \cdot (-3) + 4 \quad 0 \leq 4 < |-6|$$

$$\begin{array}{r} -22 \\ 2 \end{array} \mid \begin{array}{r} 6 \\ -4 \end{array} \Rightarrow -22 = 6 \cdot (-4) + 2 \quad 0 \leq 2 < |6|$$

$$\begin{array}{r} -22 \\ 2 \end{array} \mid \begin{array}{r} -6 \\ 4 \end{array} \Rightarrow -22 = (-6) \cdot 4 + 2 \quad 0 \leq 2 < |-6|$$

ALGORITME D'EUCLIDES + IDENTITAT DE BÉZOUT

(1) TEOREMA DE L'IDENTITAT DE BÉZOUT: donats 2 enters qualsevol, el seu mcd és una combinació lineal no única d'ells. $\forall a, b \in \mathbb{Z} \exists \alpha, \beta \in \mathbb{Z}$ tq $d = \alpha a + \beta b$ on $d = \text{mcd}(a, b)$.

$$\text{ex: } \text{mcd}(12, 32) = 4 ; \quad 4 = \alpha \cdot 12 + \beta \cdot 32 ; \quad 4 = 3 \cdot 12 + (-1) \cdot 32 \\ 4 = (3-32t) \cdot 12 + (-1+12t) \cdot 32 \quad \forall t \in \mathbb{Z}$$

$$\text{mcd}(a, a) = |a| ; \quad |a| = \begin{cases} 1 & \text{si } a > 0 \\ -1 & \text{si } a < 0 \end{cases} + a \cdot 0 \quad * \text{ quan tenim signes negatius} \\ \text{fem manipulació de signes}$$

$$\text{mcd}(12, -32) = 4 ; \quad 4 = 12 \cdot 3 + (-32) \cdot 1$$

(2) ALGORITME D'EUCIDES (amb positius)

ex: $\frac{\text{mcd}(328, 114)}{d} = \begin{cases} \text{càcul de } d \\ \text{càcul de } \alpha, \beta \end{cases}$

$$d = \frac{\alpha \cdot 328 + \beta \cdot 114}{x \quad y}$$

x	1	0	1	-1	8
y	0	1	-2	3	-23
Q	2	1	7	7	
R	328	114	100	14	(2) -d
	100	14	2	0	

* SEMPRE HEM D'ARRIVAR A UN RESÍDU "0".

Dem: Tota seqüència d'enters positius decreixent arriva a 0.

$$0 < 2 < 14 < 100 < 114$$

* $d = \text{últim residu no nul}$

$$\begin{aligned} \text{Dem: mcd}(328, 114) &= \text{mcd}(114, 328 - 2 \cdot 114) = \\ &= \text{mcd}(100, 114 - 1 \cdot 100) = \text{mcd}(14, 100 - 7 \cdot 14) = \\ &= \text{mcd}(2, 14 - 2 \cdot 7) = 2 \end{aligned}$$

$$d = \alpha \cdot 328 + \beta \cdot 114 = 2 = x \cdot 328 + y \cdot 114 \Rightarrow 2 = 8 \cdot 328 + (-23) \cdot 114$$

$$\begin{array}{l} 1r) x \rightarrow \boxed{\alpha} \quad \boxed{\beta} \quad \boxed{\gamma} \\ 2n) y \rightarrow \boxed{\alpha} \quad \boxed{\beta} \quad \boxed{\gamma} \\ Q \rightarrow \quad \quad \quad \boxed{\gamma} \end{array} \quad \gamma = \alpha - \beta \cdot \gamma$$

* Si a i/o b negatius i demanen alg. euclides + identitat de Bézout = primer fer-ho amb $|a|$ i $|b|$ i després fer Id. de Bézout manipulant signes.

LEMA DE GAUSS, LEMA D'EUCIDES

(1) LEMA DE GAUSS:

$$\left. \begin{array}{l} \text{Si } a | b \cdot c \\ a, b \text{ primers} \end{array} \right\} \Rightarrow a | c$$

entre si $\rightarrow \text{mcd}(a, b) = 1$.

$$\text{ex: } 12 | k \cdot 7 \Rightarrow \frac{7k}{12} \in \mathbb{Z} \Rightarrow 12 | k$$

això ha de ser enter

$$\text{Dem: Id. Bézout: } \exists \alpha, \beta \in \mathbb{Z} \text{ tq } \alpha a + \beta b = 1$$

$$\begin{array}{l} (\cdot c) \Rightarrow \alpha ac + \beta bc = c \text{ uneautat} \\ a | ac \text{ (trivial)} \\ a | bc \text{ (per hipòtesi)} \end{array} \left\} \Rightarrow a | \alpha ac + \beta bc \Rightarrow a | c \text{ c.v.d.}$$

(2) LEMA D'EUCIDES

$$\left. \begin{array}{l} \text{Si } a \text{ primer} \\ a | bc \end{array} \right\} \Rightarrow a | b \vee a | c$$

$$\text{ex: } p | kh \Rightarrow \frac{kh}{p} \in \mathbb{Z} \Rightarrow p | k \text{ o } p | h$$

$$\text{Dem: } (p \text{ primer}, p | bc, p \nmid b) \Rightarrow p | c. \text{ Per disjunció conseqüent}$$

$\text{mcd}(p, b) = 1$ ja que p primer i $p \nmid b$ basta aplicar lema de gauss.

* Demostra que si $p \mid b^n$ sigui $n \geq 1$ i p primer tenim que $p \mid b$.

Dem:

$$\left. \begin{array}{l} p \text{ primer} \\ p \mid b^n \ (n \geq 1) \end{array} \right\} \Rightarrow p \mid b \quad ; \quad \left. \begin{array}{l} p \mid b \cdot b^{n-1} \\ p \text{ primer} \end{array} \right\} \Rightarrow p \mid b \text{ o } p \mid b^{n-1}$$

Si $n=1$, $p \mid b$

Si n , $p \mid b \cdot b^{n-1}$ $\left. \begin{array}{l} p \mid b \cdot b^{n-2} \dots \text{ fins a } p \mid b. \\ p \text{ primer} \end{array} \right\}$

AULA LLIURE FM (24/11/2021)

Ex 2. (exàmen 14/01/2015)

$$f: \mathbb{Z}_{80} \rightarrow \mathbb{Z}_{80} ; f(x) = \bar{2}\bar{x} + \bar{1}$$

$$A = \{\bar{1}, \bar{3}, \bar{22}, \bar{43}\} ; B = \{\bar{3}, \bar{5}\}$$

a) Calcula $f[A]$, $f^{-1}[B]$

b) f és bijectiva

c) $f[A] \cap B$

$$\rightarrow 43 \cdot 2 + 1 = \bar{87}, \bar{87} \sqcup \bar{80} = \bar{7}$$

$$f[A] = f(\bar{1}), f(\bar{3}), f(\bar{22}), f(\bar{43}) = \{\bar{3}, \bar{7}, \bar{45}\}$$

$$f^{-1}[B] = f^{-1}(\bar{3}), f^{-1}(\bar{5})$$

II NO ES POT DIVIDIR! fem ús dels numeros inversos (ex: 2^{-1})

$$* f^{-1} \rightarrow \bar{y} = \bar{2}\bar{x} + \bar{1} ; \bar{y} - \bar{1} = \bar{2}\bar{x}$$

