Exercicis Resolts
de
FONAMENTS MATEMÀTICS

Rafel Farré
Francesc Prats

06/09/2021

Tema 1: LÒGICA I DEMOSTRACIONS

1.1 LÒGICA

Exercici 1. *Demostreu sintàcticament les equivalències següents:*

1. $(\varphi \to \psi) \wedge (\psi \to \varphi) \equiv (\varphi \wedge \psi) \vee (\neg\varphi \wedge \neg\psi)$.
2. $\varphi \to (\psi \wedge \theta) \equiv (\varphi \to \psi) \wedge (\varphi \to \theta)$.
3. $\varphi \vee (\psi \leftrightarrow \theta) \equiv (\varphi \vee \psi) \leftrightarrow (\varphi \vee \theta)$.

Solució:

1. $(\varphi \to \psi) \wedge (\psi \to \varphi) \equiv [trad. \to] \equiv (\neg\varphi \vee \psi) \wedge (\neg\psi \vee \varphi) \equiv [distrib.] \equiv (\neg\varphi \vee \psi) \wedge \neg\psi] \vee [(\neg\varphi \vee \psi) \wedge \varphi] \equiv [distrib.\ i\ assoc.] \equiv (\neg\varphi \wedge \neg\psi) \vee (\psi \wedge \neg\psi) \vee (\neg\varphi \wedge \varphi) \vee (\psi \wedge \varphi) \equiv [complem.] \equiv (\neg\varphi \wedge \neg\psi) \vee 0 \vee 0 \vee (\psi \wedge \varphi) \equiv [neutre] \equiv (\neg\varphi \wedge \neg\psi) \vee (\psi \wedge \varphi) \equiv [commut.] \equiv (\varphi \wedge \psi) \vee (\neg\varphi \wedge \neg\psi)$.
2. $\varphi \to (\psi \wedge \theta) \equiv [trad. \to] \equiv \neg\varphi \vee (\psi \wedge \theta) \equiv [distrib.] \equiv (\neg\varphi \vee \psi) \wedge (\neg\varphi \vee \theta) \equiv [trad. \to] \equiv (\varphi \to \psi) \wedge (\varphi \to \theta)$.
3. Aquest el farem arreglant els dos costats i arribant a la mateixa expressió.
   Costat esquerra: $\varphi \vee (\psi \leftrightarrow \theta) \equiv [trad. \leftrightarrow] \equiv \varphi \vee ((\psi \to \theta) \wedge (\theta \to \psi)) \equiv [trad. \to] \equiv \varphi \vee ((\neg\psi \vee \theta) \wedge (\neg\theta \vee \psi)) \equiv [distri.\ i\ asso.] \equiv (\varphi \vee \neg\psi \vee \theta) \wedge (\varphi \vee \neg\theta \vee \psi)$.
   Costat dret: $(\varphi \vee \psi) \leftrightarrow (\varphi \vee \theta) \equiv [trad. \leftrightarrow] \equiv ((\varphi \vee \psi) \to (\varphi \vee \theta)) \wedge ((\varphi \vee \theta) \to (\varphi \vee \psi)) \equiv [trad. \to] \equiv (\neg(\varphi \vee \psi) \vee (\varphi \vee \theta)) \wedge (\neg(\varphi \vee \theta) \vee (\varphi \vee \psi)) \equiv [DeMorgan] \equiv ((\neg\varphi \wedge \neg\psi) \vee (\varphi \vee \theta)) \wedge ((\neg\varphi \wedge \neg\theta) \vee (\varphi \vee \psi)) \equiv [dist.\ i\ assoc.] \equiv ((\neg\varphi \vee \varphi \vee \theta) \wedge (\neg\psi \vee \varphi \vee \theta)) \wedge ((\neg\varphi \vee \varphi \vee \psi) \wedge (\neg\theta \vee \varphi \vee \psi)) \equiv [compl.\ i\ anul.] \equiv (1 \wedge (\neg\psi \vee \varphi \vee \theta)) \wedge (1 \wedge (\neg\theta \vee \varphi \vee \psi)) \equiv [neut.\ i\ com.] \equiv (\varphi \vee \neg\psi \vee \theta) \wedge (\varphi \vee \neg\theta \vee \psi)$. □

Exercici 2. *Demostreu les equivalències següents:*

$\forall x\,(C(x) \to \neg N(x)) \equiv \forall x\,(N(x) \to \neg C(x)) \equiv \forall x\,(\neg C(x) \vee \neg N(x))$.

Solució: D'una banda tenim: $\forall x\,(C(x) \to \neg N(x)) \equiv [trad. \to] \equiv \forall x\,(\neg C(x) \vee \neg N(x))$.

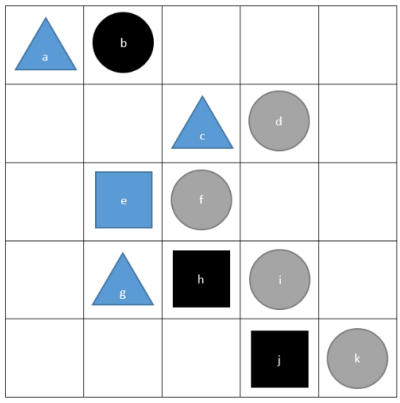
De l'altre: $\forall x\,(N(x) \to \neg C(x)) \equiv [trad. \to] \equiv \forall x\,(\neg N(x) \vee \neg C(x)) \equiv [comm.] \equiv \forall x\,(\neg C(x) \vee \neg N(x))$. □

Exercici 3. *Demostreu l'equivalència següent:*

$$\neg\exists x\exists y(x \neq y \wedge P(x) \wedge P(y)) \equiv \forall x\forall y(P(x) \wedge P(y) \rightarrow x = y)$$

Solució: $\neg\exists x\exists y(x \neq y \wedge P(x) \wedge P(y)) \equiv [neg.\ \exists] \equiv$
$\forall x\forall y\ \neg(x \neq y \wedge P(x) \wedge P(y)) \equiv [De\ Morgan\ i\ comutativa] \equiv$
$\forall x\forall y(\neg(P(x) \wedge P(y)) \vee x = y) \equiv [trad.\ \rightarrow] \equiv \forall x\forall y(P(x) \wedge P(y) \rightarrow x = y)$.
□

Exercici 4. *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*
$E(x,y)$: x *està a l'esquerra de* y
$S(x,y)$: x *està a sobre de* y

Usant els símbols indicats, formalitzeu les frases següents:

1. *Algun cercle és blau.*
2. *Tots els cercles estan a sobre de* d.
3. *Tot triangle està a l'esquerra de* a *o a sobre de* b.

Solució:

1. $\exists x(C(x) \wedge B(x))$
2. $\forall x(C(x) \rightarrow S(x,d))$
3. $\forall x(\ T(x) \rightarrow (E(x,a) \vee S(x,b))\ )$

Exercici 5. *En aquest exercici el domini és el conjunt dels enters. A més de les variables, connectives i quantificadors, podeu utilitzar només els símbols següents:* $|\ ,\ <,\ \cdot\ ,\ =,\ +,\ P,\ Q,\ 0,1,2,3,4...$

$x \mid y$ *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:

1. *Hi ha nombres senars que són primers i d'altres senars que no són primers.*
2. 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.

3. *Tot nombre parell més gran que* 2 *és suma de dos primers.*

Solució:

1. $\exists x(\ \exists y(x = 2\cdot y + 1) \wedge P(x)\ )\ \wedge\ \exists x(\ \exists y(x = 2\cdot y + 1) \wedge \neg P(x)\ )$
2. $\exists y(x = 2\cdot y)$
3. $\forall x(\ (\exists y(\ x = 2\cdot y) \wedge 2 < x) \rightarrow \exists z \exists u(P(z) \wedge P(u) \wedge x = z + u)\ )$

Exercici 6. *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:* $<,\ \cdot\ ,\ =,\ +,\ 0, 1, 2, 3, 4...$ *(Ull, ara no podem usar:* $\mid, P, Q$*). Formalitzeu:*

1. 2 *és el nombre primer més petit.*
2. Tot enter múltiple de 6 és també múltiple de 3 i de 2.
3. Cap nombre primer és un quadrat.

Solució:

1. $\forall y \forall z(2 = y\cdot z \rightarrow (y = 1 \vee y = -1 \vee z = 1 \vee z = -1)\ )$
   $\wedge\ \forall x(\ \forall y \forall z(x = y\cdot z \rightarrow (y = 1 \vee y = -1 \vee z = 1 \vee z = -1)\ )\ \rightarrow\ (x = 2 \vee x > 2)\ )$
2. $\forall x(\ \exists y(\ x = 6\cdot y)\ \rightarrow\ (\exists y(\ x = 2\cdot y) \wedge\ \exists y(\ x = 3\cdot y)\ )$
3. $\forall x(\ \forall y \forall z(x = y\cdot z \rightarrow (y = 1 \vee y = -1 \vee z = 1 \vee z = -1)\ )\ \rightarrow \neg \exists y\ (x = y\cdot y)\ )$

Exercici 7. *Sigui* $A = \{0, 1, 2, 3\}$*. Justifiqueu que són certes:*

a. $\forall x \in A\ \ x^2 \leq 3x$

b. $\forall x \in A\ (\ |x - 1| < 2\ \ \vee\ \ x^2\ -\ 9 = 0)$

Solució:

a. És evident que $0^2 \leq 0$ i $1^2 \leq 3$ i $2^2 \leq 6$ $3^2 \leq 9$.

b. És evident que $|0 - 1| < 2$, $|1 - 1| < 2$, $|2 - 1| < 2$ i $3^2\ -\ 9 = 0$. □

Exercici 8. *En aquest exercici el domini és* $\mathbb{R}$*. Justifiqueu la veritat o falsedat de:*

1. $\forall x \exists y\ (3x\ + 2y - 1 = 0)$.
2. $\exists y \forall x\ (3x\ + 2y - 1 = 0)$.

Solució:

1. És cert. Per a cada $x \in \mathbb{R}$, si prenem $y = \frac{1-3x}{2}$ es compleix $3x\ + 2y - 1 = 0$: $3x\ + 2(\frac{1-3x}{2}) - 1 = 3x\ + (1 - 3x) - 1 = 0$.
2. És fals. Si volem que $3x\ + 2y - 1 = 0$, necessàriament $y = \frac{1-3x}{2}$ i no és

és el mateix per a totes les x. També es pot fer veient que el negat és cert: $\forall y \exists x\ (3x + 2y - 1 \neq 0)$ és cert ja que si fem, per exemple, $x = \frac{-2y}{3}$ queda $3x + 2y - 1 = 3(\frac{-2y}{3}) + 2y - 1 = -2y + 2y - 1 = -1 \neq 0$. □

1.2 DEMOSTRACIONS

PROVA DIRECTA.

Exercici 9. *Demostreu que el producte de dos nombres senars és senar.*
Solució: Siguin m, n enters qualssevol:
m, n senars $\Rightarrow [def.\ senar]$ $\exists r, s \in \mathbb{Z}\ \ m = 2r + 1,\ \ n = 2s + 1$ $\Rightarrow$
$mn = (2r + 1)(2s + 1) = 4rs + 2r + 2s + 1 = 2(2rs + r + s) + 1$ $\Rightarrow [def.\ senar]$
mn és senar. □

CONTRARECÍPROC.

Exercici 10. *Demostreu que donats x, y reals, si $x + y \leq 2$ llavors $x \leq 1$* o *$y \leq 1$.*
Solució: Pel contrarecíproc, hem de veure que si $x > 1$ i $y > 1$ llavors $x + y > 2$. En efecte, $x > 1$ i $y > 1$ $\Rightarrow [Sumant]$ $x + y > 1 + 1 = 2$. □

Exercici 11. *Siguin n, m* enters. *Demostreu que si nm és parell llavors n és parell o m és parell.*
Solució: El contrarecíproc és: si n i m són senars, llavors nm és senar. I això està demostrat a l'exercici 9. □

REDUCCIÓ A L'ABSURD.

Exercici 12. *Demostreu que donats n nombres reals $a_1, \ldots, a_n$, algun d'ells ha de ser més gran o igual que la seva mitjana aritmètica $\frac{a_1 + \cdots + a_n}{n}$.*
Solució: Ho fem per reducció a l'absurd. Suposem el contrari, és a dir, que hi ha n nombres $a_1, \ldots, a_n$ tots més petits que la seva mitjana aritmètica $\frac{a_1 + \cdots + a_n}{n}$:
$a_1 < \frac{a_1 + \cdots + a_n}{n}$,

$a_2 < \frac{a_1+\cdots+a_n}{n}$,

…

$a_n < \frac{a_1+\cdots+a_n}{n}$.

Ara, sumant totes aquestes desigualtats obtenim:

$a_1 + \cdots + a_n < n \cdot \frac{a_1+\cdots+a_n}{n} = a_1 + \cdots + a_n$. Això és un contradicció. □

Exercici 13. *Demostreu que el nombre* $2\sqrt{2} - 2$ *és irracional. Useu que* $\sqrt{2}$ *és irracional.*

Solució: Ho farem per reducció a l'absurd. Suposem que $2\sqrt{2} - 2$ és racional, és a dir, que existeixen enters $a, b,$ amb b no nul, tals que $2\sqrt{2} - 2 = \frac{a}{b}$.

D'aquí resulta $\sqrt{2} = \frac{2+\frac{a}{b}}{2} = \frac{a+2b}{2b}$, que és un nombre racional i això contradiu el fet que $\sqrt{2}$ és irracional. □

Exercici 14. *Sigui* n *enter. Demostreu que si* n *és un quadrat, llavors* $n+2$ *no és un quadrat.*

Solució: Ho farem per reducció a l'absurd. Suposem que existeix un enter n que és un quadrat i que $n+2$ també és un quadrat. Així $n = r^2$ i $n+2 = s^2$ per a uns certs enters r, s que podem suposar no negatius: $r, s \geq 0$. Restant, obtenim que $2 = s^2 - r^2 = (s+r)(s-r)$. Com que 2 és un nombre primer, es tindrà: $s + r = 2, \quad s - r = 1$. Ara, sumant aquestes igualtats tenim que $2s = 3$. Això és absurd, ja que $2s$ és parell i 3 és senar. □

Exercici 15. *Demostreu que si* p *és un primer senar llavors* $log_2 p$ *és irracional.*

Solució: Per reducció a l'absurd. Suposem que $log_2 p$ és racional, és a dir, que existeixen enters a, b amb $b \neq 0$ tals que $log_2 p = \frac{a}{b}$. Com que $p > 2$, $log_2 p = \frac{a}{b} > 1$ i podem suposar que a i b són positius.

De $log_2 p = \frac{a}{b}$ resulta $2^{a/b} = p,$ i, elevant a $b,$ tenim $2^a = p^b.$ Això és un absurd, donat que 2^a és un nombre parell (ja que $a > 0$) i p^b és un nombre senar, en ser p senar. □

PROVA DE LA DISJUNCIÓ.

Exercici 16. *Donats* a, b, c *reals, demostreu que* $a \leq \frac{b+c}{2}$ *o* $b \leq \frac{a+c}{2}$ *o* $c \leq \frac{a+b}{2}$.

Solució: Demostrarem que si $a > \frac{b+c}{2}$ i $b > \frac{a+c}{2}$ llavors $c \leq \frac{a+b}{2}$. En efecte: $a > \frac{b+c}{2}$, $b > \frac{a+c}{2}$ $\Rightarrow [sumant]$ $a + b > \frac{b+c+a+c}{2}$. Multiplicant per 2 obtenim $2a + 2b > b + a + 2c$ i per tant $a + b > 2c$. D'aquí surt que $c < \frac{a+b}{2}$ i per tant $c \leq \frac{a+b}{2}$, que és el que volíem demostrar. □

DISJUNCIÓ AL CONSEQÜENT.

Exercici 17. Siguin a, b, c *enters. Demostreu que 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?*

Solució: Per demostrar $A \Rightarrow (B \text{ o } C \text{ o } D)$, farem $(A \text{ i no } B \text{ i no } C) \Rightarrow D$. En efecte: si $1 - a - 3b - 5c = 0$, $a + b + c$ és parell i $a - b - c$ és parell resulta que : $a + 3b + 5c = 1$, $a + b + c = 2r$, $a - b - c = 2s$

per a uns certs r, s enters. Sumant aquestes tres equacions tenim:

$$3a + 3b + 5c = 1 + 2r + 2s .$$

Ara, sumant $-2a - 2b - 6c$ a cada costat queda:

$$a + b - c = 1 + 2r + 2s - 2a - 2b - 6c = 1 + 2(r + s - a - b - 3c) .$$

Això demostra que $a + b - c$ és senar.

Podem afirmar que els tres són senars. Observem que $(a + b + c) - (a - b - c) = 2(b + c)$ és parell, per tant $(a + b + c)$ i $(a - b - c)$ tenen la mateixa paritat. Igualment $(a + b + c)$ i $(a + b - c)$ tenen la mateixa paritat: $(a + b + c) - (a + b - c) = 2c$. Així els tres nombres $a + b + c$, $a - b - c$, $a + b - c$ tenen la mateixa paritat. Com que algun d'ells és senar, tots tres han de ser senars.

El recíproc és fals tal com ho mostra el contraexemple següent: $a = 0$, $b = 0$, $c = 1$. □

Exercici 18. Siguin x, y, z reals. Demostreu que si $x < \frac{2y+3z}{5}$ llavors $y \geq \frac{2z+3x}{5}$ o $z \geq \frac{2x+3y}{5}$.

Solució: Per demostrar $A \Rightarrow (B \text{ o } C)$, farem $(A \text{ i no } B) \Rightarrow C$. En efecte:

$x < \frac{2y+3z}{5}$, $y < \frac{2z+3x}{5}$ $\Rightarrow [sumant]$ $x + y < \frac{2y+3z}{5} + \frac{2z+3x}{5} = \frac{3x+2y+5z}{5} =$

$\frac{3x+2y}{5} + z \quad \Rightarrow [sumant\ -\frac{3x+2y}{5}] \quad z > x + y - \frac{3x+2y}{5} = \frac{2x+3y}{5} \quad \Rightarrow [evident]$
$z \geq \frac{2x+3y}{5}$. □

DISJUNCIÓ A L'ANTECEDENT.

Exercici 19. Sigui x *enter. Demostreu 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* $4 \Leftrightarrow x = 6k + 4$ *per algun* k *enter. Idem els altres residus).*

Solució: Per demostrar que $(A\ o\ B\ o\ C) \Rightarrow D$ demostrarem tres coses: $A \Rightarrow D$, $B \Rightarrow D$, $C \Rightarrow D$.

- Si el residu de dividir x per 6 és 0 llavors $x = 6k$ per algun k enter. Elevant al quadrat, $x^2 = (6k)^2 = 6(6k^2)$ i per tant el residu de x^2 també és zero.
- Si el residu de dividir x per 6 és 3 llavors $x = 6k + 3$ per algun k enter. Elevant al quadrat, $x^2 = (6k+ 3)^2 = 36k^2 + 36k + 9 = 6(6k^2 + 6k + 1) + 3$ i per tant el residu de x^2 també és 3.
- Si el residu de dividir x per 6 és 4 llavors $x = 6k + 4$ per algun k enter. Elevant al quadrat, $x^2 = (6k+ 4)^2 = 36k^2 + 48k + 16 = 6(6k^2 + 8k + 2) + 4$ i per tant el residu de x^2 també és 4. □

PROVA PER CASOS.

Exercici 20. Sigui *n enter. El residu de la divisió de* n^2 *per 4 no és mai* 3 *(2 casos).*

Solució: Considerarem dos casos:

- n parell, és a dir, $n = 2k,$ amb k enter.
  Llavors: $n^2 = 4k,$ per tant el residu en dividir n^2 per 4 és 0.
- n senar, és a dir, $n = 2k + 1,$ amb k enter.
  Llavors: $n^2 = 4(k^2 + k) + 1$, per tant el residu en dividir n^2 per 4 és 1. □

Exercici 21. *Si* x, y, z *són nombres reals llavors:*

1. $z \leq x$ i $z \leq y \Leftrightarrow z \leq min(x, y)$ (2 casos).
2. $min(z + x, z + y) = z + min(x, y)$ *(2 casos).*

Solució: En ambdós exercicis distingim dos casos, segons $x \leq y$ o $x > y$.

1. Cas $x \leq y$. En aquest cas la part esquerra del $\Leftrightarrow$ és equivalent a $z \leq x$, ja que si $z \leq x$ i $x \leq y$ llavors $z \leq y$. Com que $min(x, y) = x$ en aquest cas, la part dreta del $\Leftrightarrow$ també és equivalent a $z \leq x$ i per tant són equivalents.
   Cas $x > y$. En aquest cas la part esquerra del $\Leftrightarrow$ és equivalent a $z \leq y$, ja que si $z \leq y$ i $y < x$ llavors $z \leq x$. Com que $min(x, y) = y$ en aquest cas, la part dreta del $\Leftrightarrow$ també és equivalent a $z \leq y$ i per tant són equivalents.
2. Cas $x \leq y$. Veurem que en aquest cas ambdós costats de la $=$ valen $z + x$. $x \leq y$ implica $min(x, y) = x$ i per tant $z + min(x, y) = z + x$. D'altra banda, $x \leq y \Rightarrow [sumant\ z]$ $z + x \leq z + y$ i per tant $min(z + x, z + y) = z + x$.
   Cas $x > y$. Veurem que en aquest cas ambdós costats de la $=$ valen $z + y$. $x > y$ implica $min(x, y) = y$ i per tant $z + min(x, y) = z + y$. D'altra banda, $x > y \Rightarrow [sumant\ z]$ $z + x > z + y$ i per tant $min(z + x, z + y) = z + y$. □

DEMOSTRACIÓ D'UNA EQUIVALÈNCIA.