Univers \mathbb{Z}_{80}

Aquest 2^{-1} existeix en un univers si només si $\text{mcd}(80, 2) = 1$, això realment és una identitat de Bézout ja que $\exists a^{-1}$ en \mathbb{Z}_n si $\text{mcd}(a, n) = 1 \rightarrow a \cdot a^{-1} \equiv 1 \pmod{n}$

Per tant en aquest cas no existeix f^{-1} , per conseqüència no té antimatge, per tant no és una funció bijectiva. (NO PODEMOS CALCULAR LA INVERSA DEMONTO!)

$$f[A] \cap B = \{\bar{3}, \bar{7}, \bar{45}\} \cap \{\bar{3}, \bar{5}\} = \{\bar{3}\}$$

ALGORISME D'EUCLIDES

$$\text{mcd}(77, 100) = 1 \Rightarrow \text{Id. Bézout} \Rightarrow 100\alpha + 77\beta = \text{mcd}(100, 77) = 1$$

$$\begin{array}{rccccccccc} \alpha & | & 0 & 1 & -3 & 7 & -10 & - & \\ \beta & 0 & | & -1 & 4 & -9 & 13 & - & \\ Q & - & | & 3 & 2 & 1 & 7 & - & \\ R & 100 & 77 & 23 & 8 & 7 & 1 & 0 & \end{array} \quad 1 = 100(-10) + 77(13)$$

ex: com calcular $\bar{11}^{-320}$ en \mathbb{Z}_{53} ; $\mathbb{Z}_{53} \quad \bar{11}^{52} = \bar{1}$

Teorema del petit fermat $\bar{a}^{p-1} = \bar{1}$

$$320 \sqcup 52 \rightarrow c=6, R=8 \Rightarrow 320 = 6 \cdot 52 + 8$$

$$\bar{11}^{320} = \bar{11}^{6 \cdot 52 + 8} = (\bar{11}^{52})^6 \cdot \bar{11}^8 = \bar{11}^8$$

ex: com calcular $\overline{1}^{32} - \overline{1}$ en \mathbb{Z}_{53}

* Descomponem el 32 en binari

$$\overline{1}^{32} \rightarrow 32 \rightarrow 100000 \quad \downarrow b_0 = 11$$

$$b_0 = 11; b_1 = (11)^2 = 121 \bmod 53 = \overline{15}; b_2 = (15)^2 = 225 \bmod 53 = \overline{13};$$

$$b_3 = (13)^2 = \overline{10}; b_4 = (10)^2 = \overline{47}, b_5 = (47)^2 = 36.$$

$$\overline{1}^{32} - \overline{1} = \overline{36} - \overline{1} = \overline{35}$$

EQUACIONS DIAFÀNTICA

$$2005x + 1015y = 15$$

* Aquestes incògnites tenen solució si $\text{mcd}(2005, 1015) \mid 15$; $\text{mcd}(2005, 1015) = 5 \mid 15$,
per tant podem resoldre l'equació.

* Cuidado luego hay que desimplificar

$$* \text{Id. Bézout } \Rightarrow 5 = 2005\alpha + 1015\beta \Rightarrow 1 = 401\alpha + 203\beta$$

* Algorisme d'Euclides

α	1	0	1	-1	40	-41	81	-
β	0	1	-1	2	-79	81	-160	-
Q	-	1	1	39	1	1	2	-
R	401	203	198	5	3	2	1	0

$I = 401 \cdot (81) + 203(-160)$
 \Downarrow
com que $5 \mid 15 = 3$
 $I = 2005(81 \cdot 3) + 203(-160 \cdot 3)$ solució específica
 $I = 2005(243) + 203(-480) \quad x_0 = 243, y_0 = -480$

Solució general $\begin{cases} x = 243 + 203t & \text{per una } x \geq 0 \text{ mínima} \\ y = -480 - 401t & \text{le cambias el signo a uno!} \end{cases} \quad 243 + 203t \geq 0; 203t \geq -243; t \geq -\frac{243}{203}$

DECOMPOSICIÓ EN FACTORS NUMÈRICS

* Teorema: tot enter $\lambda \geq 2$ és producte de primers de manera única)

$$n = \prod_{i=1}^k p_i^{e_i} = p_1^{e_1} \cdot p_2^{e_2} \cdots p_k^{e_k}$$

Calcul de $\text{mcd}(a, b)$ usant el teorema anterior

ex. $\text{mcd}(12, 32)$

Descompossem: $12 = 2^2 \cdot 3$, $\text{mcd}(12, 32) = 2^2 \cdot 3^0 = 2^2 = 4$
 $32 = 2^5 \cdot 3$

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

on $a = p_1^{e_1} \cdots p_k^{e_k}$ i $b = p_1^{f_1} \cdots p_k^{f_k}$ i on $e_i, f_i \geq 0$

Uavors $[\text{mcd}(a, b) = p_1^{\min\{e_1, f_1\}} \cdots p_k^{\min\{e_k, f_k\}}] \Rightarrow \text{important!}]$

$$\text{mcd}(2^2 \cdot 3^5, 7 \cdot 3^2, 2^5 \cdot 3^3 \cdot 11^2) = 2^0 \cdot 3^2 \cdot 7^0 \cdot 11^0 = 3^2$$

$$2^2 \cdot 3^5 \cdot 7^0 \cdot 11^0 \cdot 2^0 \cdot 3^2 \cdot 7^1 \cdot 11^0 \cdot 2^5 \cdot 3^3 \cdot 7^0 \cdot 11^2$$

* Si $a = p_1^{e_1} \cdots p_k^{e_k}$ i $b = p_1^{f_1} \cdots p_k^{f_k}$ on $e_i, f_i \geq 0$

$$a \mid b \Leftrightarrow e_i \leq f_i \quad \forall i$$

PROPIETATS MCD

$$\textcircled{1} \quad \begin{cases} z \mid a \\ z \mid b \end{cases} \Rightarrow z \mid \text{mcd}(a, b)$$

$$\text{mcd}(28, 36) = 4$$

→ divisors comuns : $\pm 1, \pm 2, \pm 4$

dem : $a = p_1^{e_1} \cdots p_k^{e_k}$
 $b = p_1^{f_1} \cdots p_k^{f_k}$ amb $e_i, f_i, g_i \geq 0$
 $z = p_1^{g_1} \cdots p_k^{g_k}$

$$\begin{array}{l} \rightarrow g_i = e_i \forall i \Rightarrow \text{per tant } g_i \leq \min\{e_i, f_i\} \forall i \text{ d'on } z \mid \text{mcd}(a, b) \\ \begin{cases} z \mid a \\ z \mid b \end{cases} \Rightarrow z \mid \text{mcd}(a, b) \\ \rightarrow g_i \leq f_i \end{array}$$

dem. alternativa :

Sabem que $\exists \alpha, \beta$ tq $\text{mcd}(a, b) = \alpha a + \beta b$

$$\begin{array}{l} \text{per linearitat} \\ \begin{cases} z \mid a \\ z \mid b \end{cases} \Rightarrow z \mid \alpha a + \beta b = \text{mcd}(a, b) \quad \text{c.v.d} \\ z \mid b \end{array}$$

$$\textcircled{2} \quad \text{mcd}\left(\frac{a}{d}, \frac{b}{d}\right) = 1$$

$$d = \text{mcd}(a, b) \neq 0$$

$$\text{ex: } \text{mcd}(28, 36) = 4$$

$$\text{mcd}\left(\frac{28}{4}, \frac{36}{4}\right) = \text{mcd}(7, 9) \Rightarrow \text{primers entre sí.}$$

$$\text{ex 80. Demostra que si } \begin{cases} a \mid c \\ b \mid d \end{cases} \Rightarrow \text{mcd}(a, b) \mid \text{mcd}(c, d)$$

$$\text{Dem: } \text{mcd}(a, b) = \alpha a + \beta b \quad i \quad \text{mcd}(c, d) = \gamma c + \delta d \quad \text{on } c = a \cdot r \quad i \quad d = b \cdot s$$

$$\begin{array}{l} c = p_1^{e_1} \cdots p_k^{e_k} \\ a = p_1^{f_1} \cdots p_k^{f_k} \end{array} \quad \begin{array}{l} \text{amb } e_i, f_i \geq 0 \quad \forall i \\ i \quad f_i \leq e_i \quad \forall i \end{array}$$

$$\begin{array}{l} d = p_1^{h_1} \cdots p_k^{h_k} \\ b = p_1^{g_1} \cdots p_k^{g_k} \end{array} \quad \begin{array}{l} \text{amb } g_i, h_i \geq 0 \quad \forall i \\ i \quad g_i \leq h_i \quad \forall i \\ \text{per } \min\{e_i, f_i\} \dots \min\{h_k, g_k\} \end{array}$$

$$\begin{array}{l} a \mid c \\ b \mid d \end{array} \Rightarrow \text{mcd}(a, b) \mid \text{mcd}(c, d)$$

$$\text{Basta veure que } \min\{f_i, g_i\} \leq \min\{e_i, h_i\}$$

AULA LLIURE FM (29/11/2021)

Ex 4 Examen 18/06/2018

a) Escriu els elements de \mathbb{Z}_{29} $\mathbb{Z}_{29} = \{\bar{x} \in \mathbb{Z} : \bar{0} \leq \bar{x} \leq \bar{28}\}$

b) Prova que si $\bar{x} \neq \bar{0}$, valors $\bar{x}^{-1} = \bar{x}^{28}$

Com que $\text{mcd}(\bar{x} \neq \bar{0}, \bar{29}) = 1 \exists x^{-1}$.

$$\bar{x} \cdot \bar{x}^{-1} = \bar{x}^{28} \cdot \bar{x} ; \quad \bar{1} = \bar{x}^{28} ; \quad \bar{1} = \bar{1}$$

d) Calcula $\bar{x} \in \mathbb{Z}_{29}$ tq $\bar{1715}^{-1} + \bar{1715}^{224} + \bar{x} = \bar{0}$

$$\bar{1715}^{-1} + \bar{1715}^{224} + \bar{x} = \bar{0} \equiv \bar{u}^{-1} + \bar{u}^{224} + \bar{x} = \bar{0}$$

Com que $\text{mcd}(\bar{u}, \bar{29}) = \bar{1} \exists \bar{u}^{-1}$.

$$\bar{u}^{-1} \cdot \bar{u} = \bar{1} ; \quad \bar{u} \cdot \bar{22} = \bar{1} \rightarrow \bar{u}^{-1} = \bar{22}$$

$$\bar{22} + \bar{u}^{224} + \bar{x} = \bar{0}$$

\bar{u}^{224} com que $\mathbb{Z}_{29} \rightarrow 29$ es primer sabem que $a^{28} = 1$

$$\frac{224}{28} = 8 ; \quad \bar{u}^{8 \cdot 28} = (\bar{u}^{28})^8 = \bar{1}^8 = \bar{1}$$

$$\bar{22} + \bar{1} + \bar{x} = \bar{0} ; \quad \bar{x} = -\bar{23} = \bar{6}$$

Ex 3. Examen 18/06/2018

$$ax + bx = a + b + 1$$

a) Trova tots els possibles valors de a, b si $x=7, y=8$ són solucions particulars.

b) Resol per $a = -1$.

$$7a + 8b = a + b + 1 ; \quad 6a + 7b = 1 ; \quad \text{mcd}(6, 7) = 1 \text{ per tant té solució}$$

$$\begin{array}{c|ccc} b & 1 & 0 & 1 \\ \hline a & 0 & 1 & -1 \\ & & 1 & 6 \\ \hline & 7 & 6 & 1 & 0 \end{array} \quad \begin{array}{l} b=1 \\ a=-1 \end{array} \quad \left\{ \begin{array}{l} a = -1 + 7t \\ b = 1 - 6t \end{array} \right. \quad t \in \mathbb{Z}$$

$$a = -1 ; \quad -x + by = -1 + b + 1 , \quad -x + by = b ; \quad -x + y = 1 \quad \begin{array}{l} x = t \\ y = t + 1 \end{array} \quad \left. \begin{array}{l} \exists \text{ solució} \\ \text{per } -x + y = 1 \end{array} \right.$$

Ex 2. Exàmen 09/06/2017

a) Sabem que a \mathbb{Z}_n tenim solucions $\bar{x} = \bar{7}, \bar{y} = \bar{8}$ calculeu els possibles valors de n .

$$\begin{cases} 3\bar{x} + 4\bar{y} = \bar{5} \\ 6\bar{x} + 7\bar{y} = \bar{8} \end{cases} \Rightarrow \begin{cases} 3\bar{7} + 4\bar{8} = \bar{5} \\ 6\bar{7} + 7\bar{8} = \bar{8} \end{cases} \Rightarrow \begin{cases} \bar{21} + \bar{32} = \bar{5} \\ \bar{42} + \bar{56} = \bar{8} \end{cases} \Rightarrow \begin{cases} \bar{53} = \bar{5} \\ \bar{98} = \bar{8} \end{cases} \Rightarrow \begin{cases} \bar{63} - \bar{5} = \bar{0} \\ \bar{98} - \bar{8} = \bar{0} \end{cases}$$

$$\begin{array}{ll} \bar{48} = \bar{0} & \text{mcd}(\bar{48}, \bar{90}) = \bar{6} \\ \bar{90} = \bar{0} & \end{array} ; \quad \mathbb{Z}_n \quad \left\{ \begin{array}{l} n \mid \bar{6} \\ n \mid \bar{10}, n \mid \bar{48} \end{array} \right. \quad \text{mcd}(\bar{48}, \bar{90}) = \bar{6}$$

\mathbb{Z}_6 (tmb seran solució tots aquells números que $n \mid \bar{6}$)

$\mathbb{Z}_3, \mathbb{Z}_2, \mathbb{Z}_1$.