Exercici 22. Sigui x *real. Són equivalents:*

1. x *irracional.*
2. $x + 1$ *irracional.*
3. $x/3$ *és irracional .*

Solució:

$1 \Rightarrow 2)$ Contrarecíproc: $x + 1$ racional $\Rightarrow$ existeixen a, b enters, b no nul, i $x + 1 = \frac{a}{b}$. Llavors $x = \frac{a}{b} - 1 = \frac{a-b}{b}$ i per tant x és racional.

$2 \Rightarrow 3)$ Contrarecíproc: $x/3$ racional $\Rightarrow$ existeixen existeixen a, b enters, b no nul, i $x/3 = \frac{a}{b}$. Llavors $x = \frac{3a}{b}$ $\Rightarrow$ $x + 1 = \frac{3a}{b} + 1 = \frac{3a+b}{b}$ i per tant $x + 1$ és racional.

$3 \Rightarrow 1)$ Contrarecíproc: x racional $\Rightarrow$ existeixen a, b enters, b no nul i $x = \frac{a}{b}$. Llavors $\frac{x}{3} = \frac{a}{3b}$ i per tant $\frac{x}{3}$ és racional. □

Exercici 23. Siguin a, b *enters. Són equivalents:*

1. $a+b, ab$ *són parells.*
2. a, b *són parells.*
3. $a+b, a+2b$ *són parells.*

Solució:

$1 \Rightarrow 2)$ ab és parell $\Rightarrow [Exercici\ 11]$ a és parell o b és parell. Si a és parell, com que $b = (a+b) - a$ és la diferència de dos parell també és parell. El cas en què b és parell es fa igual.

$2 \Rightarrow 3)$ Fem servir que la suma de dos parells és parell, fet fàcil de demostrar per prova directa.

$3 \Rightarrow 1)$ N'hi ha prou amb demostrar que ab és parell. En efecte, $a+2b$ parell $\Rightarrow$ $a = (a+2b) - 2b$ és la diferència de dos parells i per tant a és parell. Llavors $a = 2k$ per a algun k enter i per tant $ab = 2(kb)$ és parell. □

Exercici 24. Siguin a, b, c reals. Són equivalents:

1. $a > \frac{b+c}{2}$
2. $a > \frac{a+b+c}{3}$
3. $a - b > \frac{c-b}{2}$

Solució: Aquí serà més ràpid veure $1 \Leftrightarrow 2$ i $1 \Leftrightarrow 3$.

$1 \Leftrightarrow 2)$ $a > \frac{a+b+c}{3} \Leftrightarrow 3a > a+b+c \Leftrightarrow 2a > b+c \Leftrightarrow a > \frac{b+c}{2}$.

$1 \Leftrightarrow 3)$ $a - b > \frac{c-b}{2} \Leftrightarrow 2a - 2b > c - b \Leftrightarrow 2a > c + b \Leftrightarrow a > \frac{b+c}{2}$. □

DEMOSTRACIÓ DE LA UNICIAT.

Exercici 25. *Demostreu que 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.*

Solució: Hem de veure que si y, z són inversos de x llavors $y = z$. Usarem:

$y = y * u$ (u neutre)

$u = x * z$ (z és un invers de x)

$y * x = u$ (y és un invers de x)

$u * z = z$ (u neutre)

En efecte:

$$y = y * u = y * (x * z) = [assoc.] = (y * x) * z = u * z = z. \quad \square$$

Tema 2: INDUCCIÓ

Exercici 1. *Demostreu per inducció que* $\sum_{i=2}^{n} \frac{i-1}{i!} = 1 - \frac{1}{n!}$ per a tot $n \geq 2$.

Solució:

Pas base: $\sum_{i=2}^{2} \frac{i-1}{i!} = \frac{2-1}{2!} = \frac{1}{2} = 1 - \frac{1}{2!}$: cert.

Pas inductiu: Sigui $n > 2$.

- Hipòtesi d'inducció: $\sum_{i=2}^{n-1} \frac{i-1}{i!} = 1 - \frac{1}{(n-1)!}$.
- Tesi: $\sum_{i=2}^{n} \frac{i-1}{i!} = 1 - \frac{1}{n!}$.

En efecte:

$$\sum_{i=2}^{n} \frac{i-1}{i!} = \sum_{i=2}^{n-1} \frac{i-1}{i!} + \frac{n-1}{n!} = [Hip.\ ind.] = 1 - \frac{1}{(n-1)!} + \frac{n-1}{n!} = 1 - \frac{n-(n-1)}{n!} = 1 - \frac{1}{n!}. \quad \square$$

Exercici 2. *Demostreu per inducció que* $\sum_{i=1}^{n} \frac{1}{i} \leq \frac{n}{2} + 1$ si $n \geq 1$.

Solució:

Pas base: $\sum_{i=1}^{1} \frac{1}{i} = \frac{1}{1!} = 1 \leq \frac{3}{2} = \frac{1}{2} + 1$: cert.

Pas inductiu: Sigui $n > 1$.

- Hipòtesi d'inducció: $\sum_{i=1}^{n-1} \frac{1}{i} \leq \frac{n-1}{2} + 1$.
- Tesi: $\sum_{i=1}^{n} \frac{1}{i} \leq \frac{n}{2} + 1$.

En efecte:

$$\sum_{i=1}^{n} \frac{1}{i} = \sum_{i=1}^{n-1} \frac{1}{i} + \frac{1}{n} \leq [Hip.\ ind.] \leq \frac{n-1}{2} + 1 + \frac{1}{n}.$$

Si demostrem que $\frac{n-1}{2} + 1 + \frac{1}{n} \leq \frac{n}{2} + 1$ haurem acabat. Veiem-ho:

$\frac{n-1}{2} + 1 + \frac{1}{n} \leq \frac{n}{2} + 1 \iff \frac{n-1}{2} + \frac{1}{n} \leq \frac{n}{2} \iff \frac{-1}{2} + \frac{1}{n} \leq 0 \iff \frac{1}{n} \leq \frac{1}{2} \iff 2 \leq n$.

Però això últim és cert ja que $n > 1$. Per tant $\frac{n-1}{2} + 1 + \frac{1}{n} \leq \frac{n}{2} + 1$ és cert. □

Exercici 3. *Demostreu per inducció que* $2 \cdot 3^n + 5^{2n-1}$ *és múltiple de 11 per a* $n \geq 1$.

Solució:

Pas base: $2 \cdot 3^1 + 5^{2-1} = 11$, que és múltiple de 11.

Pas inductiu: Sigui $n > 1$.

- Hipòtesi d'inducció: $2 \cdot 3^{n-1} + 5^{2n-3}$ és múltiple de 11, o sigui $2 \cdot 3^{n-1} + 5^{2n-3} = 11k$, per a un cert enter k.
- Tesi: $2 \cdot 3^n + 5^{2n-1}$ és múltiple de 11 .

En efecte:

$2 \cdot 3^n + 5^{2n-1} = 2 \cdot 3^{n-1} \cdot 3 + 5^{2n-3} \cdot 25 = [truc] = 3 \cdot [2 \cdot 3^{n-1} + 5^{2n-3}] + 5^{2n-3} \cdot 22 =$

$[Hip.\ ind.] = 3 \cdot 11k + 5^{2n-3} \cdot 22 = 11 \cdot [3k + 2 \cdot 5^{2n-3}]$, que és múltiple de 11. □

Exercici 4. *Definim una successió recurrent mitjançant* $a_0 = 1$, $a_n = na_{n-1} + 1$ *per a* $n > 0$. *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*).*

Solució: Hem de tenir en compte que $0! = 1$.

Pas base: $\sum_{i=0}^{0} \frac{1}{i!} = \frac{1}{0!} = 1 = \frac{a_0}{0!}$: cert.

Pas inductiu: Sigui $n > 0$.

- Hipòtesi d'inducció: $\sum_{i=0}^{n-1} \frac{1}{i!} = \frac{a_{n-1}}{(n-1)!}$.
- Tesi: $\sum_{i=0}^{n} \frac{1}{i!} = \frac{a_n}{n!}$.

En efecte:

$\sum_{i=0}^{n} \frac{1}{i!} = \sum_{i=0}^{n-1} \frac{1}{i!} + \frac{1}{n!} = [Hip.\ ind.] = \frac{a_{n-1}}{(n-1)!} + \frac{1}{n!} = \frac{na_{n-1}+1}{n!} = [def.\ a_n] = \frac{a_n}{n!}$. □

Exercici 5. *Demostreu que la suma dels angles interiors d'un polígon de* n

costats és $180(n-2)$ *per a* $n \geq 3$.

Solució:

Pas base: quan $n = 3,$ se sap que la suma dels angles d'un triangle val 180º, i es té: $180 = 180(3-2).$

Pas inductiu: Sigui $n > 3.$

- Hipòtesi d'inducció: la suma dels angles interiors d'un polígon convex de $n-1$ costats és $180(n-3).$
- Tesi: la suma dels angles interiors d'un polígon de n costats és $180(n-2).$

En efecte:

Siguin $A_1, ..., A_n$ els vèrtexs consecutius d'un polígon de n costats. Si tracem la diagonal $A_1A_3,$ obtenim un polígon de $n-1$ costats i vèrtexs consecutius $A_1, A_{3,}A_{4,}..., A_n.$ La suma dels angles interiors d'aquest polígon, per hipòtesi d'inducció, és $180(n-3).$

Només cal adonar-se ara que la suma dels angles interiors del polígon inicial és $180(n-3)+180,$ és a dir, $180(n-2).$ □

Exercici 6. *Demostreu per inducció:* $5^n \leq 27n!$ per a $n \geq 0$.

Solució: Farem 5 casos inicials: $n = 0, 1, 2, 3, 4$.

Pas base: quan $n = 0:$ $5^0 = 1 \leq 27 = 27 \cdot 0!$: cert.

quan $n = 1:$ $5^1 = 5 \leq 27 = 27 \cdot 1!$: cert.

quan $n = 2:$ $5^2 = 25 \leq 54 = 27 \cdot 2!$: cert.

quan $n = 3:$ $5^3 = 125 \leq 162 = 27 \cdot 3!$: cert.

quan $n = 4:$ $5^4 = 625 \leq 648 = 27 \cdot 4!$: cert.

Pas inductiu: Sigui $n > 4.$

- Hipòtesi d'inducció: $5^{n-1} \leq 27 \cdot (n-1)!$
- Tesi: $5^n \leq 27n!$

En efecte:

$5^n = 5^{n-1}5 \leq [Hip.\ in.] \leq 27 \cdot (n-1)! \cdot 5 \leq [n > 4] \leq 27 \cdot (n-1)! \cdot n \leq 27n!$. □

Tema 3: CONJUNTS I RELACIONS

3.1 CONJUNTS

Exercici 1. *Demostreu que:*

1. $\emptyset \subseteq A$.
2. $A \subseteq A$.
3. $A \subseteq B$ *i* $B \subseteq C$ *implica* $A \subseteq C$.

Solució:

1. $\emptyset \subseteq A$ vol dir $\forall x(x \in \emptyset \rightarrow x \in A)$, que és una proposició certa donat que $x \in \emptyset$ és fals i per tant $x \in \emptyset \rightarrow x \in A$ és cert, sigui qui sigui x. □
2. $A \subseteq A$ vol dir $\forall x(x \in A \rightarrow x \in A)$, que és una proposició certa donat que $p \rightarrow p$ és una tautologia. □

   Alternativa menys formal: si x és un element qualsevol, i $x \in A$ és cert, llavors $x \in A$ és cert. □

3. Sigui x un element qualsevol de A. Com que $A \subseteq B$, x també és de B, i com que $B \subseteq C$, x també és de C. □

Exercici 2. *Demostreu que* $A \cup (B \cup C) = (A \cup B) \cup C$.

Solució: Sigui x un element qualsevol:

$x \in A \cup (B \cup C) \Leftrightarrow [def.\cup]\ x \in A \vee x \in (B \cup C) \Leftrightarrow [def.\cup]$
$x \in A \vee (x \in B \vee x \in C) \Leftrightarrow [assoc.\vee]\ (x \in A \vee x \in B) \vee x \in C$
$\Leftrightarrow [def.\cup]\ x \in (A \cup B) \vee x \in C \Leftrightarrow [def.\cup]\ x \in (A \cup B) \cup C$. □

Exercici 3. *Demostreu que* $A \cup B \subseteq C \Leftrightarrow A \subseteq C,\ B \subseteq C$.

Solució:

$\Rightarrow$) Veiem que $A \subseteq C$ i $B \subseteq C$ usant $A \cup B \subseteq C$.

- $A \subseteq C$: Sigui x qualsevol. $x \in A \Rightarrow [si\ p\ és\ certa,\ p \vee q\ també]$ $x \in A \vee x \in B \Rightarrow [def.\cup]\ x \in A \cup B \Rightarrow [per\ hipòtesi]\ x \in C$.

- $B \subseteq C$: Sigui x qualsevol. $x \in B \Rightarrow$ [*si p és certa, p ∨ q també*] $x \in A \vee x \in B \Rightarrow$ [*def.* ∪] $x \in A \cup B \Rightarrow$ [*per hipòtesi*] $x \in C$.

⇐) Veiem que $A \cup B \subseteq C$ usant $A \subseteq C$, $B \subseteq C$:
Sigui x qualsevol. $x \in A \cup B \Rightarrow$ [*def.* ∪] $x \in A \vee x \in B$. Ara fem dos casos. En el primer, $x \in A \Rightarrow$ [*ja que* $A \subseteq C$] $x \in C$. En el segon, $x \in B \Rightarrow$ [ja que $B \subseteq C$] $x \in C$. En ambdós casos hem vist $x \in C$. □

Exercici 4. *Demostreu que* $A \cap \emptyset = \emptyset$.
Solució: Per RA (reducció a l'absurd). Si $A \cap \emptyset$ no fos buit, tindria un element x. Però $x \in A \cap \emptyset \Rightarrow$ [*def.* ∩] $x \in A \wedge x \in \emptyset \Rightarrow$ [*Si p ∧ q és certa, q també*] $x \in \emptyset$: absurd. □

Exercici 5. *Demostreu que* $A \subseteq B \Leftrightarrow A \cap B = A$.
Solució:
⇒) Veiem $A \cap B \subseteq A$ i $A \cap B \supseteq A$:
- $A \cap B \subseteq A$: Sigui x qualsevol. $x \in A \cap B \Rightarrow$ [def. ∩] $x \in A \wedge x \in B \Rightarrow x \in A$ (aquí no hem usat la hipòtesi).
- $A \subseteq A \cap B$: Sigui x qualsevol. $x \in A \Rightarrow$ [donat que $A \subseteq B$] $x \in A \wedge x \in B \Rightarrow x \in A \cap B$.

⇐) Sigui x qualsevol. $x \in A \Rightarrow$ [*per la hipòtesi*] $x \in A \cap B \Rightarrow$ [*def.* ∩] $x \in A \wedge x \in B \Rightarrow x \in B$. □

Exercici 6. *Expresseu mitjançant quantificadors i* $\in$ *el fets següents:*
1. A *i* B *són disjunts.*
2. $A \neq B$

Solució:
1. $\neg\exists x\,(x \in A \wedge x \in B)$. També: $\forall x(x \notin A \vee x \notin B)$.
2. Hem de negar $\forall x(x \in A \leftrightarrow x \in B)$. Ara bé, $\neg\forall x\,(x \in A \leftrightarrow x \in B) \equiv \exists x \neg\,(x \in A \leftrightarrow x \in B) \equiv \exists x \neg\,((x \in A \rightarrow x \in B) \wedge (x \in B \rightarrow x \in A)) \equiv \exists x(\neg\,(x \in A \rightarrow x \in B) \vee \neg\,(x \in B \rightarrow x \in A)) \equiv \exists x((x \in A \wedge x \notin B) \vee (x \in A \wedge x \notin B)) \equiv \exists x\,(x \in A \wedge x \notin B) \vee \exists x\,(x \notin A \wedge x \in B)$. □

Exercici 7. *Demostreu que* $(A - B) \cap B = \emptyset$.
Solució: Per RA. Si $(A - B) \cap B$ no fos buit, tindria un element x. Però

$x \in (A - B) \cap B \Rightarrow [def.\ \cap]\ x \in (A - B) \wedge x \in B \Rightarrow [def.\ A - B\ i\ assoc.\ \wedge]$
$x \in A \wedge x \notin B \wedge x \in B$: absurd. □

Exercici 8. *Demostreu que* $A \subseteq B \Leftrightarrow A - B = \emptyset$.

Solució:

$\Rightarrow$) Per RA (reducció a l'absurd). Si $A - B$ no fos buit, tindria un element x. Però $x \in A - B \Rightarrow [def.\ -]\ x \in A \wedge x \notin B \Rightarrow$ [per la hipòtesi] $x \in B \wedge x \notin B$: absurd.

$\Leftarrow$) Hem de veure que tot element de A és de B. Per RA: si existís $x \in A\ i\ x \notin B$ tindríem, per def. de $A - B$, que $x \in A - B$: contradicció amb la hipòtesi $A - B = \emptyset$. □

Exercici 9. *Demostreu que* $A \cup B = A \cap B$ *sii* $A = B$.

Solució:

$\Rightarrow$) Veiem $A \subseteq B$ i $A \supseteq B$:

- $A \subseteq B$: Sigui x qualsevol. $x \in A \Rightarrow [si\ p\ certa,\ p \vee q\ també]$ $x \in A \vee x \in B \Rightarrow [def.\ \cup]\ x \in A \cup B \Rightarrow [per\ la\ hipòtesi]\ x \in A \cap B \Rightarrow [def.\ \cap]$
- $A \supseteq B$: val la demo anterior intercanviant A i B.

$\Leftarrow$) Si $A = B$, llavors evidentment es té que $A \cup B = A$ *i* $A \cap B = A$. □

Exercici 10. *Raoneu si és cert o fals i demostreu-ho:*

1. $(A \cup B) - B = A$.
2. $(A \cup B) - (A \cap B) = (A - B) \cup (B - A)$.
3. *Si* $A \cup B = \emptyset$ *llavors* $A = \emptyset,\ B = \emptyset$.

Solució:

1. Fals. Contraexemple: $A = \{1\}$, $B = \{1\}$. En aquest cas queda $(A \cup B) - B = \emptyset$, $A = \{1\}$, que són clarament diferents. □
2. Cert. Demostració: Sigui x qualsevol: $x \in (A \cup B) - (A \cap B)$ $\Leftrightarrow [def.\ -]$ $x \in (A \cup B) \wedge x \notin (A \cap B)$ $\Leftrightarrow [def.\ \notin]$ $x \in (A \cup B) \wedge \neg x \in (A \cap B)$ $\Leftrightarrow [def.\ \cup,\cap]$ $(x \in A \vee x \in B) \wedge \neg(x \in A \wedge x \in B)$ $\Leftrightarrow [DeMorgan]$ $(x \in A \vee x \in B) \wedge (x \notin A \vee x \notin B)$ $\Leftrightarrow [Distrib.]$ $(x \in A \wedge x \notin A) \vee (x \in A \wedge x \notin B) \vee (x \in B \wedge x \notin A) \vee (x \in B \wedge x \notin B)$ $\Leftrightarrow [contrad.\ i\ neutre]$ $(x \in A \wedge x \notin B) \vee (x \in B \wedge x \notin A)$ $\Leftrightarrow [def.\ -]$

$x \in (A-B) \vee x \in (B-A) \Leftrightarrow [def.\cup]\ x \in (A-B) \cup (B-A)$. □

3. Cert i ho demostrem pel contrarecíproc. Si A no fos buit o B no fos buit, un d'ells tindria un element x. Si $x \in A$ llavors $x \in A \vee x \in B$ i per tant $[def.\ \cup]\ \ x \in A \cup B,$ d'on $A \cup B$ no és buit. El cas $x \in B$ es fa igual (hem usat la prova per casos). □

Exercici 11. *Demostreu que* $(A-B)-C \subseteq A-(B \cup C)$. *Val la igualtat?*

Solució: Sigui x qualsevol: $x \in (A-B)-C \Rightarrow [def.\ -]$ $x \in (A-B) \wedge x \notin C \Rightarrow [def.\ -]\ (x \in A \wedge x \notin B) \wedge x \notin C \Rightarrow [assoc.\ \wedge]$ $x \in A \wedge (x \notin B \wedge x \notin C) \Rightarrow [DeMorgan]\ x \in A \wedge \neg(x \in B \vee x \in C)$ $\Rightarrow [def.\ \cup]\ x \in A \wedge x \notin (B \cup C) \Rightarrow [def.\ -]\ x \in A-(B \cup C)$.

Val la igualtat donat que les implicacions anteriors $\Rightarrow$ són totes dobles implicacions $\Leftrightarrow$. □

Exercici 12. *Demostreu que si* $A \cap B = \emptyset$ *llavors* $A-B=A$. *Val el recíproc?*

D'aquest exercici en donarem tres solucions diferents.

Solució 1: Ho fem pel contrarecíproc. Si $A-B \neq A$ vol di que existeix un element x de A que no és de $A-B$ o existeix un element x de $A-B$ que no és de A. La segona opció no és possible ja que si $x \in (A-B)$, $x \notin A$ resulta que $x \in A, x \notin B$, $x \notin A$: impossible. Per tant hi ha un x tal que $x \in A \wedge x \notin (A-B)$. Així $x \in A \wedge \neg(x \in A \wedge x \notin B) \equiv [DeMorgan]$ $x \in A \wedge (x \notin A \vee x \in B) \equiv [Distrib.]\ (x \in A \wedge x \notin A) \vee (x \in A \wedge x \in B) \equiv$ $x \in A \wedge x \in B$. Llavors hi ha un element $x \in A \cap B$ i per tant $A \cap B \neq \emptyset$. □

El recíproc també és cert i fem la prova pel contrarecíproc:

En efecte, si $A \cap B$ és no buit, existeix un element $x \in A \cap B$. Per tant $x \in A \wedge x \in B \equiv [Distrib.]\ x \in A \wedge (x \notin A \vee x \in B) \equiv x \in A \wedge x \notin (A-B)$. Com que tenim un element x del primer conjunt i no del segon, aquests dos conjunts són diferents: $A \neq A-B$. □

Solució 2: En aquesta segona solució veurem, usant equivalències i definicions, que els enunciats $A \cap B = \emptyset$ i $A-B=A$ són equivalent. I per tant veiem que el recíproc també és cert. Començarem per el segon:

$A-B=A \Leftrightarrow [Def]\ \forall x(\ x \in (A-B) \leftrightarrow x \in A) \Leftrightarrow [Def.-]$

$\forall x(\ (\ x \in A \wedge x \notin B) \leftrightarrow x \in A\ ) \Leftrightarrow [\leftrightarrow]$

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

$\Leftrightarrow [\rightarrow, DeMor.]\ \forall x(\ (\ x \notin A \vee x \in B \vee x \in A) \wedge (x \notin A \vee (\ x \in A \wedge x \notin B)\ )\ )$

$\Leftrightarrow$ [*Distrib.*]

$\forall x(\ (x \notin A \vee x \notin B \vee x \in A) \wedge (x \notin A \vee x \in A) \wedge (x \notin A \vee x \notin B)\ )$

$\Leftrightarrow$ [$\wedge$ *taut.*] $\forall x(x \notin A \vee x \notin B)$ $\Leftrightarrow$ [*DeMorg.*] $\forall x \neg(x \in A \wedge x \in B)$

$\Leftrightarrow$ [*Def.* $\cap$] $\forall x\ \neg(x \in A \cap B)$ $\Leftrightarrow$ [$\neg\exists$] $\neg\exists x\ (x \in A \cap B)$ $\Leftrightarrow$ [*Def.*$\emptyset$] $A \cap B = \emptyset$.

Solució 3: En aquesta solució usarem el complementari i propietats del complementari vistes a teoria. Denotem per Ω un conjunt universal que conté els conjunts A i B.

$A \cap B = \emptyset \Rightarrow (A \cap B)^C = \emptyset^C \Rightarrow A^C \cup B^C = \Omega \Rightarrow A \cap (A^C \cup B^C) = A \cap \Omega = A \Rightarrow (A \cap A^C) \cup (A \cap B^C) = A \Rightarrow \emptyset \cup (A \cap B^C) = A \Rightarrow A \cap B^C = A \Rightarrow A - B = A.$ $\square$

El recíproc és cert:

$A - B = A \Rightarrow A \cap B^C = A \Rightarrow A \cap B^C \cap B = A \cap B \Rightarrow A \cap \emptyset = A \cap B \Rightarrow \emptyset = A \cap B.$ $\square$

Exercici 13. *Demostreu que* $B = A^C \Leftrightarrow A \cap B = \emptyset$, $A \cup B = \Omega$.

Solució:

$\Rightarrow$) Veiem que $A \cap B = \emptyset$ i $A \cup B = \Omega$:

- $A \cap B = \emptyset$: ho fem per RA. Si $A \cap B$ no fos buit, tindria un element x. $x \in A \cap B$ $\Rightarrow$ [*def.* $\cap$] $x \in A \wedge x \in B$ $\Rightarrow$ [*per hipòtesi*] $x \in A \wedge x \in A^C$ $\Rightarrow$ [*def.* A^C] $x \in A \wedge x \notin A$, contradicció.
- $A \cup B = \Omega$: Com que A, B son subconjunts de Ω, n'hi ha prou amb veure que $\Omega \subseteq A \cup B$, L'altre inclusió es verifica sempre. En efecte, sigui $x \in \Omega$ qualsevol. Distingim 2 casos, segons si x és element de A o no. En el primer cas, $x \in A \Rightarrow$ [si p és certa, $p \vee q$ també] $x \in A \vee x \in B \Rightarrow$ [def. $\cup$] $x \in A \cup B$. En el segon cas, $x \notin A \Rightarrow$ [ja que $x \in \Omega$] $x \in A^C \Rightarrow$ [per hipòtesi] $x \in B \Rightarrow$ [si q és certa, $p \vee q$ també] $x \in A \vee x \in B \Rightarrow$ [def. $\cup$] $x \in A \cup B$.

$\Leftarrow$) Veiem que $B \subseteq A^C$ i $A^C \subseteq B$:

- $B \subseteq A^C$: Sigui $x \in \Omega$ qualsevol. Si $x \in B$, com que $A \cap B = \emptyset$, $x \notin A$ i per tant $x \in A^C$.
- $A^C \subseteq B$: Sigui $x \in \Omega$ qualsevol. Si $x \in A^C$ llavors $x \notin A$. Com que $x \in \Omega$ i $A \cup B = \Omega$ tenim que $x \in A \cup B$ i per tant $x \in A \vee x \in B$.

Com que $x \notin A$ concloëm que $x \in B$. $\square$

Exercici 14. *Demostreu que* $B^C \subseteq A^C \Leftrightarrow A \cap B^C = \emptyset$.

Solució:

$\Rightarrow$) Si $B^C \subseteq A^C$ llavors $A \cap B^C \subseteq A \cap A^C = \emptyset$ i per tant $A \cap B^C = \emptyset$.

$\Leftarrow$) Hem de veure que $\forall x \in \Omega\,(x \in B^C \rightarrow x \in A^C)$, és a dir, $\forall x \in \Omega\,(x \notin B \rightarrow x \notin A)$. Això és equivalent a $\forall x \in \Omega\,(x \in A \rightarrow x \in B)$. Sigui $x \in \Omega$ tal que $x \in A$. Com que per hipòtesi $A \cap B^C = \emptyset$, x no pot ser element de B^C, per tant ha de ser $x \in B$. $\square$

Exercici 15. *Demostreu que* $P(A) \cup P(B) \subseteq P(A \cup B)$. *Val la igualtat?*

Solució: Sigui x qualsevol. $x \in P(A) \cup P(B) \Rightarrow [def.\ \cup]$ $x \in P(A) \vee x \in P(B) \Rightarrow [def.\ P]$ $x \subseteq A \vee x \subseteq B$. Ara fem casos:

$x \subseteq A \Rightarrow x \subseteq A \cup B$ donat que $A \subseteq A \cup B$. Per tant $x \in P(A \cup B)$.

$x \subseteq B \Rightarrow x \subseteq A \cup B$ donat que $B \subseteq A \cup B$. Per tant $x \in P(A \cup B)$.

El recíproc és fals. Un contraexemple ve donat per $A = \{1\},\ B = \{2\}$. Es té que $A \cup B \in P(A \cup B)$, però $A \cup B \notin P(A) \cup P(B)$. $\square$

Exercici 16. *Demostreu que si* $A \subseteq B$ *llavors* $P(A) \subseteq P(B)$. *Val el recíproc?*

Solució: Sigui x qualsevol. $x \in P(A) \Rightarrow [def.\ P]$ $x \subseteq A \Rightarrow [hipòt.\ i\ transit.]$ $x \subseteq B \Rightarrow [def.\ P]$ $x \in P(B)$.

El recípoc és cert i en donem dues demostracions:

Primera: $A \in P(A) \Rightarrow [hipòtesi]$ $A \in P(B) \Rightarrow [def.\ P]$ $A \subseteq B$.

Segona: Sigui x qualsevol. $x \in A \Rightarrow [def.\ \subseteq]$ $\{x\} \subseteq A \Rightarrow [def.\ P]$ $\{x\} \in P(A) \Rightarrow [hipòtesi]$ $\{x\} \in P(B) \Rightarrow [def.\ P]$ $\{x\} \subseteq B \Rightarrow [def.\ \subseteq]$ $x \in B$. $\square$

Exercici 17. *Demostreu que si* $A \cap B = \emptyset$ *llavors* $P(A) \cap P(B) = \{\emptyset\}$. *Val el recíproc?*

Solució: Veiem que $P(A) \cap P(B) \subseteq \{\emptyset\}$ i $P(A) \cap P(B) \supseteq \{\emptyset\}$.

- $P(A) \cap P(B) \subseteq \{\emptyset\}$: Sigui x qualsevol. $x \in P(A) \cap P(B) \Rightarrow [def.\ \cap]$ $x \in P(A) \wedge x \in P(B) \Rightarrow [def.\ P]$ $x \subseteq A \wedge x \subseteq B \Rightarrow x \subseteq A \cap B$ $\Rightarrow [hipòt.]$ $x \subseteq \emptyset \Rightarrow x = \emptyset \Rightarrow x \in \{\emptyset\}$.
- $P(A) \cap P(B) \supseteq \{\emptyset\}$: Només cal verificar que $\emptyset \in P(A) \cap P(B)$, és a dir $\emptyset \in P(A),\ \emptyset \in P(B)$. I això és cert ja que $\emptyset \subseteq A$ i $\emptyset \subseteq B$.

El recíproc és cert i el demostrem per contrarecíproc. Si $A \cap B \neq \emptyset$ prenem $x \in A \cap B$. Llavors $x \in A,\ x \in B$. Així $\{x\} \subseteq A,\ \{x\} \subseteq B$ i per tant $\{x\} \in P(A),\ \{x\} \in P(B)$. Així $\{x\} \in P(A) \cap P(B)$. Com que $\{x\} \neq \emptyset$, òbviament $\{x\} \notin \{\emptyset\}$. Hem trobat un element: $\{x\}$ que pertany a un d'els conjunts: $P(A) \cap P(B)$) i no a l'altre: $\{\emptyset\}$. Per tant aquests dos conjunts són diferents: $P(A) \cap P(B) \neq \{\emptyset\}$. □

Exercici 18. *Demostreu que* $A \times (B - C) = (A \times B) - (A \times C)$.

Solució: Com que els elements del producte cartesià sempre són parelles, considerem una parella (x,y) qualsevol:

$(x,y) \in (A \times B) - (A \times C) \quad \Leftrightarrow [def.\ -] \quad (x,y) \in A \times B \wedge (x,y) \notin A \times C$

$\Leftrightarrow [def.\ \times] \quad (x \in A \wedge y \in B) \wedge \neg(x \in A \wedge y \in C) \quad \Leftrightarrow [DeMorgan]$

$(x \in A \wedge y \in B) \wedge (x \notin A \vee y \notin C) \quad \Leftrightarrow [Distrib.]$

$(x \in A \wedge y \in B \wedge x \notin A) \vee (x \in A \wedge y \in B \wedge y \notin C) \quad \Leftrightarrow [p \wedge \neg p \equiv 0]$

$0 \vee (x \in A \wedge y \in B \wedge y \notin C) \quad \Leftrightarrow [0 \vee p \equiv p] \quad x \in A \wedge y \in B \wedge y \notin C$

$\Leftrightarrow [def.\ -] \quad x \in A \wedge y \in (B - C) \quad \Leftrightarrow [def.\ \times] \quad (x,y) \in A \times (B - C)$. □

Exercici 19. *Demostreu que* $(A \times A) - (B \times B) = A \times (A - B) \cup (A - B) \times A$.

Solució: Com que els elements del producte cartesià sempre són parelles, considerem una parella (x,y) qualsevol:

$(x,y) \in (A \times A) - (B \times B) \quad \Leftrightarrow [def.\ -] \quad (x,y) \in (A \times A) \wedge (x,y) \notin (B \times B)$

$\Leftrightarrow [def.\ \times] \quad (x \in A \wedge y \in A) \wedge \neg(x \in B \wedge y \in B) \quad \Leftrightarrow [DeMorgan]$

$(x \in A \wedge y \in A) \wedge (x \notin B \vee y \notin B) \quad \Leftrightarrow [Distrib.]$

$(x \in A \wedge y \in A \wedge x \notin B) \vee (x \in A \wedge y \in A \wedge y \notin B) \quad \Leftrightarrow [def.\ -]$

$(x \in (A - B) \wedge y \in A) \vee (x \in A \wedge y \in (A - B)) \quad \Leftrightarrow [def.\ \times]$

$((x,y) \in (A - B) \times A) \vee ((x,y) \in A \times (A - B)) \quad \Leftrightarrow [def.\ \cup]$

$(x,y) \in (A \times (A - B) \cup (A - B) \times A)$. □

Exercici 20. *Demostreu que si* $A \times B = (C \times D) \cup (E \times F),\ B \neq \emptyset,\ F \neq \emptyset$ *i* $D \neq \emptyset$ *llavors* $A = C \cup E$.

Solució: Demosterm $A = C \cup E$ per doble inclusió $\subseteq$ i $\supseteq$.

- $A \subseteq C \cup E$: Sigui $x \in A$ qualsevol. Com que $B \neq \emptyset$, existeix $b \in B$. LLavors $(x,b) \in A \times B$ i també doncs $(x,b) \in (C \times D) \cup (E \times F)$, és a dir, $(x,b) \in C \times D$ o $(x,b) \in E \times F$. Si $(x,b) \in C \times D$, llavors $x \in C$, i si $(x,b) \in E \times F$, llavors $x \in E$. En ambdós casos, es té $x \in C \cup E$.

- $C \cup E \subseteq A$: Sigui $x \in C \cup E$ qualsevol, és a dir, $x \in C$ o $x \in E$.
  - Suposem $x \in C$. Com que $D \neq \emptyset$, existeix $d \in D$. LLavors $(x,d) \in C \times D$ i també doncs $(x,d) \in (C \times D) \cup (E \times F)$, per tant $(x,d) \in A \times B$. D'aquí resulta $x \in A$.
  - Suposem $x \in E$. Com que $F \neq \emptyset$, existeix $f \in F$. LLavors $(x,f) \in E \times F$ i també doncs $(x,f) \in (C \times D) \cup (E \times F)$, per tant $(x,f) \in A \times B$. D'aquí resulta $x \in A$. □

3.2 RELACIONS D'EQUIVALÈNCIA

Exercici 21. *Sigui R una relació a A. Demostreu que si R és simètrica, transitiva i compleix $\forall x \in A \exists y \in A (xRy)$ llavors R és d'equivalència.*
Solució: Falta veure que R és reflexiva. Donat $x \in A$, sigui $y \in A$ tal que xRy. Per simetria yRx i per transitivitat, xRx. □

Exercici 22. *Sigui R una relació a A. Demostreu que si R és transitiva, llavors la relació S en A definida per*

$$xSy \Leftrightarrow x = y \vee (xRy \wedge yRx)$$

és d'equivalència.
Solució: Hem de veure que S és reflexiva, simètrica i transitiva.

- S és reflexiva: sigui $x \in A$ qualsevol. $x = x \Rightarrow x = x \vee (xRx \wedge xRx) \Rightarrow xSx$.
- S és simètrica: siguin $x, y \in A$ qualssevol. $xSy \Rightarrow x = y \vee (xRy \wedge yRx) \Rightarrow y = x \vee (yRx \wedge xRy) \Rightarrow ySx$.
- S és transitiva: siguin $x, y, z \in A$ qualssevol. $xSy \wedge ySz \Rightarrow [x = y \vee (xRy \wedge yRx)] \wedge [y = z \vee (yRz \wedge zRy)]$. Després d'aplicar la distributivitat, tenim 4 casos:
  1. $x = y \wedge y = z$: llavors $x = z \Rightarrow xSz$.
  2. $x = y \wedge (yRz \wedge zRy)$: $(xRz \wedge zRx) \Rightarrow xSz$.
  3. $(xRy \wedge yRx) \wedge y = z$: $(xRz \wedge zRx) \Rightarrow xSz$.
  4. $(xRy \wedge yRx) \wedge (yRz \wedge zRy)$: $xRy \wedge yRx \wedge yRz \wedge zRy$ $\Rightarrow$ [*aquí usem 2 cops R transitiva*] $xRz \wedge zRx \Rightarrow xSz$. □

Exercici 23. *Sigui R una relació a A. Demostreu que si R és reflexiva, simètrica i antisimètrica ($\forall x,y \in A(xRy \wedge yRx \rightarrow x=y)$) llavors $R = I_A$. Val el recíproc?*

Solució: Hem de veure que donats $x,y \in A$: $xRy \Leftrightarrow x=y$.

- $\Rightarrow$: Si xRy per simetria tenim yRx. Per antisimetria $x=y$.
- $\Leftarrow$: Si $x=y$, com que R és reflexiva tenim xRx i per tant xRy.

El recíproc és cert. Ja sabem que I_A és d'equivalència, i per tant reflexiva i simètrica. És antisimètrica perquè si $R = I_A$ i xRy llavors $x=y$. □

Exercici 24. *Suposem que R és una relació antisimètrica i transitiva. Definim S així:* $xSy \Leftrightarrow xRy \wedge x \neq y$.

Demostreu que S és irreflexiva ($\forall x \neg xSx$) i transitiva.

Solució:

- S és irreflexiva: sigui x qualsevol. $\neg xSx \Leftrightarrow [DeMorgan]$ $\neg xRx \vee x=x$, que és cert donat que $x=x$ és cert.
- S és transitiva: siguin x,y,z qualssevol. Si $xSy \wedge ySz$ llavors $xRy \wedge x \neq y \wedge yRz \wedge y \neq z$. Hem de veure xSz, és a dir, $xRz \wedge x \neq z$:
  - xRz: $xRy \wedge x \neq y \wedge yRz \wedge y \neq z \Rightarrow xRy \wedge yRz \Rightarrow [R\ trans.]$ xRz.
  - $x \neq z$: *Per* RA. Si fos $x=z$, tindríem $zRy \wedge yRz \Rightarrow [R\ antisim]$ $y=z$: absurd, ja que tenim $y \neq z$. □

Exercici 25. *Demostreu que si $A \subseteq \mathbb{Z}$, la relació "tenir els mateixos divisors primers" és d'equivalència a A. Calculeu el conjunt quocient quan $A = \{1,2,...,11,12\}$.*

Solució: Primer hem de veure que la relació és d'equivalència:

- Reflexiva. Donat $x \in A$, és obvi que x té els mateixos divisors primers que x.
- Simètrica. Donats $x,y \in A$, és clar que si x té els mateixos divisors primers que y llavors y té els mateixos divisors primers que x.
- Transitiva. Donats $x,y,z \in A$, és clar que si x té els mateixos divisors primers que y i y té els mateixos divisors primers que z llavors x té els mateixos divisors primers que z.

Ara $A = \{1,2,...,11,12\}$ i calculem totes les classes d'equivalència. El mètode que usem aquí consisteix a triar un element qualsevol de A i calcular l seva

classe. A continuació triem un element que no hagi sortit en cap de les classes anteriors i calculem la seva classe. Així fins a esgotar tots els elements de A.

- $\overline{1} = \{ x \in A \mid xR1 \} =$
  $\{ x \in A \mid x \text{ té els mateixos divis. prim. que } 1 \} =$
  $\{ x \in A \mid x \text{ no té cap divisor primer} \} = \{1\}$.
- $\overline{2} = \{ x \in A \mid xR2 \} =$
  $\{ x \in A \mid x \text{ té els mateixos divis. prim. que } 2 \} =$
  $\{ x \in A \mid 2 \text{ és l'únic divisor primer de } x \} = \{2, 4, 8\}$.
- $\overline{3} = \{ x \in A \mid xR3 \} =$
  $\{ x \in A \mid x \text{ té els mateixos divis. prim. que } 3 \} =$
  $\{ x \in A \mid 3 \text{ és l'únic divisor primer de } x \} = \{3, 9\}$.
- $\overline{5} = \{ x \in A \mid xR5 \} =$
  $\{ x \in A \mid x \text{ té els mateixos divis. prim. que } 5 \} =$
  $\{ x \in A \mid 5 \text{ és l'únic divisor primer de } x \} = \{5\}$.
- $\overline{6} = \{ x \in A \mid xR6 \} =$
  $\{ x \in A \mid x \text{ té els mateixos divis. prim. que } 6 \} =$
  $\{ x \in A \mid \text{els divisors primers de } x \text{ són } 2 \text{ i } 3 \} = \{6, 12\}$.
- $\overline{7} = \{ x \in A \mid xR7 \} =$
  $\{ x \in A \mid x \text{ té els mateixos divis. prim. que } 7 \} =$
  $\{ x \in A \mid 7 \text{ és l'únic divisor primer de } x \} = \{7\}$.
- $\overline{10} = \{x \in A \mid xR10\} =$
  $\{ x \in A \mid x \text{ té els mateixos divis. prim. que } 10 \} =$
  $\{ x \in A \mid \text{els divisors primers de } x \text{ són } 2 \text{ i } 5 \} = \{10\}$.
- $\overline{11} = \{x \in A \mid xR11\} =$
  $\{ x \in A \mid x \text{ té els mateixos divis. prim. que } 11 \} =$
  $\{ x \in A \mid 11 \text{ és l'únic divisor primer de } x \} = \{11\}$.