Ex4. Exàmen 09/06/17

Calcula l'enter positiu més petit que és congruent amb $\overline{2235}^{1468}$ en \mathbb{Z}_{223} .

$$\overline{2235}^{1468} \equiv \overline{5}^{1468} \equiv \overline{5}^{222 \cdot 6 + 136} \equiv (\overline{5}^{222})^6 \cdot \overline{5}^{136} \equiv \overline{5}^{136}$$

$$\overline{5}^{136} \rightarrow 136 \text{ a binari} \quad \begin{array}{r} 1000 \\ b_7 \quad b_3 \end{array} \rightarrow 5^{136} = b_7 \cdot b_3$$

$$b_0 = 5; b_1 = 5^2 = 25; b_2 = 25^2 = 625; b_3 = 625^2 = 179^2 = 32041; b^4 = 152^2 = 23104; b^5 = 135^2 = 18225; b_6 = 162^2 = 26244; b_7 = 153^2 = 23409 = 217$$

$$\overline{5}^{136} = b_7 \cdot b_3 = 217 \cdot 152 = 32984 = \overline{203}$$

Ex4. Exàmen 09/06/2017

$$d = \text{dia que va neixer}; \quad 1 \leq d \leq 31$$

$$n = \text{número del mes}; \quad 1 \leq n \leq 12$$

$$12d + 31n = 492$$

$\text{mcd}(12, 31) = 1$ | 492 per tant té solució

$$\begin{array}{c|cccccc} n & 1 & 0 & 1 & -1 & 2 & -5 \\ \hline d & 0 & 1 & -2 & 3 & -5 & 13 \\ & 2 & 1 & 1 & 2 & 2 & \\ \hline & 3 & 1 & 2 & 7 & 5 & 2 & 1 & 0 \end{array} \quad \begin{array}{l} 31(-5) + 12(13) = 1 \quad (\cdot 492) \\ 31(-2460) + 12(6396) = 492 \end{array} \quad \begin{array}{l} d_0 = 6396 \\ m_0 = -2460 \end{array} \quad \begin{array}{l} d = 6396 - 31t \\ m = -2460 + 12t \end{array}$$

Com que $1 \leq m \leq 12$; $1 \leq -2460 + 12t \leq 12$; $1 + 2460 \leq 12t \leq 12 + 2460$;

$$2461 \leq 12t \leq 2472 \quad (\div 12); \quad 205 \frac{8}{12} \leq t \leq 206; \quad t = 206$$

★ EQUACIONS DIAFANTÍQUES

$ax + by = c \quad (a, b, c \in \mathbb{Z} \text{ i } x, y \in \mathbb{Z})$, si $\text{mcd}(a, b) | c$ té solució.

Són equacions lineals amb 2 incògnites enteres i coeficients enteros.

$$\text{ex: } 2005x + 1015y = 15$$

* Aquestes incògnites tenen solució si $\text{mcd}(2005, 1015) | 15$; $\text{mcd}(2005, 1015) = 5 | 15$, $5 | 15$ per tant podem resoldre l'equació.

* cuidado luego hay que desimplificar

$$\star \text{ Id. Bézout} \Rightarrow s = 2005\alpha + 1015\beta \Rightarrow 1 = 401\alpha + 203\beta$$

* Algorisme d'Eucides

$$\begin{array}{r} \alpha & 1 & 0 & 1 & -1 & 40 & -41 & 81 & - \\ \beta & 0 & 1 & -1 & 2 & -79 & 81 & -160 & - \\ Q & - & 1 & 1 & 39 & 1 & 1 & 2 & - \\ R & 401 & 203 & 198 & 5 & 3 & 2 & 1 & 0 \end{array}$$

$$1 = 401 \cdot (81) + 203(-160)$$

com que $5 | 15 = 3$

$$5 = 2005(81 \cdot 3) + 203(-160 \cdot 3) \quad \text{solució específica}$$

$$5 = 2005(243) + 203(-480) \quad x_0 = 243, y_0 = -480$$

$$\text{Solució general } \begin{cases} x = 243 + 203t \text{ per una } x \geq 0 \text{ mínima} \\ y = -480 - 401t \end{cases} \quad \begin{array}{l} 243 + 203t \geq 0, \quad 203t \geq -243; \\ t \geq -\frac{243}{203} \end{array}$$

le cambias el signo a uno!!

PROCEDIMENT GENÈRIC

1. $ax + by = c$; $\overbrace{mcd(a,b)}^d \mid c$; $\frac{ax}{d} + \frac{by}{d} = \frac{c}{d} \xrightarrow{k}$ simplicar
2. Id. Bezout ; $mcd(a,b) = ax + b\beta = d$
3. Multipiquem per k ; $a\alpha k + b\beta k = dk$; $\underbrace{a\alpha k}_{x_0} + \underbrace{b\beta k}_{y_0} = c$; Sol. parcial (x_0, y_0)
4. Sol. general $\begin{cases} x = x_0 + \frac{b}{d}t \\ y = y_0 - \frac{a}{d}t \end{cases} (t \in \mathbb{Z}) \rightarrow (x, y) = (x_0, y_0) + t(\frac{b}{d}, \frac{a}{d})$

AULA LLIURE 01/12/2021

Ex 2. Exàmen 14/01/2013

Sigui $a, b \in \mathbb{Z}$. Prova que si $15 \mid ab$, llavors $5 \mid a$ o $5 \mid b$.

$$\begin{array}{l} 15 \mid ab \\ 5 \mid 15 \end{array} \left. \begin{array}{l} \text{per linearitat} \\ \text{per linearitat} \end{array} \right\} 5 \mid 15 \mid ab, 5 \mid ab$$

Lema d'Euclides $p \mid ab \rightarrow p \mid a \vee p \mid b$, per tant, $5 \mid a \vee 5 \mid b$

Ex 3. Examen 14/01/2013

$f: \mathbb{Z} \times \mathbb{Z} \rightarrow \mathbb{Z}$ definida $f(x, y) = 52x + 21y$

- 1) Comprova que $mcd(52, 21) = 1$; escribiu la Id. Bezout
- 2) Comprova que f és exhaustiva

TEOREMA D'EUCLIDES

$$mcd(52, 21) = mcd(52-21, 21) = mcd(31-21, 21) = mcd(21-10, 10) = mcd(11, 10) = 1$$

$$\text{Id. Bezout } mcd(52, 21) = 52\alpha + 21\beta$$

Algorisme d'Euclides

$$\begin{array}{r|rrrr} & 1 & 0 & 1 & -2 \\ & 0 & 1 & -2 & 5 \\ \hline & 2 & 2 & 10 & \\ \hline 52 & 21 & 10 & 1 & 0 \end{array} \quad \alpha = -2, \beta = 5; \quad mcd(52, 21) = 52(-2) + 21(5)$$

$$f(x, y) = 52x + 21y; \quad f(x, y) = z; \quad 52(-2z) + 21(5z) = z; \quad f^{-1}(z) = (-2z, 5z)$$

Ex. Prova que hi ha infinitos nombres primers.