Aquestes són totes les classes, ja que tot element de A pertany a una d'elles. Finalment, el conjunt quocient és el conjunt de totes les classes:

$$A/R = \{\overline{1}, \overline{2}, \overline{3}, \overline{5}, \overline{6}, \overline{7}, \overline{10}, \overline{11}\}.$$

Exercici 26. *Si B, C són conjunts i $B \subseteq C$, al conjunt $A = P(C)$ definim la relació següent: donats $x, y \in P(C)$:*

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

Demostreu que és una relació d'equivalència. Calculeu totes les classes de R i

el conjunt quocient A/R *quan* $C = \{1,2,3,4\}$ *i* $B = \{1,2\}$.

Solució:

- Reflexiva: per a qualsevol $x \in A$, es té xRx donat que $x \cap B = x \cap B$.
- Simètrica: donats $x, y \in A$ qualssevol: $xRy \Rightarrow x \cap B = y \cap B \Rightarrow y \cap B = x \cap B \Rightarrow yRx$.
- Transitiva: donats $x, y, z \in A$ qualssevol: $xRy \wedge yRz \Rightarrow x \cap B = y \cap B \wedge y \cap B = z \cap B \Rightarrow x \cap B = z \cap B \Rightarrow xRz$.

Suposem ara $C = \{1,2,3,4\}$ i $B = \{1,2\}$. Per la mateixa definició de R, podem afirmar que hi haurà tantes classes com subconjunts té el conjunt B, és a dir, 4 classes, amb representants: $\emptyset,\ \{1\},\ \{2\},\ \{1,2\}$:

- $\overline{\emptyset} = \{ x \in A \mid xR\emptyset \} = \{ x \in A \mid x \cap B = \emptyset \cap B \} = \{ x \in A \mid x \cap B = \emptyset \} = \{ \emptyset,\ \{3\},\ \{4\},\ \{3,4\} \}$
- $\overline{\{1\}} = \{ x \in A \mid xR\{1\} \} = \{ x \in A \mid x \cap B = \{1\} \cap B \} = \{ x \in A \mid x \cap B = \{1\} \} = \{ \{1\},\ \{1,3\},\ \{1,4\},\ \{1,3,4\} \}$
- $\overline{\{2\}} = \{ x \in A \mid xR\{2\} \} = \{ x \in A \mid x \cap B = \{2\} \cap B \} = \{ x \in A \mid x \cap B = \{2\} \} = \{ \{2\},\ \{2,3\},\ \{2,4\},\ \{2,3,4\} \}$
- $\overline{\{1,2\}} = \{ x \in A \mid xR\{1,2\} \} = \{ x \in A \mid x \cap B = \{1,2\} \cap B \} = \{ x \in A \mid x \cap B = \{1,2\} \} = \{ \{1,2\},\ \{1,2,3\},\ \{1,2,4\},\ \{1,2,3,4\} \}$

Aquestes són totes les classes, ja que tot element de A pertany a una d'elles. Finalment, el conjunt quocient és el conjunt de totes les classes:

$$A/R = \{\overline{\emptyset},\ \overline{\{1\}},\ \overline{\{2\}},\ \overline{\{1,2\}}\}.$$

Exercici 27. *Si* R *és una relació d'equivalència a* A *i* $x, y, z \in A$*, demostreu (usant només les definicions de relació d'equivalència i classe) que si* $x \in \overline{z},\ y \in \overline{z}$ *llavors* $\overline{x} = \overline{y}$.

Solució: Cal veure $\overline{x} \subseteq \overline{y}$, $\overline{x} \supseteq \overline{y}$.

- $\overline{x} \subseteq \overline{y}$*: sigui* u *qualsevol. Si* $u \in \overline{x}$*, per definició* uRx*. Igualment, de* $x \in \overline{z},\ y \in \overline{z}$ *tenim que* xRz *i* yRz*. Per simetria,* zRy *i per transitivitat* xRy*. Ara, de* uRx *i* xRy *deduïm* uRy*. Per definició* $u \in \overline{y}$.
- $\overline{x} \supseteq \overline{y}$*. Es fa igual que l'anterior intercanviant els papers de* x *i* y. □

Exercici 28. *Si* R *és una relació d'equivalència a* A *i* $x, y \in A$*, demostreu (usant només les definicions de relació d'equivalència i classe) que són equivalents:*

a. xRy.

b. $x \in \overline{y}$.

c. $\overline{x} \cup \overline{y} = \overline{y}$.

Solució:

a. $\Rightarrow$ b.) evident per la mateixa definició de classe d'equivalència.

b. $\Rightarrow$ c.) veurem $\overline{x} \cup \overline{y} \subseteq \overline{y}$ i $\overline{x} \cup \overline{y} \supseteq \overline{y}$.

- $\overline{x} \cup \overline{y} \subseteq \overline{y}$*:* sigui $z \in \overline{x} \cup \overline{y}$ qualsevol. Si $z \in \overline{y}$, ja hem acabat. Si $z \in \overline{x}$, llavors zRx i, usant la hipòtesi $x \in \overline{y}$ (és a dir, xRy) i la transitivitat, tenim zRy, és a dir, $z \in \overline{y}$.
- $\overline{x} \cup \overline{y} \supseteq \overline{y}$ *:* evident, tot conjunt X està inclòs a l a unió $X \cup Y$, sigui qui sigui el conjunt Y.

c. $\Rightarrow$ a.) $xRx \Rightarrow x \in \overline{x} \Rightarrow x \in \overline{x} \cup \overline{y} \Rightarrow [\textit{per la hipòtesi}]\ x \in \overline{y} \Rightarrow xRy$. □

Exercici 29. *Sigui* $A \subseteq \mathbb{Z}$*, i* a *un enter fixat. Demostreu que la relació en el conjunt* A : $xRy \Leftrightarrow mcd(x,a) = mcd(y,a)$

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

Solució: Primer hem de veure que la relació és d'equivalència:

- Reflexiva. Donat $x \in A$, és obvi que $mcd(x,a) = mcd(x,a)$.
- Simètrica. Donats $x, y \in A$, $xRy \Rightarrow mcd(x,a) = mcd(y,a) \Rightarrow mcd(y,a) = mcd(x,a) \Rightarrow yRx$.
- Transitiva. Donats $x, y, z \in A$, $xRy,\ yRz \Rightarrow mcd(x,a) = mcd(y,a) \wedge mcd(y,a) = mcd(z,a) \Rightarrow mcd(x,a) = mcd(z,a) \Rightarrow xRz$.

Ara $a = 8$ i $A = \{1, 2, ..., 11, 12\}$. Calculem totes les classes d'equivalència. El mètode que usem aquí consisteix a triar un element qualsevol de A i calcular l seva classe. A continuació triem un element que no hagi sortit en cap de les classes anteriors i calculem la seva classe. Així fins a esgotar tots els elements de A.

- ❑ $\overline{1} = \{ x \in A \mid xR1 \} = \{ x \in A \mid mcd(x,8) = mcd(1,8) \} = \{ x \in A \mid mcd(x,8) = 1 \} = \{1, 3, 5, 7, 9, 11\}$.
- ❑ $\overline{2} = \{ x \in A \mid xR2 \} = \{ x \in A \mid mcd(x,8) = mcd(2,8) \} = \{ x \in A \mid mcd(x,8) = 2 \} = \{2, 6, 10\}$.
- ❑ $\overline{4} = \{ x \in A \mid xR4 \} = \{ x \in A \mid mcd(x,8) = mcd(4,8) \} = \{ x \in A \mid mcd(x,8) = 4 \} = \{4, 12\}$.
- ❑ $\overline{8} = \{ x \in A \mid xR8 \} = \{ x \in A \mid mcd(x,8) = mcd(8,8) \} =$

$\{ x \in A \mid mcd(x, 8) = 8 \} = \{8\}$.

Aquestes són totes les classes, ja que tot element de A pertany a una d'elles. Finalment, el conjunt quocient és el conjunt de totes les classes: $\{\overline{1}, \overline{2}, \overline{4}, \overline{8}\}$.

Exercici 30. *A $\mathbb{Z}$ definim la relació següent: donats $x, y \in \mathbb{Z}$,*

$$xRy \iff x^2 - 2y = y^2 - 2x.$$

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

Solució: veiem que $x^2 - 2y = y^2 - 2x \Leftrightarrow x^2 + 2x = y^2 + 2y$, i si escrivim $f(t) = t^2 + 2t$, tindrem $xRy \Leftrightarrow f(x) = f(y)$.

- Reflexiva: per a qualsevol enter x, es té $f(x) = f(x)$, per tant xRx.
- Simètrica: per a qualssevol enters x, y:
$$xRy \Rightarrow f(x) = f(y) \Rightarrow f(y) = f(x) \Rightarrow yRx.$$
- Transitiva: per a qualssevol enters x, y, z:
$$xRy \wedge yRz \Rightarrow f(x) = f(y) \wedge f(y) = f(z) \Rightarrow f(x) = f(z) \Rightarrow xRz.$$

Ara calculem la classe d'equivalència d'un element qualsevol $n \in \mathbb{Z}$:

$$\overline{n} = \{x \in \mathbb{Z} \mid xRn\} = \{x \in \mathbb{Z} \mid x^2 + 2x = n^2 + 2n\} =$$
$$\{x \in \mathbb{Z} \mid x^2 - n^2 + 2(x - n) = 0\} = \{x \in \mathbb{Z} \mid (x - n)(x + n + 2) = 0\} =$$
$$\{n, -n - 2\}.$$

Per tant: $\overline{0} = \{0, -2\}$, $\overline{1} = \{1, -3\}$, $\overline{2} = \{2, -4\}$, $\overline{3} = \{3, -5\}$.

Conjunt quocient: $\mathbb{Z}/R = \{\overline{n} \mid n \in \mathbb{Z}\} = \{\{n, -n - 2\} \mid n \in \mathbb{Z}\}$.

Exercici 31. *A $\mathbb{R}$ definim la relació següent: donats $x, y \in \mathbb{R}$,*

$$xRy \iff xy > 0 \vee x = y = 0.$$

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

Solució: Primer hem de veure que la relació és d'equivalència:

- Reflexiva. Donat $x \in \mathbb{R}$, hem de veure que xRx. Distingim dos casos, segons $x = 0$ o no. En el primer cas es té $x = x = 0$. En el segon, $xx = x^2 > 0$ ja que $x \neq 0$.
- Simètrica. Donats $x, y \in \mathbb{R}$, $xRy \Rightarrow xy > 0 \vee x = y = 0 \Rightarrow yx > 0 \vee y = x = 0 \Rightarrow yRx$.
- Transitiva. Donats $x, y, z \in \mathbb{R}$, si xRy i yRz distingim 4 casos:
  - $xy > 0$, $yz > 0$. Multiplicant-los tenim $xyyz > 0$. Multiplicant per

$(\frac{1}{y})^2$ (que és > 0) tenim $(\frac{1}{y})^2 xy^2 z > 0$. Així $xz > 0$ i per tant xRz .

- $xy > 0$, $y = z = 0$. Aquest cas és impossible: $y = 0 \Rightarrow xy = 0$.
- $x = y = 0$, $yz > 0$. Aquest cas és impossible: $y = 0 \Rightarrow yz = 0$.
- $x = y = 0$, $y = z = 0$. En aquest cas $x = z = 0$ i per tant xRz .

Ara calculem totes les classes d'equivalència:

- $\overline{0} = \{ x \in \mathbb{R} \mid xR0 \} = \{ x \in \mathbb{R} \mid x \cdot 0 > 0 \vee x = 0 = 0 \} = \{ x \in A \mid x = 0 \} = \{0\}$.
- $\overline{1} = \{ x \in \mathbb{R} \mid xR1 \} = \{ x \in \mathbb{R} \mid x \cdot 1 > 0 \vee x = 1 = 0 \} = \{ x \in A \mid x > 0 \}$.
- $\overline{-1} = \{ x \in \mathbb{R} \mid xR-1 \} = \{ x \in \mathbb{R} \mid x \cdot (-1) > 0 \vee x = -1 = 0 \} = \{ x \in A \mid -x > 0 \} = \{ x \in A \mid x < 0 \}$.

Aquestes són totes les classes, ja que tot element de $\mathbb{R}$ pertany a una d'elles. Finalment, el conjunt quocient és el conjunt de totes les classes: $\{\overline{0}, \overline{1}, \overline{-1}\}$.

Exercici 32. *A $\mathbb{R} \times \mathbb{R}$ considerem la relació "estar a la mateixa distància de l'origen".*

a. Proveu que R és una relació d'equivalència.
b. Dibuixeu en el pla la classe del punt $(1,0)$.
c. Dibuixeu en el pla la classe del punt (a,b).
d. Doneu el conjunt quocient.
e. Quina partició determina? Dibuixeu les classes.

Solució:

a. R és una relació d'equivalència:
   i. Reflexiva: per a tot punt $P \in \mathbb{R} \times \mathbb{R}$, es té $dist(P,(0,0)) = dist(P,(0,0))$
   ii. Simètrica: si P, Q són punts qualssevol de $\mathbb{R} \times \mathbb{R}$, es té: $dist(P,(0,0)) = dist(Q,(0,0)) \Rightarrow dist(Q,(0,0)) = dist(P,(0,0))$
   iii. Transitiva: si P, Q, S són punts qualssevol de $\mathbb{R} \times \mathbb{R}$, es té: $dist(P,(0,0)) = dist(Q,(0,0)) \wedge dist(Q,(0,0)) = dist(S,(0,0)) \Rightarrow dist(P,(0,0)) = dist(S,(0,0))$

b. $\overline{(1,0)} = \{(x,y) \in \mathbb{R} \times \mathbb{R} \mid dist((x,y),(0,0)) = dist((1,0),(0,0)) = 1\}$,
   i aquest conjunt és un cicumferència en el pla de centre $(0,0)$ i radi 1, que té per equació $x^2 + y^2 = 1$.

c. $\overline{(a,b)} = \{(x,y) \in \mathbb{R} \times \mathbb{R} \mid dist((x,y),(0,0)) = dist((a,b),(0,0)) = \sqrt{a^2 + b^2}\}$, i aquest conjunt és un cicumferència en el pla de centre $(0,0)$ i radi $\sqrt{a^2 + b^2}$, que té per equació $x^2 + y^2 = a^2 + b^2$.

d. El conjunt quocient és el conjunt format per totes les circumferències del pla centrades en l'origen i radis $r \in [0,+\infty)$.

e. El pla $\mathbb{R} \times \mathbb{R}$ queda partit en una col.lecció de circumferències concèntriques de centre $(0,0)$ i radis nombres reals creixents a partir de 0.

Exercici 33. *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.*

Solució: Primer hem de veure que la relació és d'equivalència:

- Reflexiva. Donat $x \in \mathbb{Z} - \{0\}$, hem de veure que xRx. Òbviament x té el mateix signe i mateixa paritat que x.
- Simètrica. Donats $x, y \in \mathbb{Z} - \{0\}$, $xRy \Rightarrow x$ té el mateix signe i la mateixa paritat que y o diferent signe i diferent paritat que $y \Rightarrow y$ té el mateix signe i la mateixa paritat que x o diferent signe i diferent paritat que $x \Rightarrow yRx$.
- Transitiva. Donats $x, y, z \in \mathbb{R}$, si xRy, yRz distingim 4 casos:
  - x té el mateix signe i la mateixa paritat que y, y té el mateix signe i la mateixa paritat que z. En aquest cas x té el mateix signe i la mateixa paritat que z per tant xRz.
  - x té el mateix signe i la mateixa paritat que y, y té diferent signe i diferent paritat que z. En aquest cas x té diferent signe i diferent paritat que z per tant xRz.
  - x té diferent signe i diferent paritat que y, y té diferent signe i diferent paritat que z. Com que només hi ha dos signes possibles i el signe de x i y són diferent i el signe de z i y són diferents, els signes de x, z són iguals. El mateix passa amb la paritat. En aquest cas x té el mateix signe i la mateixa paritat que z per tant xRz.

Ara calculem totes les classes d'equivalència:

❑ $\overline{1} = \{ x \in A \mid xR1 \} =$

$\{ x \in \mathbb{Z} - \{0\} \mid x \text{ mateix sig. i par. que } 1 \text{ o } x \text{ diferent sig. i par. que } 1\} =$
$\{ x \in \mathbb{Z} - \{0\} \mid x \text{ senar i positiu o } x \text{ parell i negatiu } \}$.

- $\overline{2} = \{ x \in A \mid xR2 \} =$
  $\{ x \in \mathbb{Z} - \{0\} \mid x \text{ mateix sig. i par. que } 2 \text{ o } x \text{ diferent sig. i par. que } 2\} =$
  $\{ x \in \mathbb{Z} - \{0\} \mid x \text{ parell i positiu o } x \text{ senar i negatiu } \}$.

Aquestes són totes les classes, ja que tot element de $\mathbb{Z} - \{0\}$ pertany a una d'elles. Finalment, el conjunt quocient és el conjunt de totes les classes: $\{\overline{1}, \overline{2}\}$.

Exercici 34. *Sigui P una partició de A. Definim una relació R a A així:*

$$xRy \quad \Leftrightarrow \quad \exists B \in P(x \in B \wedge y \in B)$$

Demostreu que:

a. *Per a cada $x \in A$ hi ha un únic $B \in P$ tal que $x \in B$.*
b. *R és una relació d'equivalència a A.*
c. *Si $x \in B$ i $B \in P$ llavors $\overline{x} = B$.*
d. *$A/R = P$.*

Solució:

a. Sigui $x \in A$ qualsevol. L'existència d'un $B \in P$ que conté x ve de la definició de partició. La unicitat de B ve del fet que els subconjunts de la partició són disjunts dos a dos.
b. R és d'equivalència:
   - Reflexiva: per a qualsevol $x \in A$, si $B \in P$ és el subconjunt que conté x, es té $x \in B \wedge x \in B$, per tant xRx.
   - Simètrica: per a qualssevol $x, y \in A$, es té:
     $xRy \Rightarrow \exists B \in P(x \in B \wedge y \in B)$
     $\Rightarrow \exists B \in P(y \in B \wedge x \in B) \Rightarrow yRx.$
   - Transitiva: per a qualssevol $x, y, z \in A$, es té:
     $xRy \wedge yRz \Rightarrow$
     $\exists B \in P(x \in B \wedge y \in B) \wedge \exists B' \in P(y \in B' \wedge z \in B')$
     $\Rightarrow [\text{usem la unicitat de } B]\ B = B' \Rightarrow \exists B \in P(x \in B \wedge z \in B) \Rightarrow xRz.$
c. Sigui $x \in B$ i $B \in P$. Veiem $\overline{x} = B$:
   - $\overline{x} \subseteq B$: $y \in \overline{x} \Rightarrow yRx \Rightarrow x, y$ pertanyen a un únic subconjunt de la partició $\Rightarrow y \in B$.
   - $B \subseteq \overline{x}$: $y \in B \Rightarrow y \in B \wedge x \in B \Rightarrow yRx \Rightarrow y \in \overline{x}$.
d. Veiem que el conjunt quocient A/R és justament la partició P:
   - $A/R \subseteq P$: sigui $\overline{x}$ una classe qualsevol de A/R. Existeix $B \in P$

tal que $x \in B$, llavors, segons c., es tindrà $\overline{x} = B$. Per tant $\overline{x} \in P$.

- $P \subseteq A/R$: sigui B un element qualsevol de P. Com que B no és el conjunt buit, existeix $x \in B$. Llavors, segons c., es tindrà $\overline{x} = B$ i per tant $B \in A/R$.

Tema 4: FUNCIONS

Exercici 1. Estudieu la injectivitat, exhaustivitat i bijectivitat de:

1. $f : \mathbb{R} \to \mathbb{R}$ definida per $f(x) = e^x$.
2. $f : \mathbb{Z} \to \mathbb{N}$ definida per $f(x) = |x|$.
3. $f : \mathbb{Q} \to \mathbb{Q}$ definida per $f(x) = \frac{3x-5}{4}$.
4. $f : \mathbb{Q} \to \mathbb{R}$ definida per $f(x) = \frac{3x-5}{4}$.
5. $f : \mathbb{R} \to \mathbb{R}$ definida per $f(x) = \frac{3x-5}{4}$.
6. $f : \{1,2,3\} \to \{a,b,c,d\}$ definida per $f(1) = d$, $f(2) = d$, $f(3) = c$.
7. La identitat en A, que denotem per I_A, és l'aplicació $I_A : A \to A$ definida per $I_A(x) = x$.