Demostració per reducció a l'absurd

Suposem que tenim un nombre primer $Q = p_1 \cdot p_2 \cdot p_3 \dots p_n + 1$, $Q > 2$

$$\frac{Q}{p_i} < \frac{p_1 \cdot p_2 \cdot p_3}{p_i} > 2.$$

a) Quantes inverses existeixen a \mathbb{Z}_7 ? Si (del 1 al 6) i totes seran vàlides ja que \mathbb{Z}_7 es un cos i totes les inverses.

$$\mathbb{Z}_7^* = \{x : 0 \leq x \leq 6\}, \text{ mcd}(7, x) = 1 \exists \text{ la inversa.}$$

b) Resol a \mathbb{Z}_7 , ($\bar{x} = \bar{3}$, $\bar{y} = \bar{5}$) ~~A~~

$$\begin{aligned} \bar{5}x - \bar{5}y &= \bar{4} \\ \bar{3}x + \bar{2}y &= \bar{6} \end{aligned}$$

ne \mathbb{Z} definim $M_n = \{x \in \mathbb{Z} : n|x\}$

1) Sigui p, q nombres primers, prova que $M_p \cap M_q = M_{pq}$

2) Sigui p un nombre primer, proveu que $M_{p^2} \subset M_p$.

$$x \in M_p \cap M_q \Leftrightarrow x \in p|x \wedge q|x \Leftrightarrow \text{mcm}(p, q)|x \Leftrightarrow pq|x \Leftrightarrow x \in M_{pq}$$

$$x \in M_{p^2} \Rightarrow p|p^2 \Rightarrow \text{per l'inealitat transitiva } p|x \Rightarrow x \in M_{p^2} \Rightarrow x \in M_p$$

$$M_p \neq M_{p^2}$$

Com que $p \nmid p \Rightarrow p \in M_p \Rightarrow$ per tant per que $p \in M_{p^2} \Rightarrow p^2|p \Rightarrow \text{absurd! C.V.D.}$

$$f: \mathbb{Z}_7 \rightarrow \mathbb{Z}_7, f(\bar{x}) = \bar{4}\bar{x} + \bar{2}, \text{ considera } A = \{\bar{1}, \bar{2}, \bar{3}, \bar{5}\} \quad B = \{\bar{1}, \bar{6}, \bar{5}\}$$

1) Obtened $f[S]$, on $S = A - B$, $S = \{\bar{2}, \bar{3}\}$

$$f[\bar{2}] ; \quad f(\bar{2}) = \bar{10} = \bar{3}$$

$$f(\bar{3}) = \bar{14} = \bar{0}$$

2) Demostra que és bijectiva e inversa

Que una funció sigui bijectiva significa que es tant injectiva com exhaustiva, es a dir, $[f(x) = f(x') \rightarrow x = x']$ i $[\forall y \in \mathbb{Z}_7 \exists x \in \mathbb{Z}_7 \text{ tq } y = \bar{4}\bar{x} + \bar{2}]$

$$* \bar{4}\bar{x} + \bar{2} = \bar{4}\bar{x}' + \bar{2} ; \quad \bar{4}\bar{x} \cdot \bar{4}^{-1} = \bar{4}\bar{x}' \cdot \bar{4}^{-1} ; \quad \text{com que } \text{mcd}(7, 4) = 1 \exists \bar{4}^{-1}. \text{ per tant 1 = 1 C.V.D.}$$

$$* \bar{y} = \bar{4}\bar{x} + \bar{2} ; \quad \bar{4}^{-1}(\bar{y} - \bar{2}) = (\bar{4}\bar{x}) \cdot \bar{4}^{-1} ; \quad f^{-1}(\bar{y}) = \bar{2}\bar{y} - \bar{4} ; \quad \bar{2}\bar{y} - \bar{4} = \bar{x} ; \quad \bar{x} = \bar{2}\bar{y} + \bar{4}$$

$$* \text{ El } \bar{4} \text{ equival al } \bar{3} \text{ en } \mathbb{Z}_7$$

3) Calcula $f^{-1}[A \cap B]$

Demostra que $6 \mid 7^n + 5 \quad \forall n \in \mathbb{N}$, inducció, congruències, classes residus.

1) Inducció

Pass base $n=0$; $6 \mid 7^0 + 5$; $6 \mid 1+5$; $6 \mid 6$. cert.

Hipòtesi inductiva $6 \mid 7^n + 5$

Cas inductiu $6 \mid 7^{n+1} + 5$



JOHNNY DEEP!

$$7^{n+1} + 5 = 7^n \cdot 7 + 5 = 7^n \cdot (6+1) + 5 = 7^n \cdot 6 + \underbrace{7^n + 5}_{\text{HI} \rightarrow 6k} = 7^n 6 + 6k = 6(7^n + k) = 6k'$$

2) Congruències

3) Per classes

$$\mathbb{Z}_6; \quad \overline{7}^n + \overline{5} = \overline{0} \equiv \overline{7}^n + \overline{5} = \overline{0} \equiv \overline{7} + \overline{5} = \overline{0} \equiv \overline{1} - \overline{1} = \overline{0} \equiv \overline{0} = \overline{0} \text{ cvd}$$

PROPIETATS mcm

Definició:

- si algun dels números és 0 el mcm = 0.
- si tots són $\neq 0$. Mínim comú múltiple positiu, $\text{mcm}(a_1, \dots, a_n)$

Si $m = \text{mcm}(a_1, \dots, a_n)$ $\left[\begin{array}{l} m = \hat{a}_i \forall i \text{ (múltiple de totes les "a") } \\ m' = \hat{a}_i \forall i \Rightarrow m' \geq m \end{array} \right]$

1) $\text{mcm}(a, b) = |ab|$

2) mcm no depèn del signe

Càcul del mcm:

* Primer fem la descomposició factorial

$\hookrightarrow \text{mcm}(a, b)$ on $a = p_1^{e_1} \cdots p_k^{e_k}$ i $b = p_1^{f_1} \cdots p_k^{f_k}$ per tant $\text{mcm}(a, b) = p_1^{\max(e_1, f_1)} \cdots p_k^{\max(e_k, f_k)}$

* Fórmula $\text{mcd}(a, b) \cdot \text{mcm}(a, b) = |a \cdot b|$

* Associativitat de mcm

* $x = \hat{a}$ i $x = \hat{b} \Leftrightarrow x = \text{mcd}(a, b)$

- TEMA 6 : CONGRUÈNCIES -

Treballarem en moduls en els enteros.

$$a \equiv b \pmod{m} \Leftrightarrow \begin{cases} 1. & \frac{a}{m} \text{ i } \frac{b}{m} \text{ són residus} \\ 2. & a - b = mt \text{ per una tal } t. \end{cases}$$

$$\text{ex: } 17 \not\equiv -19 \pmod{5} \rightarrow 17 - (-19) \not\equiv 0 \pmod{5}$$

\hookrightarrow mateix residu \pmod{m}

Relació d'equivalència $\equiv a \pmod{m}$

\rightarrow Tantes classes com residus \rightarrow conjunt cocient \mathbb{Z}_m

$$a \equiv b \pmod{m} \Leftrightarrow \frac{a}{r} \not\mid m \text{ i } \frac{b}{r} \not\mid m \Leftrightarrow a - b = rm \Leftrightarrow \exists t \text{ tq } a = b + mt$$

PROPIETATS

1. $a \equiv a' \pmod{m}$ i $b \equiv b' \pmod{m} \Rightarrow a+b \equiv a'+b' \pmod{m}$ i $ab \equiv a'b' \pmod{m}$

2. $k > 0$; $ka \equiv kb \pmod{km} \Rightarrow a \equiv b \pmod{m}$. ex: $3x \equiv 6 \pmod{9}$

$$x \equiv 2 \pmod{3} \Rightarrow \exists t \text{ tq } x = 2 + 3t$$

3. k, m primers entre si $ka \equiv kb \pmod{m} \Rightarrow a \equiv b \pmod{m}$. ex $3x \equiv 6 \pmod{7}$

$$x \equiv 2 \pmod{7} \Rightarrow \exists t \text{ tq } x = 2 + 7t$$

4. "Trenguem \equiv ": $a \equiv b \pmod{m_1} \wedge \dots \wedge a \equiv b \pmod{m_n} \Leftrightarrow a \equiv b \pmod{\text{lcm}(m_1, \dots, m_n)}$

ex: $x \equiv 2 \pmod{5} \wedge x \equiv 2 \pmod{6} \Leftrightarrow x \equiv 2 \pmod{30}$

exercici $\forall n > 0 \quad A = 15 \cdot 2^{3n+2} + 8(-9)^n = 68 \rightarrow A \equiv 0 \pmod{4}$ i $A \equiv 17 \pmod{17}$, $\text{lcm}(4, 17) = 68$.

$\exists y : \bar{A} = \frac{60 \cdot 8^n + 8(-9)^n}{60 \cdot 8^n + 8(-9)^n} = \bar{0} \cdot \bar{8}^n + \bar{0} \cdot (-\bar{9})^n = \bar{0}$

$\exists : \bar{A} = \frac{60 \cdot 8^n + 8(-9)^n}{60 \cdot 8^n + 8(-9)^n} = \bar{q} \bar{8}^n + \bar{8} (\bar{8})^n = 17 \bar{8}^n = \bar{0}$

exercici. $\exists n \in \mathbb{Z} \text{ tq } 7n+2$ és un cub

Dem: RA. suposem que $\exists n, t \in \mathbb{Z} \text{ tq } 7n+2 = t^3$

Passem a \mathbb{Z}_7 : $\bar{7}n + \bar{2} = \bar{t}^3$; $\bar{0}n + \bar{2} = \bar{t}^3$; $\bar{2} = \bar{t}^3$ absurd. cvd.

* $a \equiv b \pmod{m}$ $\begin{cases} a-b = rm \\ a \not\mid m \wedge b \not\mid m \end{cases} \quad [a \equiv b \pmod{m_1} \wedge \dots \wedge a \equiv b \pmod{m_n} \Leftrightarrow a \equiv b \pmod{\text{lcm}(m_1, \dots, m_n)}]$

* $\bar{a} = \bar{b}$ en \mathbb{Z}_m $[\bar{a} = \bar{b} \text{ a } \mathbb{Z}_{m_1}, \dots, \bar{a} = \bar{b} \text{ a } \mathbb{Z}_{m_n} \Leftrightarrow \bar{a} = \bar{b} \text{ a } \mathbb{Z}_{\text{lcm}}]$
 $\nwarrow \{a + tm_n \mid t \in \mathbb{Z}\}$

INVERSES

$\bar{a} \in \mathbb{Z}_m \Rightarrow \bar{a}^{-1} = ? \Rightarrow \bar{a} \cdot \bar{a}^{-1} = \bar{1}$

Una classe que pertany a \mathbb{Z}_m tindrà inversa si només si $\text{lcm}(m, \bar{a}) = 1$.

ex: Demostra que $\overline{m-1}^{-1} = \overline{m-1}$. Dem: $\overline{m-1} \cdot \overline{m-1} = \bar{1} \cdot \bar{1} = \bar{1}$ cvd.

ex: Demostra que $\bar{a} \in \mathbb{Z}_m$ té inversa si només si a, m primers entre si.

Dem: $\text{lcm}(a, m) = 1 \Rightarrow \exists \alpha, \beta \Rightarrow a\alpha + m\beta = 1 \Rightarrow \bar{a} \cdot \bar{\alpha} + \cancel{m\beta} = \bar{1} \Rightarrow \bar{a} \cdot \bar{\alpha} = \bar{1}$
 $\Rightarrow \bar{a}^{-1} = \bar{\alpha}$ cvd.

\nwarrow passem a \mathbb{Z}_m

- AULA LLIURE 15/12 -

ex: $f : \mathbb{Z} \rightarrow \mathbb{Z}$ exhaustiva

$g : \mathbb{Z} \rightarrow \mathbb{Z}$: $g(n) = f(n+1) - 1$ és exhaustiva?

$f(x)$ exhaustiva $\Rightarrow \exists f(x)^{-1} \forall x \in \mathbb{Z}$

$n \in \mathbb{Z}$ $g(n) = m \Rightarrow m = f(n+1) - 1 \Rightarrow m+1 = f(n+1)$ com que f és exhaustiva sabem que existeix una $i \in \mathbb{Z}$ tq $f(i) = m+1 \Rightarrow g(i-1) = f(i-1) = m+1-1 = m \Rightarrow g$ exhaustiva

ex: $f: \mathbb{N} \rightarrow \mathbb{N}$ aplicació injectiva

Prova que $g: \mathbb{N} \rightarrow \mathbb{N}$ $g(n) = 2 \cdot f(n)$ també és injectiva.

Que sigui injectiva implica $f(x) = f(x') \Rightarrow x = x'$

Que $g(n)$ sigui injectiva implica que $\exists n, n' \in \mathbb{N}$ tq $g(n) = g(n')$

$2 \cdot f(n) = 2 \cdot f(n') \Rightarrow$ com que f injectiva $f(n) = f(n') \Rightarrow 2n = 2n' \Rightarrow n = n'$ cvd.

ex: $x = \{n \in \mathbb{N} : 1 \leq n \leq 100\}$ $f: x \rightarrow x$; $f(n) = \begin{cases} 2n, & \text{si } 1 \leq n \leq 50 \\ 2(n-51)+1, & \text{si } 51 \leq n \leq 100 \end{cases}$

a) Prova que és bijectiva

Si es bijectiva serà tant exhaustiva com injectiva.