Solució:

1. $f : \mathbb{R} \to \mathbb{R}$ definida per $f(x) = e^x$:
   - Injectiva: $e^x = e^{x'} \Rightarrow ln\, e^x = ln\, e^{x'} \Rightarrow x = x'$. Per tant la funció és injectiva.
   - Exhaustiva: donat que $e^x > 0 \ \forall x \in \mathbb{R}$, els reals $y \leq 0$ no tenen antiimatge, per tant la funció no és exhaustiva.
   - No és exhaustiva, per tant no és bijectiva.
2. $f : \mathbb{Z} \to \mathbb{N}$ definida per $f(x) = |x|$:
   - Injectiva: no és injectiva donat que $f(1) = f(-1) = 1$.
   - Exhaustiva: tota $y \in \mathbb{N}$ té 2 antiimatges: $y, -y \in \mathbb{Z}$ (llevat del cas $y = 0$ que només té antiimatge $0 \in \mathbb{Z}$), per tant és exhaustiva.
   - No és injectiva, per tant no és bijectiva.

3. $f:\mathbb{Q}\to\mathbb{Q}$ definida per $f(x)=\frac{3x-5}{4}$:
   - Injectiva: $\frac{3x-5}{4}=\frac{3x'-5}{4}\Rightarrow 3x-5=3x'-5\Rightarrow 3x=3x'\Rightarrow x=x'$. Per tant la funció és injectiva.
   - Exhaustiva: donat $y\in\mathbb{Q}$ qualsevol, $\frac{3x-5}{4}=y\Leftrightarrow x=\frac{4y+5}{3}$, i $\frac{4y+5}{3}\in\mathbb{Q}$, per tant cada $y\in\mathbb{Q}$ té una única antiimatge $x=\frac{4y+5}{3}\in\mathbb{Q}$. La funció és doncs exhaustiva.

     Nota: en el 2n ítem la unicitat de l'antiimatge ens assegura la injectivitat, o sigui que ens podíem haver estalviat fer el 1r ítem.
   - La funció és bijectiva per ser injectiva i exhaustiva.
4. $f:\mathbb{Q}\to\mathbb{R}$ definida per $f(x)=\frac{3x-5}{4}$:
   - Injectiva: $\frac{3x-5}{4}=\frac{3x'-5}{4}\Rightarrow 3x-5=3x'-5\Rightarrow 3x=3x'\Rightarrow x=x'$. Per tant la funció és injectiva.
   - Exhaustiva: donat $y\in\mathbb{R}$ qualsevol, es té, formalment: $\frac{3x-5}{4}=y\Leftrightarrow x=\frac{4y+5}{3}$. Però si $y\notin\mathbb{Q}$, llavors $x=\frac{4y+5}{3}\notin\mathbb{Q}$ (demo per RA), i així els irracionals no tenen antiimatge a $\mathbb{Q}$. Per tant la funció no és exhaustiva
   - No és exhaustiva, per tant no és bijectiva.

5. $f:\mathbb{R}\to\mathbb{R}$ definida per $f(x)=\frac{3x-5}{4}$:
   - Injectiva: $\frac{3x-5}{4}=\frac{3x'-5}{4}\Rightarrow 3x-5=3x'-5\Rightarrow 3x=3x'\Rightarrow x=x'$. Per tant la funció és injectiva.
   - Exhaustiva: donat $y\in\mathbb{R}$ qualsevol, $\frac{3x-5}{4}=y\Leftrightarrow x=\frac{4y+5}{3}\in\mathbb{R}$, per tant $y\in\mathbb{R}$ té una única antiimatge $x\in\mathbb{R}$. La funció és doncs exhaustiva.
   - La funció és bijectiva per ser injectiva i exhaustiva.
6. $f:\{1,2,3\}\to\{a,b,c,d\}$ definida per $f(1)=d$, $f(2)=d$, $f(3)=c$:
   - Injectiva: no ho és donat que $f(1)=f(2)=d$.
   - Exhaustiva: no ho és donat que a i b no tenen cap antiimatge.
   - No és bijectiva per no ser injectiva.
7. $I_A:A\to A$ definida per $I_A(x)=x\ \ \forall x\in A.$ Donat que tota $y\in A$ té una única antiimatge $x=y\in A,$ la funció és bijectiva.

Exercici 2. *Demostreu que* $f:\mathbb{Z}\to\mathbb{N}$ *definida per* $f(x)=2x-1$, *si* $x>0$,

$f(x) = -2x$, *si* $x \leq 0$ *és bijectiva.*

Solució: abans que res, i encara que no ho demanen, comprovem que tenim una funció ben definida veient que tot $x \in \mathbb{Z}$ té una única imatge $f(x)$ que pertany a $\mathbb{N}$. És clar que la imatge és única, comprovem que $f(x) \in \mathbb{N}$:

1. $x \in \mathbb{Z},\ x > 0 \ \Rightarrow\ 2x > 0 \ \Rightarrow\ 2x - 1 > -1 \ \Rightarrow\ 2x - 1 \geq 0$ $\Rightarrow\ 2x - 1 \in \mathbb{N}.$
2. $x \in \mathbb{Z},\ x \leq 0 \ \Rightarrow\ -2x \geq 0 \ \Rightarrow\ -2x \in \mathbb{N}.$

Passem a demostrar la bijectivitat de f: el mètode serà veure que cada $y \in \mathbb{N}$ té una única antiimatge $x \in \mathbb{Z}$.

Sigui $y \in \mathbb{N}$ qualsevol. Distingirem 2 casos, segons y sigui senar o parell.

- Suposem $y = 2k - 1 \in \mathbb{N}$ (on $k \in \{1, 2, 3, ...\}$). Es té: $x \in \mathbb{Z} \wedge f(x) = y$ $\Rightarrow$ [quan $x \leq 0$ $f(x)$ és parell] $x > 0 \wedge 2x - 1 = 2k - 1 \ \Rightarrow\ x = k$. Per tant tot senar $y = 2k - 1 \in \mathbb{N}$ té una única antiimatge $x = k = \frac{y+1}{2} \in \mathbb{Z}$.
- Suposem $y = 2k \in \mathbb{N}$ (on $k \in \mathbb{N}$). Es té: $x \in \mathbb{Z} \wedge f(x) = y \ \Rightarrow$ [quan $x > 0$ $f(x)$ és senar] $x \leq 0 \wedge -2x = 2k \ \Rightarrow\ x = -k$. Per tant tot parell $y = 2k \in \mathbb{N}$ té una única antiimatge $x = -k = -\frac{y}{2} \in \mathbb{Z}$.

Conclusió: hem trobat una única antiimatge $x \in \mathbb{Z}$ per a cada element $y \in \mathbb{N}$. Per tant, la funció és bijectiva.

Exercici 3. *Considerem la funció* $f : \mathbb{N} \to \mathbb{N}$ *definida per* $f(x) = x + 1$ *si* x *és parell;* $f(x) = 2x$ *si* x *és senar. Demostreu que* f *és injectiva però no és exhaustiva.*

Solució: Per veure que és injectiva, hem de veure que si $x, x' \in \mathbb{N}$ i $f(x) = f(x')$ llavors $x = x'$.

Primer observem que si x és parell $f(x)$ és senar i si x és senar, $f(x)$ és parell. Per tant si $f(x) = f(x')$ han de tenir la mateixa paritat i per tant x i x' també tenen la mateixa paritat. Llavors només hi ha dos casos:

- x, x' parells. En aquest cas $f(x) = x + 1$ i $f(x') = x' + 1$. Així $f(x) = f(x')$ $\Rightarrow\ x + 1 = x' + 1 \ \Rightarrow\ x = x'$.
- x, x' senars. En aquest cas $f(x) = 2x$ i $f(x') = 2x'$. Així $f(x) = f(x') \Rightarrow$ $2x = 2x' \ \Rightarrow\ x = x'$.

Per veure que no és exhaustiva hem de trobar un element $y \in \mathbb{N}$ que no tingui antiimatge. Veiem que $y = 4$ no té antiimatge per f. La imatge dels elements parells és senar i la imatge d'un nombre senar x és $2x$. Al ser x senar, $2x$ no és mai múltiple de 4. Per tant 4 no és imatge de cap nombre $x \in \mathbb{N}$.

Exercici 4. *Sabem que* $f:\mathbb{Z}\to\mathbb{N}$ *és injectiva. Considerem la funció* $g:\mathbb{Z}\to\mathbb{N}$ *definida per* $g(x)=3f(x)^2+1$. *Demostreu que* g *és injectiva però no exhaustiva.*

Solució: Primer veiem que g és injectiva. Siguin $x,x'\in\mathbb{Z}$ qualssevol. $g(x)=g(x') \Rightarrow 3f(x)^2+1=3f(x')^2+1 \Rightarrow [sumant\ -1]\ 3f(x)^2=3f(x')^2$ $\Rightarrow [mult.\ per\ 1/3]\ f(x)^2=f(x')^2 \Rightarrow |f(x)|=|f(x')| \Rightarrow [f(x),f(x')\in\mathbb{N}]$ $f(x)=f(x') \Rightarrow [f\ injectiva]\ x=x'$.

La funció g no és exhaustiva ja que 0 no té antiimatge: $3f(x)^2+1\geq 1$ ja que $f(x)^2$ és ≥ 0 per ser un quadrat. També es pot veure observant que $3f(x)^2+1$ té residus 1 al dividir per 3. Per tant cap múltiple de 3 té antiimatge.

Exercici 5. *Sabem que* $f:\mathbb{Z}\to\mathbb{N}$ *és exhaustiva. Considerem l'aplicació* $g:\mathbb{Z}\to\mathbb{N}$ *definida per* $g(x)=E(f(x)/2)$. *Demostreu que* g *és exhaustiva pero no injectiva. Aquí* E *indica la funció part entera inferior.*

Solució: Sabem que $\forall y\in\mathbb{N}\ \exists x\in\mathbb{Z}\ f(x)=y$.

- g no és injectiva: basta trobar dos elements diferents amb la mateixa imatge: $a,b\in\mathbb{Z},\ a\neq b,$ i $E(f(a)/2)=E(f(b)/2)$.
  Siguin $a,b\in\mathbb{Z}$ tals que $f(a)=0, f(b)=1$ (existeixen i són enters per ser f exhaustiva i són diferents donat que f és una aplicació). Es té:
  $g(a)=E(f(a)/2)=E(0/2)=0$ i $g(b)=E(f(b)/2)=E(1/2)=0$.
- g és exhaustiva: hem de provar $\forall y\in\mathbb{N}\ \exists x\in\mathbb{Z}\ g(x)=E(f(x)/2)=y$.
  Sigui $y\in\mathbb{N}$ qualsevol. Com que f és exhaustiva i $2y\in\mathbb{N}$, existeix $x\in\mathbb{Z}$ tal que $f(x)=2y$. Aquesta $x\in\mathbb{Z}$ és l'antiimatge per g de y buscada: $g(x)=E(f(x)/2)=E(2y/2)=E(y)=[y\ és\ enter]=y$.

Exercici 6. *Demostreu que estan ben definides, són bijectives i calculeu la inversa de:*

1. $f:\mathbb{Q}\to\mathbb{Q}$, *definida per* $f(x)=\frac{3x-5}{4}$.
2. $f:\mathbb{R}-\{1/3\}\to\mathbb{R}-\{2/3\}$ *definida per* $f(x)=\frac{2x+5}{3x-1}$.
3. $f:\mathbb{Z}\to\mathbb{N}$ *definida per* $f(x)=2x-1$, *si* $x>0$, $f(x)=-2x$, *si* $x\leq 0$.
4. $f:\mathbb{R}\to(1,\infty)$ *definida per* $f(x)=2e^{x-1}+1$.

Solució:

1.

a. Per tal de veure que està ben definida cal veure que donat $x \in \mathbb{Q}$ hi ha un únic $f(x)$ que a més pertany a $\mathbb{Q}$. Si x és racional, clarament $\frac{3x-5}{4}$ és únic i també és racional.

b. Veure que és bijectiva ho podem fer veient que donat $y \in \mathbb{Q}$ existeix un únic $x \in \mathbb{Q}$ tal que $\frac{3x-5}{4} = y$. Ara bé, $\frac{3x-5}{4} = y$
$\Leftrightarrow [\Rightarrow mult.\,per\ 4, \Leftarrow mult.\,per\ 1/4]$ $3x - 5 = 4y$
$\Leftrightarrow [\Rightarrow sumant\ 5, \Leftarrow sumant\ -5]$ $3x = 4y + 5$
$\Leftrightarrow [\Rightarrow mult.\,per\ 1/3, \Leftarrow mult.\,per\ 3]$ $x = \frac{4y+5}{3}$. Observem que $\frac{4y+5}{3} \in \mathbb{Q}$ ja que x és racional. Com que $\frac{3x-5}{4} = y \Leftrightarrow x = \frac{4y+5}{3}$, donat $y \in \mathbb{Q}$ existeix un únic $x \in \mathbb{Q}$ tal que $\frac{3x-5}{4} = y$ i aquest x és $\frac{4y+5}{3}$.

c. Hem vist doncs que f és bijectiva i que la seva inversa és: $f^{-1} : \mathbb{Q} \to \mathbb{Q} \quad y \to \frac{4y+5}{3}$. Si canviem el nom de la variable ho podem expressar així: $f^{-1}(x) = \frac{4x+5}{3}$.

2.

a. Per tal de veure que està ben definida cal veure que donat $x \in \mathbb{R} - \{1/3\}$, $\frac{2x+5}{3x-1}$ és únic i que a més pertany a $\mathbb{R} - \{2/3\}$. Si $x \neq 1/3$ llavors $3x - 1 \neq 0$ i per tant $\frac{2x+5}{3x-1}$ existeix. Que és únic és obvi. Falta veure que $\frac{2x+5}{3x-1} \in \mathbb{R} - \{2/3\}$, és a dir, que $\frac{2x+5}{3x-1}$ és real i que $\frac{2x+5}{3x-1} \neq \frac{2}{3}$. $\frac{2x+5}{3x-1}$ és real ja que x també ho és. Que $\frac{2x+5}{3x-1} \neq \frac{2}{3}$ ho fem per RA: $\frac{2x+5}{3x-1} = \frac{2}{3} \Rightarrow 3(2x-5) = 2(3x-1) \Rightarrow$ $6x - 15 = 6x - 2 \Rightarrow -15 = -2$, absurd.

b. Veurem ara que és bijectiva demostrant que donat $y \in \mathbb{R} - \{2/3\}$ existeix un únic $x \in \mathbb{R} - \{1/3\}$ tal que $\frac{2x+5}{3x-1} = y$. Ara bé, $\frac{2x+5}{3x-1} = y$ $\Rightarrow [mult.\,per\ 3x-1]$ $2x + 5 = y(3x-1) \Rightarrow 2x + 5 = 3yx - y \Rightarrow$ $5 + y = 3xy - 2x = x(3y-2)$. Ara bé, com que $y \in \mathbb{R} - \{2/3\}$, $y \neq 2/3$ i per tant $3y - 2 \neq 0$. Multiplicant l'equació $x(3y-2) = 5 + y$ per $1/(3y-2)$ tenim que $x = \frac{y+5}{3y-2}$. Acabem de veure que donat $y \in \mathbb{R} - \{2/3\}$ hi ha com molt un x tal que $\frac{2x+5}{3x-1} = y$ i que aquest x és $x = \frac{y+5}{3y-2}$. Això demostra que f és

injectiva. Falta veure la exhaustivitat i en aquest cas es redueix a provar $\frac{y+5}{3y-2} \in \mathbb{R} - \{1/3\}$ i que $f(\frac{y+5}{3y-2}) = y$. Com que $y \in \mathbb{R}$ clarament $\frac{y+5}{3y-2} \in \mathbb{R}$. Veiem que $\frac{y+5}{3y-2} \neq \frac{1}{3}$ per RA. Si fós $\frac{y+5}{3y-2} = \frac{1}{3}$ tindríem $3(y+5) = 3y-2$ i per tant $15 = -2$, absurd. Ara calculem $f(\frac{y+5}{3y-2})$: $f(\frac{y+5}{3y-2}) = \frac{2(\frac{y+5}{3y-2})+5}{3(\frac{y+5}{3y-2})-1} = \frac{\frac{2(y+5)+5(3y-2)}{3y-2}}{\frac{3(y+5)-(3y-2)}{3y-2}} = \frac{\frac{17y}{3y-2}}{\frac{17}{3y-2}} = \frac{17y}{17} = y$.

c. Finalment observem que la inversa $f^{-1} : (\mathbb{R} - \{2/3\}) \to (\mathbb{R} - \{1/3\})$, vé donada per $f^{-1}(y) = \frac{y+5}{3y-2}$. Expressada en la variable x: $f^{-1}(x) = \frac{x+5}{3x-2}$.

3. Ja hem vist que és bijectiva a l'**exercici 5**. Fixem-nos, que quan hem calculat l'antiimatge d'un $y \in \mathbb{N}$ depenia de la seva paritat i era $-y/2$ quan y és parell i $(y+1)/2$ quan y és senar. Això vol dir que la inversa de f és la funció $f^{-1} : \mathbb{N} \to \mathbb{Z}$ definida per $f^{-1}(x) = -x/2$ si x és parell i $f^{-1}(x) = (x+1)/2$ altrament.

4.

a. Per a veure que f està ben definida hem de veure que per a tot $x \in \mathbb{R}$ l'expressió $2e^{x-1}+1$ *es pot calcular (obvi) i que pertany a* $(1,\infty)$*, és a dir,* $2e^{x-1}+1 > 1$. *Ara bé,* $2e^{x-1}+1 > 1 \Leftrightarrow 2e^{x-1} > 0 \Leftrightarrow e^{x-1} > 0$. *Això últim és cert ja la funció exponencial pren valors estrictament positius.*

b. Veurem ara que és bijectiva demostrant que donat $y \in (1,\infty)$ existeix un únic $x \in \mathbb{R}$ tal que $2e^{x-1}+1 = y$. *Ara bé,* $2e^{x-1}+1 = y \Leftrightarrow 2e^{x-1} = y-1 \Leftrightarrow e^{x-1} = \frac{y-1}{2} \Leftrightarrow [\Rightarrow \frac{y-1}{2} > 0$ *que* $y > 1\,]$ $x - 1 = ln(\frac{y-1}{2}) \Leftrightarrow x = ln(\frac{y-1}{2}) + 1$. *Observem que* x *existeix gràcies a que quan* $y > 1$ *es pot calcular* $ln(\frac{y-1}{2})$. *La unicitat ens la dóna la implicació* $\Rightarrow$.

c. *Finalment la inversa* $f^{-1} : (1,\infty) \to \mathbb{R}$ *vé definida per* $f^{-1}(x) = ln(\frac{x-1}{2}) + 1$.

Exercici 7. *Sigui* $f : \mathbb{Z} \to \mathbb{Z}$ *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 dels conjunts següents:

$\{1,2,3,4,5,6,7,8,9,10\}$, $\{x \in \mathbb{Z} \mid x \text{ és } senar\}$, $\mathbb{N}$, $\mathbb{Z}$, $\{x \in \mathbb{Z} \mid x \leq 0\}$, $\{x \in \mathbb{Z} \mid x < 0\}$.

Solució:

a. $f(\{-2,-1,0,1,2,3,4\}) = \{f(-2), f(-1), f(0), f(1), f(2), f(3), f(4)\} = \{0,1,4,9,16\}$.

$f(\mathbb{N}) = \{n^2 \mid n \in \mathbb{N}\} = \{0,1,4,9,16,...,n^2,...\}$.

$f(\mathbb{Z}) = \{n^2 \mid n \in \mathbb{Z}\} = \{0,1,4,9,16,...,n^2,...\}$.

$f(\{x \in \mathbb{Z} \mid x \text{ és } parell\}) = \{(2k)^2 \mid k \in \mathbb{Z}\} = \{4k^2 \mid k \in \mathbb{N}\}$.

$f(\{x \in \mathbb{Z} \mid x < 0\}) = \{n^2 \mid n \in \mathbb{N},\ n \neq 0\} = \{1,4,9,16,...,n^2,...\}$.

b. $f^{-1}(\{1,2,3,4,5,6,7,8,9,10\}) = \{n \in \mathbb{Z} \mid n^2 \in \{1,2,3,4,5,6,7,8,9,10\}\} = \{-3,-2,-1,1,2,3\}$.

$f^{-1}(\{x \in \mathbb{Z} \mid x \text{ és } senar\}) = \{x \in \mathbb{Z} \mid x^2 \text{ és } senar\} = [x^2 \ senar \Leftrightarrow x \ senar]$ $\{x \in \mathbb{Z} \mid x \text{ és } senar\}$.

$f^{-1}(\mathbb{N}) = \{x \in \mathbb{Z} \mid x^2 \in \mathbb{N}\} = \mathbb{Z}$.

$f^{-1}(\mathbb{Z}) = \{x \in \mathbb{Z} \mid x^2 \in \mathbb{Z}\} = \mathbb{Z}$.

$f^{-1}(\{x \in \mathbb{Z} \mid x \leq 0\}) = \{0\}$ i $f^{-1}(\{x \in \mathbb{Z} \mid x < 0\}) = \emptyset$.

Exercici 8. *Sigui* $f : A \to B$ *i siguin* $Y_1, Y_2 \subseteq B$. *Demostreu que* $f^{-1}(Y_1 \cup Y_2) = f^{-1}(Y_1) \cup f^{-1}(Y_2)$.

Solució: Sigui $x \in A$ qualsevol. Demostrarem la igualtat dels conjunts usant dobles implicacions:

$x \in f^{-1}(Y_1 \cup Y_2) \Leftrightarrow [def.\ f^{-1}(T)]\ f(x) \in Y_1 \cup Y_2 \Leftrightarrow [def.\ \cup]$

$f(x) \in Y_1 \vee f(x) \in Y_2 \Leftrightarrow [def. f^{-1}(T)]\ x \in f^{-1}(Y_1) \vee x \in f^{-1}(Y_2)$

$\Leftrightarrow [def.\ \cup]\ x \in f^{-1}(Y_1) \cup f^{-1}(Y_2)$. □

Exercici 9. *Sigui* $f : A \to B$ *i sigui* $X \subseteq A$. *Demostreu que* $X \subseteq f^{-1}(f(X))$.

Solució: Sigui $x \in A$ qualsevol. Es té:

$x \in X \Rightarrow [def.\ f(X)]\ f(x) \in f(X) \Rightarrow [def.\ f^{-1}(T)]\ x \in f^{-1}(f(X))$. □

Exercici 10. *Doneu un exemple de* $f : A \to B$ *i* $X \subseteq A$ *tals que* $f^{-1}(f(X)) \neq X$.

Solució: Sabem per l'exercici 3 que $X \subseteq f^{-1}(f(X))$, per tant haurem de pensar en un conjunt $X \subseteq A$ *tal que* $f^{-1}(f(X))$ no estigui inclòs a X.

Si prenem $f : \{1,2\} \to \{3\}$ (per tant $f(1) = f(2) = 3$), i $X = \{1\}$, es té:

$f(\{1\}) = \{3\}$, en canvi $f^{-1}(f(\{1\})) = f^{-1}(\{3\}) = \{1,2\} \neq \{1\}$.

Exercici 11. *Sigui $f : A \to B$ injectiva i sigui $X \subseteq A$. Demostreu que $f^{-1}(f(X)) = X$.*

Solució: La primera inclusió $X \subseteq f^{-1}(f(X))$ l'hem vist a l'exercici 3. Ara falta veure $f^{-1}(f(X)) \subseteq X$. Sigui $x \in A$ qualsevol. Es té:

$x \in f^{-1}(f(X)) \quad \Rightarrow [def\ f^{-1}(T)] \quad f(x) \in f(X) \quad \Rightarrow [def\ f(X)]$

$\exists x' \in X\ f(x') = f(x) \quad \Rightarrow [f\ injectiva] \quad x = x' \quad \Rightarrow [x' \in X] \quad x \in X$. □

Exercici 12. *Sigui $f : A \to B$ i siguin $X_1, X_2 \subseteq A$. Demostreu que $f(X_1 \cap X_2) \subseteq f(X_1) \cap f(X_2)$.*

Solució: Sigui $y \in B$ un element qualsevol.

$y \in f(X_1 \cap X_2) \quad \Rightarrow [def.\ f(T)] \quad \exists x \in X_1 \cap X_2\ \ f(x) = y \quad \Rightarrow [def.\ \cap]$

$x \in X_1 \wedge x \in X_2 \quad \Rightarrow \quad \exists x \in X_1\ f(x) = y \ \wedge\ \exists x \in X_2\, f(x) = y \quad \Rightarrow [def.\ f(T)]$

$y \in f(X_1) \wedge y \in f(X_2) \quad \Rightarrow [def.\ \cap] \quad y \in f(X_1) \cap f(X_2)$. □

Exercici 13. *Doneu exemples de $f : A \to B$ i $X_1, X_2 \subseteq A$ tals que $f(X_1 \cap X_2) \neq f(X_1) \cap f(X_2)$.*

Solució: Si prenem $f : \{1,2\} \to \{3\}$ (per tant $f(1) = f(2) = 3$), es té:
$f(\{1\} \cap \{2\}) = f(\emptyset) = \emptyset$ i en canvi $f(\{1\}) \cap f(\{2\}) = \{3\} \cap \{3\} = \{3\}$.
Un altre exemple una mica més sofisticat:
$f : \mathbb{R} \to \mathbb{R}$ definida per $f(x) = x^2$, tenim $f((-\infty, 0] \cap [0, +\infty)) = f(\{0\}) = \{0\}$
i en canvi $f((-\infty, 0]) \cap f([0, +\infty)) = [0, +\infty) \cap [0, +\infty) = [0, +\infty)$.

Exercici 14. *Sigui $f : A \to B$ injectiva i siguin $X_1, X_2 \subseteq A$. Demostreu que $f(X_1 \cap X_2) = f(X_1) \cap f(X_2)$.*

Solució: A l'exercici 6 hem demostrat que $f(X_1 \cap X_2) \subseteq f(X_1) \cap f(X_2)$. Falta ara demostrar la inclusió recíproca: $f(X_1) \cap f(X_2) \subseteq f(X_1 \cap X_2)$.
Sigui $y \in B$ un element qualsevol.

$y \in f(X_1) \cap f(X_2) \quad \Rightarrow [def.\ \cap] \quad y \in f(X_1) \wedge y \in f(X_2) \quad \Rightarrow [def.\ f(T)]$

$\exists x_1 \in X_1\ f(x_1) = y \wedge\ \exists x_2 \in X_2\ f(x_2) = y \quad \Rightarrow \quad f(x_1) = f(x_2) \quad \Rightarrow [f\ injectiva]$

$x_1 = x_2 \Rightarrow [def.\ \cap] \quad x_1 = x_2 \in X_1 \cap X_2 \quad \Rightarrow [def.\ f(T)] \quad y \in f(X_1 \cap X_2)$.

□

Exercici 15. *Donades* $f:\mathbb{R}\to\mathbb{R}$ *definida per* $f(x)=e^x$, $g:\mathbb{R}\to\mathbb{R}$ *definida per* $g(x)=2x$, *calculeu la composada* $g\circ f$. *Es pot calcular* $f\circ g$ *?*
Solució: Es té $g\circ f:\mathbb{R}\to\mathbb{R}$ definida per $(g\circ f)(x)=g(f(x))=g(e^x)=2e^x$.
També es té $f\circ g:\mathbb{R}\to\mathbb{R}$ definida per $(f\circ g)(x)=f(g(x))=f(2x)=e^{2x}$.

Exercici 16. *Donades* $f:\mathbb{Z}\to\mathbb{Z}$ *definida per* $f(x)=x^3-11$, $g:\mathbb{Z}\to\mathbb{N}$ *definida per* $g(x)=2x-1$, *si* $x>0$, $g(x)=-2x$, *si* $x\le 0$, *calculeu la composada* $g\circ f$ *. Es pot calcular* $f\circ g$ *?*
Solució: Si $x\in\mathbb{Z}$ és qualsevol, es té $(g\circ f)(x)=g(f(x))=g(x^3-11)$.
Hem de distingir 2 casos, segons sigui $x^3-11>0$ o bé $x^3-11\le 0$.

- Cas $x^3-11>0\Leftrightarrow x^3>11\Leftrightarrow x\ge 3$ (donat que $x\in\mathbb{Z}$).
  LLavors $(g\circ f)(x)=g(f(x))=g(x^3-11)=2(x^3-11)-1=2x^3-23$.
- Cas $x^3-11\le 0\Leftrightarrow x^3\le 11\Leftrightarrow x\le 2$ (donat que $x\in\mathbb{Z}$).
  LLavors $(g\circ f)(x)=g(f(x))=g(x^3-11)=-2(x^3-11)=-2x^3+22$.

Només es pot composar quan el codomini de la primera aplicació és el mateix que (o està contingut a) el domini de la segona.
En el cas de $f\circ g$ es compleix la segona condició: $\mathbb{N}\subseteq\mathbb{Z}$. Per tant, considerem
$f\circ g:\mathbb{Z}\to\mathbb{Z}$ definida per $(f\circ g)(x)=f(g(x))$.
Hem de distingir 2 casos, segons sigui $x>0$ o bé $x\le 0$.

- Cas $x>0$: llavors $(f\circ g)(x)=f(g(x))=f(2x-1)=(2x-1)^3-11$.
- Cas $x\le 0$: llavors $(f\circ g)(x)=f(g(x))=f(-2x)=(-2x)^3-11=-8x^3-11$.

Exercici 17. *Sigui* $f:\mathbb{N}\to\mathbb{N}$ *definida per* $f(x)=x+1$, *si* x *és parell,* $f(x)=2x$, *altrament. Calculeu* $f\circ f$ *i proveu que* f *és injectiva.*
Solució: Es té $f\circ f:\mathbb{N}\to\mathbb{N}$ definida per:

- Si x és parell, $(f\circ f)(x)=f(f(x))=f(x+1)=[x+1\ \text{és}\ \textit{senar}]=2(x+1)$.
- Si x és senar, $(f\circ f)(x)=f(f(x))=f(2x)=[2x\ \text{és}\ \textit{parell}]=2x+1$.

f és injectiva: si $x,y\in\mathbb{N}$ són qualssevol, veiem que $f(x)=f(y)\Rightarrow x=y$.
Donat que la imatge d'un parell és senar i la imatge d'un senar és parell, la igualtat $f(x)=f(y)$ només es pot donar en el cas que x,y tinguin la mateixa paritat. Per tant només hi ha dos casos:

- Cas x,y parells: $f(x)=f(y)\ \Rightarrow\ x+1=y+1\ \Rightarrow\ x=y$.

- Cas x, y senars: $f(x) = f(y) \Rightarrow 2x = 2y \Rightarrow x = y.$ □

Exercici 18. *Demostreu la propietat associativa de la composició: si* $f : A \to B$, $g : B \to C$, $h : C \to D$ *llavors* $h \circ (g \circ f) = (h \circ g) \circ f$.
Solució: Es té $h \circ (g \circ f) : A \to D$ i $(h \circ g) \circ f : A \to D$, per tant per veure que són iguals basta comprovar que $(h \circ (g \circ f))(x) = ((h \circ g) \circ f)(x) \ \forall x \in A$.
En efecte, si $x \in A$ és un element qualsevol:

- $(h \circ (g \circ f))(x) = [def.\ h \circ (g \circ f)] = h(\ (g \circ f)(x)\ ) = [def.\ g \circ f]\ h(g(f(x)))$.
- $((h \circ g) \circ f)(x) = [def.\ (h \circ g) \circ f] = (h \circ g)(f(x)) = [def.\ h \circ g]\ h(g(f(x)))$. □

Exercici 19. *Demostreu que la composició d'aplicacions injectives és injectiva.*
Solució: Siguin $f : A \to B,\ g : B \to C,$ ambdues injectives. Veiem que $g \circ f : A \to C$ és també injectiva. Si $x, y \in A$ són qualssevol:
$(g \circ f)(x) = (g \circ f)(y) \Rightarrow [def.\ g \circ f] \quad g(f(x)) = g(f(y)) \Rightarrow [g\ injectiva] \Rightarrow$
$f(x) = f(y) \Rightarrow [f\ injectiva] \quad x = y.$ □

Exercici 20. *Demostreu que si* $g \circ f$ *és exhaustiva llavors* g *és exhaustiva.*
Solució: Siguin dues aplicacions $f : A \to B$, $g : B \to C$. Suposem que $g \circ f : A \to C$ és exhaustiva, i demostrem que g també ho és.
En efecte: sigui $z \in C$ qualsevol, volem veure que $\exists y \in B\ g(y) = z$. Com que $g \circ f$ és exhaustiva, sabem que $\exists x \in A\ (g \circ f)(x) = z$. Donat que $(g \circ f)(x) = g(f(x)) = z$ i $f(x) \in B$, basta prendre $y = f(x)$ com a antiimatge buscada de $z \in C$ per g: $g(y) = g(f(x)) = z$. □

Exercici 21. *Sigui* $f : \mathbb{Z} \to \mathbb{Z}$ *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.*
Solució: Es té $f \circ f : \mathbb{Z} \to \mathbb{Z}$ definida per:

- Si x és parell, $(f \circ f)(x) = f(f(x)) = f(x + 1) = [x + 1$ és *senar*$] =$ $(x + 1) - 1 = x.$
- Si x és senar, $(f \circ f)(x) = f(f(x)) = f(x - 1) = [x - 1$ és *parell*$] =$ $(x - 1) + 1 = x.$

Acabem de veure que $f \circ f = I_{\mathbb{Z}}$. Com que $I_{\mathbb{Z}}$ és bijectiva, per la propietat 10 de la composició, deduïm que f és bijectiva i que la seva inversa és f. □

Exercici 22. *Demostreu que si $g \circ f$ és exhaustiva i g és injectiva llavors f és exhaustiva.*
Solució: Siguin dues aplicacions $f : A \to B$, $g : B \to C$. Suposem que $g \circ f : A \to C$ és exhaustiva i $g : B \to C$ és injectiva, i demostrem que $f : A \to B$ és exhaustiva.
En efecte: sigui $y \in B$ qualsevol, volem veure que $\exists x \in A \ f(x) = y$.
Considerem l'element $g(y) \in C$, que té una antiimatge $x \in A$ per $g \circ f$: $\exists x \in A \ \ (g \circ f)(x) = g(y)$, o sigui $g(f(x))) = g(y)$. Com que g és injectiva, es té que $f(x) = y$, i ja tenim l'antiimatge buscada $x \in A$ de y per l'aplicació f. □

Tema 5: DIVISIBILITAT

Exercici 1. *Siguin a, b enters. Demostreu que $a \mid ab$.*
Solució: $\exists q \in \mathbb{Z} \ ab = aq$ és cert, només cal prendre $q = b$. □

Exercici 2. *Siguin a, b, c enters. Demostreu que $a \mid b \ \Rightarrow \ ac \mid bc$.*
Solució: $a \mid b \ \Rightarrow [def.\ a \mid b] \ \ \exists q \in \mathbb{Z} \ b = aq \ \Rightarrow [multipl.\ per\ c] \ \ bc = acq$ $\Rightarrow \ [def.\ x \mid y] \ \Rightarrow \ ac \mid bc$. □

Exercici 3. *Siguin a, b, c enters. Demostreu que si $c \neq 0$, $ac \mid bc \ \Rightarrow \ a \mid b$.*
Solució: $ac \mid bc \ \Rightarrow [def.\ x \mid y] \ \ \exists q \in \mathbb{Z} \ bc = acq \ \Rightarrow [multipl.\ per\ 1/c]$ $b = aq \Rightarrow [def.\ x \mid y] \ \Rightarrow \ a \mid b$. Observeu que quan hem multiplicat per $1/c$ hem usat la hipòtesi $c \neq 0$. □

Exercici 4. *Siguin a, b enters. Demostreu que $a \mid b$, $b \mid a \ \Rightarrow \ |a| = |b|$.*
Solució: En donarem dues demostracions.
1a demo: $a \mid b, \ b \mid a \ \Rightarrow [def.\ x \mid y] \ \ \exists q, q' \in \mathbb{Z} \ b = aq, \ a = bq' \ \Rightarrow [subs.]$ $a = aqq'$. Ara distingim dos casos:

- Cas $a = 0$: $a = 0 \Rightarrow [b = aq] \quad b = 0 \Rightarrow |a| = |b| = 0.$
- Cas $a \neq 0$: $a = aqq' \Rightarrow [mult.\ per\ 1/a] \quad 1 = qq' \Rightarrow [q, q' \in \mathbb{Z}] \quad |q| = 1$ $\Rightarrow \quad |a| = |b| \cdot |q| = |b|.$ □

2a demo: En aquesta usarem la propietat 9:

Si $b \neq 0$, $\quad a \mid b \quad \Rightarrow \quad |a| \leq |b|$.

Distingim tres casos:

- Cas $a = 0$: $a \mid b \Rightarrow b = aq$ per un cert $q \Rightarrow b = 0 \Rightarrow |a| = |b| = 0.$
- Cas $b = 0$: Es fa igual.
- Cas $a \neq 0, b \neq 0$: de $a \mid b,\ b \mid a$, per la propietat 9 tenim $|a| \leq |b|$, $|b| \leq |a|$ i per tant $|a| = |b|$. □

Exercici 5. *Siguin a, b, c, u, v enters. Demostreu que $a \mid b$, $a \mid c \Rightarrow a \mid ub + vc$*

Solució: $a \mid b$, $a \mid c \quad \Rightarrow [def.\ x \mid y] \quad \exists q, q' \in \mathbb{Z} \ \ b = aq, c = aq'$. Ara multiplicant $b = aq$ per u, multiplicant $c = aq'$ per v i sumant obtenim: $ub + vc = uaq + vaq' = a(uq + vq')$. Per definició, $a \mid ub + vc$.

Exercici 6. *Siguin a, b enters, n natural. Demostreu que $a \mid b$ implica $a^n \mid b^n$.*

Solució: $a \mid b \quad \Rightarrow [def.\ a \mid b] \quad \exists q \in \mathbb{Z} \ \ b = aq \quad \Rightarrow [elevant\ a\ \ n] \quad b^n = a^n q^n$ $\Rightarrow [def.\ x \mid y] \quad a^n \mid b^n$. □

Exercici 7. *Calculeu el $mcd(a, b)$ en els casos següents:*

a. $b = 2a$.

b. $b = a + 1$.

c. $b \mid a$.

d. $b = mcd(a, c)$.

Solució:

a. Com que $a \mid b$, per la propietat 1, $mcd(a, b) = |a|$.

b. $mcd(a, b) = mcd(a, a + 1) = mcd(a + 1, a) = [Teor.\ Euclides] = mcd(1, a) = [1 | a] = 1$.

c. per la propietat 1, $mcd(a, b) = |b|$.

d. $b = mcd(a, c)$. Observem que en aquest cas $b \mid a$ i per la propietat 1, $mcd(a, b) = |b|$.

Exercici 8. *Demostreu que* $mcd(2k+5, 3k+7) = 1.$

Solució: Utilitzem el Teorema d'Euclides diverses vegades:

$mcd(2k+5, 3k+7) = [T.\,Euclides] = mcd(2k+5, (3k+7)-(2k+5)) =$
$mcd(2k+5, k+2) = [T.\,Euclides] = mcd((2k+5)-2(k+2), k+2) =$
$mcd(1, k+2) = [\,1 \mid (k+2)\,] = 1.$ □

Exercici 9. *Calculeu* $mcd(a^2+1,\ a^3+1)$.

Solució: Utilitzem el Teorema d'Euclides diverses vegades:

$mcd(a^2+1,\ a^3+1) = [T.\,Euclides] = mcd(a^2+1,\ a^3+1-a(a^2+1)) =$
$mcd(a^2+1,\ 1-a) = [T.\,Euclides] = mcd(a^2+1+a(1-a),\ 1-a) =$
$mcd(1+a,\ 1-a) = [T.\,Euclides] = mcd(1+a,\ 1-a+(1+a)) =$
$mcd(1+a,\ 2)$. Ara hem de distingir dos casos, segons la paritat de a:

- a parell: llavors $a+1$ és senar i per tant $mcd(1+a,\ 2) = 1$.
- a senar: llavors $2 \mid a+1$ i per tant $mcd(1+a,\ 2) = 2$.

Resumint, tenim que $mcd(a^2+1,\ a^3+1) = 1$ si a és parell i $mcd(a^2+1,\ a^3+1) = 2$ si a és senar.

Exercici 10. *Demostreu que si* p, q *són primers i* $p \mid q$ *llavors* $p = q$.

Solució: Com que q és primer, els seus únics divisors positius són $1, q$. Com que p és un dels divisor positius de q i no és 1 (ja que és primer) ha de ser $p = q$. □

Exercici 11. *Demostreu que si* $ab + cd = 1$ *llavors* $mcd(a,c) = mcd(b,c) = mcd(a,d) = mcd(b,d) = 1$.

Solució: És suficient demostrar $mcd(a,c) = 1$, els altres es fan igual. Si k és un divisor comú de a i c, per linealitat, $k \mid ab + cd = 1$ i per tant $k = \pm 1$. Per tant a, c només tenen dos divisors comuns: $1, -1$, i el màxim és 1. □

Exercici 12. *Demostreu que si* $b \mid a$ *llavors* $mcd(a,b,c,..) = mcd(b,c,..)$.

Solució: Posem $d_1 = mcd(a,b,c...),\ d_2 = mcd(b,c...)$. Hem de veure $d_1 = d_2$ i per tant n'hi ha prou amb veure que $d_1 \le d_2$ i $d_2 \le d_1$. Com que $d_1 \mid b$, $d_1 \mid c, \ldots$, d_1 és un divisor comú de $b, c, \ldots$ i per tant $\le$ que el seu mcd. Així $d_1 \le d_2$. Per a l'altra desigualtat, com que $d_2 \mid b$, i $b \mid a$, deduïm (transitivitat) que $d_2 \mid a$. Per tant d_2 és divisor de $a, b, c, \ldots$ i així $d_2 \le d_1$. □

Exercici 13. *Calculeu* $mcd\,(512, 88)$ *usant l'algorisme d'Euclides.*

Solució:

q		5	1	4		
r	512	88	72	16	8	0

Exercici 14. Demostreu que l'aplicació $f : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ definida per $f(x, y) = 1004x + 189y$ és exhaustiva.