* Injectiva $f(n) = f(n') \Rightarrow n = n'$

Si $f(n)$ és parell, $f(n')$ també serà parell, $1 \leq n, n' \leq 50 \Rightarrow 2n = 2n' \Rightarrow n = n'$

Si $f(n)$ és senar, $f(n')$ també serà senar, $51 \leq n, n' \leq 100 \Rightarrow 2(n-51)+1 = 2(n'-51)+1 \Rightarrow n = n'$

* Exhaustiva $\forall y \in x, \exists n \in x$ tq $f(n) = y$

Si $f(n)$ és parell, $1 \leq n \leq 50 \Rightarrow y = 2n \Rightarrow n = \frac{y}{2} \Rightarrow f(n)^{-1} = \frac{n}{2}$

Si $f(n)$ és senar, $51 \leq n \leq 100 \Rightarrow y = 2(n-51)+1 \Rightarrow n = \frac{y-1}{2} + 51 \Rightarrow f(n)^{-1} = \frac{y-1}{2} + 51$

$$f(y)^{-1} = \begin{cases} \frac{y}{2} & \text{si } y \text{ par} \\ \frac{y-1}{2} + 51 & \text{si } y \text{ senar} \end{cases}$$

b) $f(s)^{-1}$; $s = \{n \in x \mid n \text{ senar}\}$

$$f(s)^{-1} = \left\{ \frac{y-1}{2} + 51 \mid n \in x \mid 51 \leq n \leq 100 \right\}$$

ex: Sigui $a, m \in \mathbb{Z}$ tq $\text{mcd}(a, m) = 2$ prova que $\exists x \in \mathbb{Z}$ tq $ax \equiv 2 \pmod{m}$

Id. Bezout $\Rightarrow \text{mcd}(a, m) = ax + my \Rightarrow 2 = ax + my^0 \Rightarrow$ passem a mod. m $2 = ax \Rightarrow 2 \equiv ax$

ex: $3510x + by = 52$

a) valor de b per que tingui solució

$\text{mcd}(3510, b) | 152$

Descomosem:

$$\begin{aligned} 52 &= 2^2 \cdot 13 \\ 3510 &= 2 \cdot 3^3 \cdot 5 \cdot 13 \end{aligned} \quad \left. \begin{array}{l} \text{per tant } b \text{ no pot tenir el } 3 \text{ i el } 5 \text{ en la seva descomposició} \\ \text{per tant } b \text{ ha de ser un nombre que no conté factors } 3 \text{ i } 5 \end{array} \right\}$$

Per tant $5 \nmid b \wedge 3 \nmid b$ i $b = 2k \vee b = 13k \vee b = 2k \cdot 13k$

ex: $f: \mathbb{N} \rightarrow \mathbb{N}$ $f(x) = 2x+1$, $\forall n > 1$ $f^{(n)}(x) = 2^n x + 2^n - 1$

Per base per $n=1$

$$2^1 x + 2^1 - 1 = 2x + 1 \Rightarrow 2x + 1 = 2x + 1 \text{ cert}$$

$$\text{HI} \Rightarrow f^{(n)}(x) = 2^n x + 2^n - 1$$

$$\text{Tesi} \Rightarrow f^{(n+1)}(x) = 2^{n+1} x + 2^{n+1} - 1$$

$$\begin{aligned} f^{(n+1)}(x) &= f \circ f^n = f(f^n) = f(2^n x + 2^n - 1) = 2(2^n x + 2^n - 1) + 1 = (2^{n+1} x + 2^{n+1} - 2) + 1 = \\ &= 2^{n+1} x + 2^{n+1} - 1 \Rightarrow \text{Tesi cvd} \end{aligned}$$

ex: Trova x tq $k = 12x$, $x, k \in \mathbb{Z}$ i $\frac{k}{11} \not\equiv \frac{35}{35} \Rightarrow \bar{k} = \bar{11} \not\equiv \bar{35}$, k mínima > 10000.

$$k = 12x$$

$$k = 11 + 35y \Rightarrow 12x = 11 + 35y \Rightarrow 12x - 35y = 11 \Rightarrow \text{mcd}(35, 12) = 1 \mid 11 \Rightarrow \text{té solució}$$

$$\begin{array}{r|rrrr} y & 1 & 0 & 1 & -1 \\ \hline x & 0 & 1 & -2 & 3 \\ C & 2 & 1 & 11 \\ \hline Q & 35 & 12 & 11 & \underline{-1} \\ & & & & 0 \end{array} \quad \begin{array}{l} \text{Id. Bezout } \text{mcd}(35, 11) = 1 \Rightarrow 12 \cdot 3 - 35 \cdot 1 = 1 \\ \text{Eq. Diofantica } \Rightarrow 12(3 \cdot 11) - 35(1 \cdot 11) = 11 \Rightarrow 12 \cdot 33 - 35 \cdot 11 = 11 \\ x_0 = 33 \\ y_0 = 11 \end{array} \quad \left. \begin{array}{l} \{ (x_0, y_0) = (33, 11) \\ \Rightarrow \text{solució específica} \end{array} \right.$$

$$\begin{cases} x = 33 + 35t \\ y = 11 + 12t \end{cases} \Rightarrow \text{solució general}$$

k mínima > 10000 :

$$k = 12x = 12(33 + 35t) = 396 + 420t \Rightarrow \text{Deduïm que } k = \{396 + 420t \mid t \in \mathbb{Z}\}$$

$$k > 10000 \Rightarrow 396 + 420t > 10000 \Rightarrow 420t > 9604 \Rightarrow t > \frac{9604}{420} \Rightarrow t > 22.8 \Rightarrow t \geq 23$$

ja que $t \in \mathbb{Z}$.

$$k = 396 + 420(23) = 10056.$$

SISTEMES DE CONGRUÈNCIES

Resol el sistema $\begin{cases} x \equiv 1 \pmod{10} \\ x \equiv 4 \pmod{15} \\ x \equiv 5 \pmod{6} \end{cases} \Rightarrow x = 1 + 10t = 4 + 15s \Rightarrow 10t - 15s = 3 \Rightarrow \text{mcd}(15, 10) = 5 \nmid 3 \text{ no té solució}$

$$\begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_n \pmod{m_n} \end{cases} \quad \text{Proposició: si } x_0 \text{ és 1. solució PARTICULAR. Llavors el sistema és equivalent a l'equació } x \equiv x_0 \pmod{\text{lcm}(m_1, \dots, m_n)}$$

Dem: x sol de (1) $\Rightarrow x$ sol de (2)

$$x \text{ sol de (1)} \Rightarrow \begin{cases} x \equiv a_1 \pmod{m_1} \\ \vdots \\ x \equiv a_n \pmod{m_n} \end{cases} \Rightarrow \begin{cases} x_0 \equiv a_1 \pmod{m_1} \\ x_0 \equiv a_n \pmod{m_n} \end{cases} \Rightarrow \begin{cases} x \equiv x_0 \pmod{m_1} \\ \vdots \\ x \equiv x_0 \pmod{m_n} \end{cases} \Rightarrow x \equiv x_0 \pmod{\text{lcm}(m_1, \dots, m_n)}$$

Prop. t.S: $k = m_i \forall i \Leftrightarrow k = \text{lcm}(m_i)$

$$\text{ex: } n \geq 1, x \in \mathbb{Z}, n \mid 1+x(2n+1)$$

$$\exists t \in \mathbb{Z} \text{ tq } 1+x(2n+1) = nt \overset{\mathbb{Z}_n}{\Rightarrow} \bar{1} + \bar{x} = \bar{0} \Rightarrow \bar{x} = -\bar{1} \Rightarrow x = -1 + nk \quad (k \in \mathbb{Z}) \Rightarrow n \mid 1 + (-1 + nk)(2n+1)$$

$$\Rightarrow 1 - 2n - 1 + nk(2n+1) \Rightarrow n \cdot (\dots) \text{ cvd.}$$

AULA LLIURE 22/12/2021

ex: Definim R^2

$$(x, y) R (x', y') \Leftrightarrow x = x'$$

a) Demostra la equivalència

· Reflexiva $(x, y) R (x, y) \Rightarrow x = x$

· Simétrica $(x, y) R (x', y') \Rightarrow (x', y') R (x, y)$

· Transitiva $(x, y) R (x', y') \wedge (x', y') R (x'', y'') \Rightarrow (x, y) R (x'', y'')$

b) calcula $(\overline{a}, \overline{b}) \in \mathbb{R}^2$

$$(\overline{a}, \overline{b}) = \{ (x, y) \in \mathbb{R}^2 : a = x \wedge b = y \}$$

c) conjunt cocient

$$\mathbb{R}^2 / R = \{ (\overline{a}, \overline{b}) \in \mathbb{R}^2 : (a, b) \in R \}$$

$$\text{ex: } 1 + 2^{3n-1} + 2^{3n+1} \equiv 0 \pmod{7} \quad n \geq 1$$

$$\begin{aligned} \text{Dem: } 1 + 2^{3n} \cdot 2^{-1} + 2^{3n} \cdot 2^1 &\equiv 0 \Rightarrow 1 + (2^3)^n \cdot 2^{-1} + (2^3)^n \cdot 2^1 \equiv 0 \Rightarrow 1 + 8^n \cdot 2^{-1} + 8^n \cdot 2^1 \equiv 0 \\ &\Rightarrow 1 + 1 \cdot 2^{-1} + 1 \cdot 2^1 \equiv 0 \Rightarrow \exists 2^{-1} \text{ ja que } \text{mod}(2, 7) = 1, 2^{-1} = 4 \Rightarrow 3 + 4 \equiv 0 \Rightarrow 7 \equiv 0 \Rightarrow 0 \equiv 0 \end{aligned}$$

$$\begin{aligned} \text{ex: } f: \mathbb{R} - \{0\} &\rightarrow \mathbb{R} - \{1\} & f(x) = \frac{x+5}{x} \\ g: \mathbb{R} - \{1\} &\rightarrow \mathbb{R} - \{2\} & g(x) = \frac{2-x}{x-1} \end{aligned}$$

$$\text{a) comprova que } h = g \circ f, \quad h(x) = \frac{2x+10}{5}$$

$$g(f(x)) = \frac{2\left(\frac{x+5}{x}\right)}{\left(\frac{x+5}{x}\right)-1} = \frac{\frac{2x+10}{x}}{\frac{x+5-x}{x}} = \frac{(2x+10)x}{5x} = \frac{2x+10}{5}$$

$$\text{b) } h \text{ bijectiva? } \forall y \in \mathbb{R}, \exists x \text{ s.t. } f(x) = y \wedge f(x) = f(x') \Rightarrow x = x'$$

$$h = \frac{2x+10}{5}, \quad h: \mathbb{R} - \{0\} \rightarrow \mathbb{R} - \{2\}$$

$$\text{1) injectiva: } \frac{2x+10}{5} = \frac{2x'+10}{5} \Rightarrow x = x' \text{ cvd.}$$

$$\text{2) exhaustiva: } y = \frac{2x+10}{5} \Rightarrow \frac{5y-10}{2} = x \Rightarrow h^{-1}(y) = x \text{ cvd.}$$

INTENSIVO 27/12

$$\text{ex: } a T b \Leftrightarrow a R b \wedge a S b$$

a) sigui $\bar{a}_r, \bar{a}_s, \bar{a}_t$. Demostra que $\bar{a}_t = \bar{a}_r \wedge \bar{a}_s$

$$x \in \bar{a}_t \Rightarrow x T a \Rightarrow x R b \wedge x S b \Rightarrow x \in \bar{a}_r \wedge x \in \bar{a}_s \Rightarrow x \in \bar{a}_r \cap \bar{a}_s$$

$$\text{ex: } I = (1, +\infty), \quad x S y \Leftrightarrow x+y > 2$$

a) S és una relació d'equivalència?

b) classes d'equivalència i conjunt cocient

c) Definim S a \mathbb{R} prova que no és conjunt d'equivalència

$$\text{Reflexiva } x S x \Rightarrow x+x > 2 \Rightarrow 2x > 2 \Rightarrow x > 1$$

$$\text{Simètrica } x S y \Rightarrow x+y > 2 \Rightarrow y+x > 2 \Rightarrow y S x$$

$$\text{Transitiva } x S y \wedge y S z \Rightarrow x+y > 2 \wedge y+z > 2 \Rightarrow x \in I, z \in I \quad \left\{ \begin{array}{l} x > 1 \\ z > 1 \end{array} \right. \Rightarrow x+z > 2$$

classes d'equivalència $\bar{a} = \{x \in I : x \sim a\}$

conjunt cocient $I/S = \{\bar{a}\}$

Si $S \in \mathbb{R} \Rightarrow x \sim x \Rightarrow x + x > 2 \Rightarrow 2x > 2 \Rightarrow$ contraexemple $x=0 \neq 2$ and.
no es relació d'equivalència

ex: $A = \{-3, -2, -1, 0, 1, 2, 3\}$ Defineix A: $a R b \Leftrightarrow a^2 - b^2 = b - a$

a) Relació d'equivalència

reflexiva $aRa \Rightarrow a^2 - a^2 = a - a \Rightarrow 0 = 0$

simètrica $aRb \Rightarrow a^2 - b^2 = b - a \Rightarrow b^2 - a^2 = a - b \Rightarrow bRa$

transitiva $aRb \wedge bRc \Rightarrow a^2 - b^2 = b - a \Rightarrow a^2 - c^2 = c - a \Rightarrow aRc$
 $b^2 - c^2 = c - b$