Solució: Que f és exhaustiva significa que per a tot $z \in \mathbb{Z}$ existeix $(x, y) \in \mathbb{Z} \times \mathbb{Z}$ tal que $z = 1004x + 189y$. Això és el mateix que dir que qualsevol enter es pot posar com a combinació lineal de 1004 i 189.

Comencem calculant el mcd de 1004 i 189 i dóna 1. A continuació calculem una identitat de Bézout amb la taula i obtenim:

x	1	0	1	-3	13	-16	
y	0	1	-5	16	-69	85	
q		5	3	4	1		
r	1004	189	59	12	11	1	0

$$1 = 1004(-16) + 189(85)$$

Per la identitat de Bézout sabem que 1 és combinació lineal de 1004 i 189. Ara, si multipliquem la identitat de Bézout per z obtenim:

$$z = 1004(-16z) + 189(85z),$$

i per tant veiem que per a tot enter z hi ha enters $x = -16z$, $y = 85z$ tals que $z = 1004x + 189y$. □

Exercici 15. *Demostreu que si* a, b *són primers entre si llavors* a^n, b^m *també són primers entre si (*$n, m \geq 0$*).*

Solució: Contrarecíproc: si a^n, b^m no són primers entre si llavors a, b no són primers entre si.

En efecte: a^n, b^m no primers entre si $\Rightarrow$ [*vist a teoria*] tenen un divisor primer comú p. Ara $p \mid a^n$, $p \mid b^m$ $\Rightarrow$ [*p primer, lema d'Euclides*] $p \mid a$, $p \mid b$. Així p és un divisor primer comú de a i de b i per tant a, b no són primers entre

si. □

Nota 1: el recíproc de l'enunciat és cert, el seu contrarecíproc és:

si a, b *no són primers entre si llavors* a^n, b^m *no són primers entre si,*

i la seva demostració és similar pero no requereix del lema d'Euclides.

Nota 2: aquest problema es pot fer també usant les factoritzacions de a i b.

Exercici 16. *Demostreu que si* $a^2 = 5b^2$ *llavors tant* a *com* b *són múltiples de* 5.

Solució: $a^2 = 5b^2 \Rightarrow 5 \mid a^2 \Rightarrow [5\ primer,\ lema\ d'Euclides]\ 5 \mid a \Rightarrow [def\ x \mid y]$

$\exists t \in \mathbb{Z}\ a = 5t \Rightarrow a^2 = 25t^2 \Rightarrow [subst.]\ 25t^2 = 5b^2 \Rightarrow 5t^2 = b^2 \Rightarrow 5 \mid b^2 \Rightarrow [5\ primer,\ lema\ d'Euclides]\ 5 \mid b \Rightarrow 5 \mid a \wedge 5 \mid b$. □

Exercici 17. *Demostreu que* a, b *són primers entre si* $\Leftrightarrow$ *existeixen* x, y *tals que* $1 = ax + by$.

Solució:

$\Rightarrow$) a, b primers entre si $\Rightarrow$ $mcd(a,b) = 1 \Rightarrow [Id.\ Bézout]$ existeixen enters x, y tals que $ax + by = 1$.

$\Leftarrow$) suposem que existeixen enters x, y tals que $ax + by = 1$. Sigui k divisor comú de a i de b. Per linealitat, k serà divisor de $ax + by = 1$, per tant $k = -1\ o\ k = 1$. D'aquí resulta que $mcd(a,b) = 1$. □

Exercici 18. *Demostreu que* $mcd(a,b) = 1$ *i* $mcd(a,c) = 1 \Leftrightarrow mcd(a, bc) = 1$.

Solució: En donem tres demostracions.

1a demo: (amb el Lema d'Euclides)

$\Rightarrow$) Demostem el contrarecíproc, és dir:

$$mcd(a,bc) \neq 1 \Rightarrow mcd(a,b) \neq 1\ o\ mcd(a,c) \neq 1.$$

En efecte: $mcd(a,bc) \neq 1 \Rightarrow$ existeix p divisor primer de a i de $bc \Rightarrow p \mid bc \Rightarrow [p\ primer,\ lema\ d'Euclides]\ p \mid b$ o $p \mid c$. Si $p \mid b$, p és un divisor comú de a, b i per tant $mcd(a,b) \neq 1$. Si $p \mid c$ tindrem $mcd(a,c) \neq 1$.

$\Leftarrow$) Demostrem el contrarecíproc:

$$mcd(a,b) \neq 1\ o\ mcd(a,c) \neq 1 \Rightarrow mcd(a,bc) \neq 1.$$

En efecte, ho fem per casos:

$mcd(a,b) \neq 1 \Rightarrow \exists p$ divisor primer de a i de $b \Rightarrow \exists p$ divisor primer de a i

de $bc \Rightarrow mcd(a,bc) \neq 1$. El cas $mcd(a,c) \neq 1$ es fa igual. □

2a demo: (algebraica, amb Id. Bézout i Exercici 3)

$\Rightarrow$) $mcd(a,b) = 1$ i $mcd(a,c) = 1 \Rightarrow [Id.\ Bézout]$ hi ha enters x,y,z,t tals que

$ax + by = 1$ i $az + ct = 1 \Rightarrow [multiplicant]$ $(ax+by)(az+ct) = 1 \Rightarrow$

$a(axz + cxt + byz) + bc(yt) = 1 \Rightarrow [Exercici\ 3]$ $mcd(a,bc) = 1$.

$\Leftarrow$) $mcd(a,\ bc) = 1 \Rightarrow [Bézout]$ existeixen enters x,y tals que $ax + bcy = 1 \Rightarrow ax + b(cy) = 1$ i $ax + c(by) = 1 \Rightarrow [Exercici\ 3]$ $mcd(a,b) = 1$ i $mcd(a,c) = 1$. □

3a demo: (usant conjunts i Lema d'Euclides)

Primer veiem que si denotem per $DP(a)$ el conjunt dels divisors primers de a tenim: $DP(bc) = DP(b) \cup DP(c)$.

En efecte, si p és primer:

$p \in DP(bc) \Leftrightarrow p \mid bc \Leftrightarrow [\Rightarrow Lema\ Euclides, \Leftarrow transitivitat]$

$p \mid b \vee p \mid c \Leftrightarrow p \in DP(b) \vee p \in DP(c) \Leftrightarrow p \in DP(b) \cup DP(c)$.

D'altra banda, observem que: $mcd(a,b) = 1 \Leftrightarrow DP(a) \cap DP(b) = \emptyset$.

Utilitzant-ho tot plegat:

$mcd(a,bc) = 1 \Leftrightarrow DP(a) \cap DP(bc) = \emptyset \Leftrightarrow$

$DP(a) \cap (DP(b) \cup DP(c)) = \emptyset \Leftrightarrow [DeMorgan]$

$(DP(a) \cap DP(b)) \cup (DP(a) \cap DP(c)) = \emptyset \Leftrightarrow DP(a) \cap DP(b) = \emptyset$ i

$DP(a) \cap DP(c) = \emptyset \Leftrightarrow mcd(a,b) = 1$ i $mcd(a,c) = 1$ □

Exercici 19. *Suposem 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. $mcd(p^2, a) = p^2$.

Solució:

$a \Rightarrow b)$ $p^2 \mid a \Rightarrow \exists r\ enter\ a = rp^2 \Rightarrow a^2 = r^2p^4 \Rightarrow p^4 \mid a^2$.

$b \Rightarrow c)$ $p^4 \mid a^2 \Rightarrow [p^3 \mid p^4\ i\ transitivitat] \Rightarrow p^3 \mid a^2$.

$c \Rightarrow d)$ $p^3 \mid a^2 \Rightarrow [p \mid p^3\ i\ transitivitat] \Rightarrow p \mid a^2 \Rightarrow [p\ primer\ i\ lema\ Euclides]$

$p \mid a \Rightarrow \exists k\ enter\ a = kp \Rightarrow a^2 = k^2p^2$. **(1)**

D'altra banda, $p^3 \mid a^2 \Rightarrow \exists r\ enter\ a^2 = rp^3$. **(2)**

Combinant **(1)** i **(2)**: $k^2p^2 = rp^3 \Rightarrow k^2 = rp \Rightarrow p \mid k^2$

$\Rightarrow [p\ primer, lem.\ d'Eucl.]\quad p \mid k \quad \Rightarrow \quad \exists t\ enter\ \ k = tp \quad \Rightarrow \quad a = kp = tp^2$

$\Rightarrow [p^2 \mid a]\quad mcd(p^2, a) = p^2$.

$d \Rightarrow a)$ evident donat que $mcd(p^2, a) = p^2$ és divisor de a . □

Exercici 20. *Trobeu tots els divisors de* 600 *.*

Solució: $600 = 6 \cdot 100 = 2 \cdot 3 \cdot 10^2 = 2 \cdot 3 \cdot (2 \cdot 5)^2 = 2^3 \cdot 3 \cdot 5^2.$

Els divisors positius de 600 són de la forma $2^r \cdot 3^s \cdot 5^t,$ amb $0 \le r \le 3,$ $0 \le s \le 1$, $0 \le t \le 2$. La llista dels 24 divisors positius de 600 és doncs:

1	2	2^2	2^3
$3 \cdot 1$	$3 \cdot 2$	$3 \cdot 2^2$	$3 \cdot 2^3$
$5 \cdot 1$	$5 \cdot 2$	$5 \cdot 2^2$	$5 \cdot 2^3$
$5 \cdot 3 \cdot 1$	$5 \cdot 3 \cdot 2$	$5 \cdot 3 \cdot 2^2$	$5 \cdot 3 \cdot 2^3$
$5^2 \cdot 1$	$5^2 \cdot 2$	$5^2 \cdot 2^2$	$5^2 \cdot 2^3$
$5^2 \cdot 3 \cdot 1$	$5^2 \cdot 3 \cdot 2$	$5^2 \cdot 3 \cdot 2^2$	$5^2 \cdot 3 \cdot 2^3$

Ara cal afegir els 24 divisors negatius de $600,$ que són els nombres de la llista anterior amb signe negatiu. En total, 48 divisors té 600 .

Exercici 21. *Si* $mcd(a, b) = p$ *, on* p *és primer, raoneu i justifiqueu quins són els possibles valors de:*

1. $mcd(a^2, b)$.
2. $mcd(a^3, b)$.
3. $mcd(a^2, b^3)$.

Solució: Com que $mcd(a, b) = p$, p és l'únic divisor primer comú de a i de b i exactament un dels dos nombres $a \ o \ b$ té en la seva descomposició factorial p i no p^2 . Farem dos casos, (1) a conté p i no p^2 i (2) b conté p i no p^2 .

Per raonar sobre mcd de potències de a i b ens anirà bé escriure-l's així:

(1) $a = \varepsilon_1 p \cdot A,$ *amb* p, A *primers entre si,* $b = \varepsilon_2 p^f \cdot B,$ *amb* p, B *primers entre si,* A, B *primers entre si, junt amb* $f \ge 1$ *, i* $\varepsilon_1, \varepsilon_2 = \pm 1.$

Llavors, en general, $mcd(a^n, b^m) = mcd(\ \varepsilon_1{}^n p^n \cdot A^n\ , \varepsilon_2{}^m p^{\,mf} \cdot B^m\ ) = p^{min\{n, mf\}}$.

Per tant:

a. $mcd(a^2, b) = mcd(p^2 \cdot A^2,\ \varepsilon_2 p^f \cdot B) = p^{min\{2, f\}}\ =$
   - $p,$ si $f = 1.$
   - $p^2,$ si $f \ge 2.$

b. $mcd(a^3, b) = mcd(\varepsilon_1 p^3 \cdot A^3,\ \varepsilon_2 p^f \cdot B) = p^{min\{3,f\}} =$
   - p, si $f = 1$.
   - p^2, si $f = 2$.
   - p^3, si $f \geq 3$.

c. $mcd(a^2, b^3) = mcd(p^2 \cdot A^2,\ \varepsilon_2 p^{3f} \cdot B^3 = p^{min\{2,3f\}} =$
   - p^2, en qualsevol cas, donat que $f \geq 1$ *i* $3f \geq 3$.

(2) $a = \varepsilon_1 p^f \cdot A$, *amb* p, A *primers entre si,* $b = \varepsilon_2 p \cdot B$, *amb* p, B *primers entre si,* A, B *primers entre si, junt amb* $f \geq 1$, *i* $\varepsilon_1, \varepsilon_2 = \pm 1$.
Llavors, en general, $mcd(a^n, b^m) = mcd(\ \varepsilon_1{}^n p^{nf} \cdot A^n\ , \varepsilon_2{}^m p^m \cdot B^m\ ) = p^{min\{nf,m\}}$.
Per tant:

a. $mcd(a^2, b) = mcd(p^{2f} \cdot A^2,\ \varepsilon_2 p \cdot B) = p^{min\{2f,1\}} = p.$
b. $mcd(a^3, b) = mcd(\varepsilon_1 p^{3f} \cdot A^3,\ \varepsilon_2 p \cdot B) = p^{min\{3f,1\}} = p.$
c. $mcd(a^2, b^3) = mcd(p^{2f} \cdot A^2,\ \varepsilon_2 p^3 \cdot B^3 = p^{min\{2f,3\}} =$
   - p^2, si $f = 1$.
   - p^3, si $f \geq 2$.

Exercici 22. *Si* $mcd(a, b) = p^3$, *on* p *és primer, calculeu* $mcd(a^2, b^2)$.
Solució: com a l'exercici anterior (ara no cal fer dos casos, donat que $mcd(a^2, b^2)$ és simètric en a, b).
Escrivim: $a = \varepsilon_1 p^3 \cdot A$, amb p, A primers entre si, $b = \varepsilon_2 p^f \cdot B$, amb p, B primers entre si, A, B primers entre si, junt amb $f \geq 3$, i $\varepsilon_1, \varepsilon_2 = \pm 1$.
Llavors:
$mcd(a^2, b^2) = mcd(\ p^6 \cdot A^2\ , p^{2f} \cdot B^2\ ) = p^{min\{6,2f\}} = p^6$ donat que $2f \geq 6$.

Exercici 23. *Tenim* 1000 *rajoles quadrades. De quantes maneres es poden disposar de manera que formin un rectangle?*
Solució: Com que $1000 = (2 \cdot 5)^3 = 2^3 \cdot 5^3$, 1000 té $(3 + 1)(3 + 1) = 16$ divisors positius. Per tant hi ha 16 maneres de disposar-les formant un rectangle: hi ha 16 maneres de triar la base i un cop triada la base l'altura queda determinada. Aquí interpretem que els rectangles $10 \cdot 100$ i $100 \cdot 10$ són diferents.

Exercici 24. *Digueu si les equacions diofàntiques següents tenen solució. Si en tenen, trobeu totes les solucions.*

$$20x+8y=6,\qquad 20x+8y=12,\qquad 20x-8y=12,$$
$$-20x+8y=12,\qquad -20x-8y=12.$$

Solució: Com que $mcd(20,8)=mcd(2^2\cdot 5,2^3)=2^2$ i 4 no divideix 6, la primera equació no té solució. En canvi, com que 4 divideix 12 les altres quatre equacions tenen solució. Ara resoldrem la segona de dues maneres diferents. La primera forma és millor, però només es pot aplicar amb valors "petits". Simplificant l'equació, queda: $5x+2y=3$,
i en aquest cas ens adonem que $5-3=2$ i tenim solució particular fent $x=1, y=-1$. Aplicant la fórmula de la solució general i donat que $mcd(5,2)=1$, totes les solucions són de la forma: $x=1-\frac{2}{1}t$, $y=-1+\frac{5}{1}t$ amb t enter. És a dir:

$$x=1-2t,\ y=-1+5t,\qquad t\in\mathbb{Z}.$$

Ara la resolem pel mètode general. És el que funciona sempre i hem d'aplicar per a valors "alts". Primer executem Euclides i Bézout amb entrada $20,8$:

x	1	0	1	
y	0	1	-2	
q		2		
r	20	8	4	0

Per tant, una identitat de Bézout per la parella $20,8$ és:

$$20(1)+8(-2)=4.$$

Multiplicant-la per 3 queda:

$$20(3)+8(-6)=12,$$

i per tant $x=3$, $y=-6$ és una solució de l'equació. Aplicant la mateixa fórmula que abans, la solució general quedarà ara:

$$x=3-2t,\ y=-6+5t,\qquad t\in\mathbb{Z}.$$

Un cop resolta la segona equació, les altres tres es resolen canviant signes a la primera.

Ho fem per a la tercera: si escrivim $20x-8y=12$ com $20x+8(-y)=12$, tenim que: (x,y) és solució de $20x-8y=12$ $\Leftrightarrow$ $(x,-y)$ és solució de $20x+8y=12$. per tant les solucions de la tercera equació s'obtenen canviant el signe de la y a les solucions de la segona:

$$x = 1 - 2t,\ y = 1 - 5t, \qquad t \in \mathbb{Z}\ .$$

Anàlogament, les solucions de la cuarta s'obtenen canviant el signe de la x:

$$x = -1 + 2t,\ y = -1 + 5t, \qquad t \in \mathbb{Z}\ .$$

i les solucions de la cinquena canviant el signe de la x i de la y:

$$x = -1 + 2t,\ y = 1 - 5t, \qquad t \in \mathbb{Z}\ .$$

Nota. Encara que l'exercici no ho demana, és fàcil verificar la solució substituint a l'equació. Ho fem amb la primera:

$$20x + 8y = 20(1 - 2t) + 8(-1 + 5t) = 12 - 40t + 40t = 12\ .$$

Amb això hem comprovat que tots els nombres de la forma $x = 1 - 2t$, $y = -1 + 5t$ són solució de l'equació. Per estar segurs que no ens deixem cap solució cal verificar que els coeficients de t són primers entre si: $mcd(-2, 5) = 1$.

Exercici 25. *Trobeu la solució (x, y) de les equacions anteriors que tingui la x positiva mínima.*

Solució: Usant les solucions de la segona equació trobada a l'exercici anterior:
Si ho fem amb la primera solució:

$$x = 1 - 2t,\ y = -1 + 5t,\ \ t \in \mathbb{Z}$$

ja es veu que és 1: correspon al valor $t = 0$ i els altres li sumem ± 2. Aquesta solució és justament la particular ha haviem trobat a ull.
En aquest cas per la forma de les equacions és molt fàcil. Si ho féssim amb la segona expressió de la solució:

$$x = 3 - 2t,\ y = -6 + 5t, \qquad t \in \mathbb{Z}\ .$$

Podem fer $x > 0 \Leftrightarrow 3 - 2t > 0 \Leftrightarrow 3 > 2t \Leftrightarrow \frac{3}{2} > t \Leftrightarrow t < 1.5 \Leftrightarrow t \leq 1$.
Si volem $x = 1 - 2t$ mínima , hem de fer t màxima. La màxima $t \leq 1$ és $t = 1$ i la solució és $x = 1,\ y = -1$.

Exercici 26. *Descomponeu de totes les maneres possibles la fracció $230/247$ en suma de dues fraccions positives de denominadors 19 i 13.*

Solució: Busquem enters x, y positius tals que $\frac{x}{19} + \frac{y}{13} = \frac{230}{247}$. Traient denominadors, l'equació queda:

$$13x + 19y = 230\ .$$

Fixem-nos que volem les solucions enteres positives de l'equació $230 = 13x + 19y$, per tant la tractem com una equació diofàntica.
Primer observem que els coeficients són primers entre si, ja que són dos

nombres primers diferents. Per tal de trobar una solució particular executem Euclides estès:

	1	0	1	-2	
	0	1	-1	3	
q		1	2		
r	19	13	6	1	0

$$13(3)+19(-2)=1$$

Multiplicant per 230:

$$13(3\cdot 230)+19(-2\cdot 230)=230\,.$$

Així $x=690$, $y=-460$ és una solució de l'equació. Usant la fórmula de la solució general:

$$x=690-19t,\ y=-460+13t,\qquad t\in\mathbb{Z}\ .$$

Encara que no és necessari, és aconsellable verificar la solució abans de seguir:

$13x+19y=13(690-19t)+19(-460+13t)=13\cdot 690-19\cdot 460-13\cdot 19\,t+19\cdot 13\,t=230$.

Ara imposem que tant x com y siguin positives:

$x>0 \iff 690-19t>0 \iff 690>19t \iff \frac{690}{19}>t \iff t<36,3.. \iff t\le 36$.

$y>0 \iff -460+13t>0 \iff 13t>460 \iff t>\frac{460}{13}\approx 35,4 \iff t\ge 36$.

Tot plegat, veiem que hi ha una única solució, que correspon a $t=36$ $x=690-19\cdot 36=6$, $y=-460+13\cdot 36=8$. L'única manera de descomposar la fracció és:

$$\frac{6}{19}+\frac{8}{13}=\frac{230}{247}\,.$$

Exercici 27. *Calculeu totes les parelles possibles de nombres enters (incloent negatius!) que tenen màxim comú divisor 5 i mínim comú múltiple 70.*

Solució: Denotem aquestes parelles per (x,y). Com que $mcd(x,y)=5$ tenim que 5 divideix x,y i si posem $(x,y)=(5x',5y')$ queda $mcd(x',y')=1$. Així, com que $70=2\cdot 5\cdot 7$, $x'y'=mcm(x',y')=14$. Les possibles parelles positives de (x',y') són $(1,14)$, $(2,7)$, $(7,2)$ i $(14,1)$. Cada una d'aquestes parelles dóna quatre parelles de (x,y) canviant signe, en total hi ha 16 parelles: $(\pm 5,\pm 70)$, $(\pm 35,\pm 10)$, $(\pm 10,\pm 35)$, $(\pm 70,\pm 5)$.

Exercici 28. *Demostreu que, per a qualssevol enters* $a, b,$ *no nuls es té:*

$mcm(a,b) = |ab|$ *si i només si* a *i* b *són primers entre si.*

Solució: Usarem la fórmula $mcd(a.b)\cdot mcm(a,b) = |ab|$ i que $|ab| \neq 0$:

$\Rightarrow$) Si $mcm(a,b) = |ab|$, substituint a la fórmula tenim $mcd(a,b)\cdot|ab| = |ab|$. Com que $|ab| \neq 0$, simplificant tenim $mcd(a,b) = 1$.

$\Leftarrow$) Si $mcd(a,b) = 1$, substituint a la fórmula queda $mcm(a,b) = |ab|$. □

Exercici 29. *Demostreu que si* a, b *són primers entre si i* $a \mid c,\ b \mid c$ *llavors* $ab \mid c$.

Solució: Si a, b primers entre si $\Rightarrow$ $mcd(a,b) = 1$. Substituint a $mcd(a,b)\ mcm(a,b) = |ab|$ queda $mcm(a,b) = |ab|$. Usant el fet que tot múltiple comú de a i b és múltiple de $mcm(a,b)$, $a \mid c,\ b \mid c \Rightarrow |ab| \mid c$ $\Rightarrow [x \mid y \text{ no depèn del signe}]$ $ab \mid c$. □

Tema 6: CONGRUÈNCIES

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

Solució: Abans que res, observem que:

$8^{n+1} - 8 - 56n$ és múltiple de $392 \Leftrightarrow 8^{n+1} - 8 - 56n \equiv 0\ (m\grave{o}d\ 392)$

$\Leftrightarrow [simplif.\ per\ 8]\ \ 8^n - 1 - 7n \equiv 0\ (m\grave{o}d\ 49) \Leftrightarrow 8^n \equiv 1 + 7n\ (m\grave{o}d\ 49)$.

Demostrem per inducció que per a tot $n \geq 0$: $8^n \equiv 1 + 7n\ (m\grave{o}d\ 49)$.

- Pas bàsic: $8^0 \equiv 1 + 7\cdot 0\ (m\grave{o}d\ 49)$, cert, ja que és $1 \equiv 1(m\grave{o}d\ 49)$.
- Pas inductiu: Sigui $n > 0$:
  - Hipòtesi d'inducció: $8^{n-1} \equiv 1 + 7(n-1)\ (m\grave{o}d\ 49)$.
  - Tesi: $8^n \equiv 1 + 7n\ (m\grave{o}d\ 49)$.

En efecte: $8^n \equiv 8\cdot 8^{n-1} \equiv [H.I.]\ 8(1 + 7(n-1)) \equiv 1 + 7n\ \ (m\grave{o}d\ 49)$. □

Exercici 2. *Demostreu:* $ka \equiv kb \ (\text{mòd } m) \ \Leftrightarrow \ a \equiv b \ (\text{ mòd } \ m/mcd(k,m))$ **.**
Solució: Posem $d = mcd(k,m)$. Llavors $ka \equiv kb \ (\text{mòd } m) \ \Leftrightarrow [simplif. per\ d]$ $\frac{k}{d}\, a \equiv \frac{k}{d}\, b \ (\text{ mòd } \ m/d) \ \Leftrightarrow [simplif. per\ \frac{k}{d},\ mcd(\frac{k}{d}, \frac{m}{d}) = 1] \ \ a \equiv b \ (\text{ mòd } \ m/d)$ **.**

Exercici 3. *Demostreu:* $ac \equiv bc \ (\text{mòd } m) \ \Rightarrow \ a^n c \equiv b^n c \ (\text{mòd } m) \ \ (n \geq 1)$.
Solució: En donarem dues demostracions.
1a Demo: Per inducció sobre n.

- Pas bàsic: $ac \equiv bc \ (\text{mòd } m)$ és la hipòtesi.
- Pas inductiu: Sigui $n > 1$:
  - Hipòtesi d'inducció: $a^{n-1}c \equiv b^{n-1}c \ (\text{mòd } m)$
  - Tesi: $a^n c \equiv b^n c \ (\text{mòd } m)$

En efecte, $a^n c \equiv aa^{n-1}c \equiv [H.I.]\ ab^{n-1}c \equiv acb^{n-1} \equiv [hipòtesi]\ bcb^{n-1} \equiv b^n c \ (\text{mòd } m)$. □
2a Demo: Fem servir la fórmula:

$$a^n - b^n = (a-b)(a^{n-1} + a^{n-2}b + \cdots + ab^{n-2} + b^{n-1}).$$

De la hipòtesi $ac \equiv bc \ (\text{mòd } m)$ deduïm que $m \mid ac - bc = (a-b)c$. La fórmula diu que $(a-b) \mid (a^n - b^n)$ i multiplicant per c: $(a-b)\, c \mid (a^n - b^n)c$. Per transitivitat: $m \mid (a^n - b^n)c = a^n c - b^n c$ i per tant $a^n c \equiv b^n c \ (\text{mòd } m)$. □

Exercici 4. *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)*
Solució: En termes de congruències hem de demostrar que $2 \cdot 5^{2n+1} + 8 \cdot 7^n \equiv 0 \ (\text{mòd } 18)$. Això és equivalent a $2 \cdot 5^{2n+1} \equiv -\, 8 \cdot 7^n \ (\text{ mòd } 18)$ o també, simplificant per 2: $5^{2n+1} \equiv -\, 4 \cdot 7^n \ (\text{ mòd } 9)$ per a tot $n \geq 0$. Això últim ho fem per inducció sobre n.

- Pas bàsic: $5^1 \equiv -\, 4 \cdot 7^0 \ (\text{mòd } 9)$, cert ja que $9 \mid 9$.
- Pas inductiu: Sigui $n > 0$:
  - Hipòtesi d'inducció: $5^{2n-1} \equiv -\, 4 \cdot 7^{n-1} \ (\text{mòd } 9)$
  - Tesi: $5^{2n+1} \equiv -\, 4 \cdot 7^n \ (\text{mòd } 9)$

En efecte, $5^{2n+1} \equiv 5^2 5^{2n-1} \equiv 25(-\, 4 \cdot 7^{n-1}) \equiv 7(-\, 4 \cdot 7^{n-1}) \equiv -\, 4 \cdot 7^n \ (\text{mòd } 9)$.

Exercici 5. *Demostreu les propietats associativa de la suma i distributiva del producte respecte de la suma a* $\mathbb{Z}_m$ *.*

Solució: *Associativa de la suma*: $(\overline{a}+\overline{b})+\overline{c}=\overline{a}+(\overline{b}+\overline{c})$.

En efecte: $(\overline{a}+\overline{b})+\overline{c}=[def.\ suma\ classes]\ \overline{a+b}+\overline{c}=[def.\ suma\ classes]$

$\overline{(a+b)+c}=[assoc.\ suma\ enters]\ \overline{a+(b+c)}=[def.\ suma\ classes]$

$\overline{a}+\overline{b+c}=[def.\ suma\ classes]\ \overline{a}+(\overline{b}+\overline{c}).$ □

Distributiva del producte respecte de la suma: $\overline{a}\cdot(\overline{b}+\overline{c})=\overline{a}\cdot\overline{b}+\overline{a}\cdot\overline{c}$

En efecte: $\overline{a}\cdot(\overline{b}+\overline{c})=[def.\ suma\ classes]\ \overline{a}\cdot\overline{b+c}=[def.\ prod.\ classes]$

$\overline{a\cdot(b+c)}=[distrib.\ amb\ enters]\ \overline{a\cdot b+a\cdot c}=[def.\ suma\ classes]$

$\overline{a\cdot b}+\overline{a\cdot c}=[def.\ prod.\ classes]\ \overline{a}\cdot\overline{b}+\overline{a}\cdot\overline{c}.$ □

Exercici 6. *Demostreu per inducció que* $\overline{a}^{\,n}=\overline{a^n}$ *per a tot* $n\geq 1$ *.*

Solució: Abans que res, diem que $\overline{a}^{\,n}=\overline{a}\cdot\ldots\cdot\overline{a}$ (producte de n classes).

- Pas bàsic: $\overline{a}^{1}=\overline{a^1}$ cert, ja que ambdós costats valen $\overline{a}$.
- Pas inductiu: Sigui $n>1$:
  - Hipòtesi d'inducció: $\overline{a}^{\,n-1}=\overline{a^{n-1}}.$
  - Tesi: $\overline{a}^{\,n}=\overline{a^n}$.

En efecte: $\overline{a}^{\,n}=\overline{a}\cdot\ldots\cdot\overline{a}=[assoc.\ prod.\ classes]\ \overline{a}^{\,n-1}\cdot\overline{a}=$

$[hip.\ inducció]\ \overline{a^{n-1}}\cdot\overline{a}=[def.\ prod.\ classes]=\overline{a^{n-1}\cdot a}=\overline{a^n}.$ □

Exercici 7. *Demostreu que per a tot* $n\geq 0$ 19^n+3^{2n+2} *acaba en* 0 *usant classes modulars.*

Solució: es té: 19^n+3^{2n+2} *acaba en* $0 \Leftrightarrow 19^n+3^{2n+2}$ *és múltiple de* $10 \Leftrightarrow$

$\overline{19^n+3^{2n+2}}=\overline{0}$ *a* $\mathbb{Z}_{10}$.

Procedim: $\overline{19^n+3^{2n+2}}=\overline{19^n}+\overline{3^{2n+2}}=\overline{19}^{\,n}+\overline{3}^{\,2n+2}=\overline{9}^{\,n}+\overline{3}^{\,2n}\cdot\overline{3}^{\,2}=$

$\overline{9}^{\,n}+\overline{9}^{\,n}\cdot\overline{9}=\overline{9}^{\,n}\cdot(\overline{1}+\overline{9})=\overline{9}^{\,n}\cdot\overline{10}=\overline{9}^{\,n}\cdot\overline{0}=\overline{0}.$ □

Exercici 8. *Demostreu que* n *és congruent mòdul* 3 *amb la suma dels seus dígits.*

Solució: Si $a_k a_{k-1}...a_1 a_0$ és l'expressió en base 10 de n, veiem que $n \equiv \sum_{i=0}^{k} a_i \ (m\grave{o}d\ 3)$.

En efecte: com que $n = a_k 10^k + a_{k-1}10^{k-1} + ... + a_1 10 + a_0$, prenent classes a $\mathbb{Z}_3$ es té: $\overline{n} = \overline{a_k 10^k + a_{k-1}10^{k-1} + ... + a_1 10 + a_0} =$

$\overline{a_k}\cdot\overline{10}^k + \overline{a_{k-1}}\cdot\overline{10}^{k-1} + ... + \overline{a_1}\cdot\overline{10} + \overline{a_0} = \overline{a_k}\cdot\overline{1}^k + \overline{a_{k-1}}\cdot\overline{1}^{k-1} + ... + \overline{a_1}\cdot\overline{1} + \overline{a_0} =$

$\overline{a_k} + \overline{a_{k-1}} + ... + \overline{a_1} + \overline{a_0} = \overline{a_k + a_{k-1} + ... + a_1 + a_0} = \overline{\sum_{i=0}^{k} a_i}.$

Per tant, hem demostrat que $n \equiv \sum_{i=0}^{k} a_i \ (m\grave{o}d\ 3)$, i aquest resultat ens dóna el criteri de divisibilitat per 3: n és múltiple de 3 si i només si la suma dels seus dígits és múltiple de 3. □

Exercici 9. *Demostreu el criteri de divisibilitat per 11: n és múltiple de 11 sii la suma dels dígits de n que ocupen un lloc parell menys la suma dels que ocupen un lloc senar és múltiple de 11.*

Solució: Demostrarem que si $a_k a_{k-1}...a_1 a_0$ és l'expressió en base 10 de n, llavors $n \equiv (a_0 + a_2 + a_4 + \cdots) - (a_1 + a_3 + a_5 + \cdots)\ (m\grave{o}d\ 11)$. Igual que a l'exercici 4, això implica el criteri de divisibilitat.

En efecte. De $n = a_k 10^k + a_{k-1}10^{k-1} + ... + a_1 10 + a_0$, prenent classes a $\mathbb{Z}_{11}$ es té: $\overline{n} = \overline{a_k 10^k + a_{k-1}10^{k-1} + ... + a_1 10 + a_0} =$

$\overline{a_k}\cdot\overline{10}^k + \overline{a_{k-1}}\cdot\overline{10}^{k-1} + ... + \overline{a_1}\cdot\overline{10} + \overline{a_0} = \overline{a_k}\cdot\overline{-1}^k + \overline{a_{k-1}}\cdot\overline{-1}^{k-1} + ... + \overline{a_1}\cdot\overline{-1} + \overline{a_0} =$

$= \overline{a_k}\cdot\overline{(-1)^k} + \overline{a_{k-1}}\cdot\overline{(-1)^{k-1}} + ... + \overline{a_1}\cdot\overline{-1} + \overline{a_0} =$

$\overline{a_k(-1)^k + a_{k-1}(-1)^{k-1} + ... + a_2 - a_1 + a_0} = \overline{(a_0 + a_2 + a_4 + \cdots) - (a_1 + a_3 + a_5 + \cdots)}$

□

Exercici 10. *Proveu que no hi ha cap n tal que $5n + 3$ és un quadrat.*

Solució: Ho farem per RA. Suposem que existeix un enter n tal que $5n + 3 = t^2$ per a un cert enter t. Prenem classes a $\mathbb{Z}_5$*:*

$\overline{5n + 3} = \overline{5}\cdot\overline{n} + \overline{3} = \overline{0} + \overline{3} = \overline{3} = \overline{t^2} = \overline{t}^2 \ \Rightarrow\ \overline{t}^2 = \overline{3}$, i això és un absurd, perquè no hi ha cap classe a $\mathbb{Z}_5 = \{\overline{0}, \overline{1}, \overline{2}.\overline{3}, \overline{4}\}$ tal que el seu quadrat val $\overline{3}$:

$\overline{0}^2 = \overline{0},\quad \overline{1}^2 = \overline{1},\quad \overline{2}^2 = \overline{4},\quad \overline{3}^2 = \overline{4},\quad \overline{4}^2 = \overline{1}.$ □

Exercici 11. *Calculeu, si en tenen, els inversos modulars de* $\overline{50}$ *i* $\overline{39}$ *a* $\mathbb{Z}_{1.210}$.
Solució: Com que tant 50 com 1.210 són múltiples de 10, no són primers entre si i per tant $\overline{50}$ no té invers $\mathbb{Z}_{1.210}$. Si fem Euclides estès amb 1.210 i 39 obtenim:

y	0	1	-31	
q		31	5	
r	1.210	39	1	0

Per tant, l'invers de $\overline{39}$ és $\overline{-31}$. De manera equivalent: $\overline{39}^{-1} = \overline{-31} = \overline{1.179}$ a $\mathbb{Z}_{1.210}$.

Exercici 12. *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* $\mathbb{Z}_{11}$.
Solució: la segona equació $\overline{3}\overline{x} + \overline{3}\overline{y} = \overline{y} + \overline{16}$ és equivalent a $\overline{3}\overline{x} + \overline{2}\overline{y} = \overline{5}.$
Escrivim: (1) $\overline{4}\overline{x} + \overline{7}\overline{y} = \overline{0}$ i (2) $\overline{3}\overline{x} + \overline{2}\overline{y} = \overline{5}.$
Fem $\overline{3}\cdot(1) - \overline{4}\cdot(2)$: $(\overline{21} - \overline{8})\cdot\overline{y} = \overline{-20} \Rightarrow \overline{2}\cdot\overline{y} = \overline{2} \Rightarrow \overline{y} = \overline{2}^{-1}\cdot\overline{2} = \overline{1}.$
I ara: $\overline{3}\overline{x} + \overline{2}\overline{y} = \overline{5} \Rightarrow \overline{3}\overline{x} + \overline{2}\cdot\overline{1} = \overline{5} \Rightarrow \overline{3}\cdot\overline{x} = \overline{3} \Rightarrow \overline{x} = \overline{1}.$
Hem fet implicacions $\Rightarrow$, falta doncs $\Leftarrow$, és a dir, comprovar la solució:
$\overline{4}\,\overline{1} + \overline{7}\,\overline{1} = \overline{22}$, $\overline{3}\,\overline{1} + \overline{3}\,\overline{1} = \overline{1} + \overline{16},$ totes dues certes.

Exercici 13. *Resoleu les congruències següents:*

a. $3x \equiv 5\ (mod\ 8)$.
b. $2x \equiv 4\ (mod\ 8)$.
c. $6x \equiv 4\ (mod\ 8)$.
d. $2x \equiv 5\ (mod\ 8)$.

Solució:

a. Treballant a $\mathbb{Z}_8$ tenim: $3x \equiv 5\ (mod\ 8) \Leftrightarrow \overline{3}\cdot\overline{x} = \overline{5}$ $\Leftrightarrow [\Rightarrow Mult.\ per\ \overline{3}^{-1}, \Leftarrow Mult.\ per\ \overline{3}]$ $\overline{x} = \overline{3}\cdot\overline{5} = \overline{15} = \overline{7}$. Aquí hem usat que $\overline{3}\cdot\overline{3} = \overline{9} = \overline{1}$, i per tant l'invers de $\overline{3}$ és $\overline{3}$. Així, totes les solucions són de la forma $x = 7 + 8t$ amb $t \in \mathbb{Z}$.
b. Simplificant per 2 tenim: $2x \equiv 4\ (mod\ 8) \Leftrightarrow x \equiv 2\ (mod\ 4)$. Així, totes

les solucions son de la forma $x = 2 + 4t$ amb $t \in \mathbb{Z}$.

c. Simplificant per 2 tenim: $6x \equiv 4\ (mod\ 8) \Leftrightarrow 3x \equiv 2\ (mod\ 4)$. Treballant a $\mathbb{Z}_4$ tenim $3x \equiv 2\ (mod\ 4) \Leftrightarrow \overline{3}\cdot\overline{x} = \overline{2}$ $\Leftrightarrow [\Rightarrow Mult.\ per\ \overline{3}^{-1}, \Leftarrow Mult.\ per\ \overline{3}]$ $\overline{x} = \overline{3}\cdot\overline{2} = \overline{6} = \overline{2}$. Aquí hem usat que $\overline{3}\cdot\overline{3} = \overline{9} = \overline{1}$, i per tant l'invers de $\overline{3}$ és $\overline{3}$ a $\mathbb{Z}_4$. Així, totes les solucions són de la forma $x = 2 + 4t$ amb $t \in \mathbb{Z}$.

d. Existeix x tal que $2x \equiv 5\ (mod\ 8) \Leftrightarrow$ existeixen x, y tals que $2x - 5 \equiv 8y \Leftrightarrow 2x - 8y \equiv 5$ té solució. Com que $mcd(2,8) = 2$ no divideix 5, $2x - 8y \equiv 5$ no té solució i per tant $2x \equiv 5\ (mod\ 8)$ tampoc.

Exercici 14. *Demostreu que el producte de dues classes invertibles de $\mathbb{Z}_m$ és invertible. Qui és l'invers del producte?*

Solució: siguin $\overline{a},\ \overline{b} \in \mathbb{Z}_m$ invertibles, és a dir, existeixen $\overline{c},\ \overline{d} \in \mathbb{Z}_m$ tals que $\overline{a}\cdot\overline{c} = \overline{b}\cdot\overline{d} = \overline{1}$. Del producte $(\overline{a}\cdot\overline{b})\cdot(\overline{c}\cdot\overline{d}) = (\overline{a}\cdot\overline{c})\cdot(\overline{b}\cdot\overline{d}) = \overline{1}\cdot\overline{1} = \overline{1}$ deduïm que $\overline{a}\cdot\overline{b}$ és invertible i la seva inversa és $\overline{c}\cdot\overline{d}$. O sigui: $(\overline{a}\cdot\overline{b})^{-1} = \overline{a}^{-1}\cdot\overline{b}^{-1}$. □

Exercici 15. *Demostreu que per a tota classe $\overline{a}$ de $\mathbb{Z}_m$ són equivalents:*

a. $mcd(a,m) = 1$

b. $\overline{a}\cdot\overline{b} = \overline{a}\cdot\overline{c} \Rightarrow \overline{b} = \overline{c}$ (podem "simplificar" per $\overline{a}$)

c. No existeix $\overline{d} \neq \overline{0}$ tal que $\overline{a}\cdot\overline{d} = \overline{0}$.

Solució:

a ⇒ b). Suposem que $mcd(a,m) = 1$. Llavors $\overline{a}$ té invers a $\mathbb{Z}_m$. Si $\overline{a}\cdot\overline{b} = \overline{a}\cdot\overline{c}$ $\Rightarrow [Multip.\ per\ \overline{a}^{-1}]$ $\overline{a}^{-1}\overline{a}\cdot\overline{b} = \overline{a}^{-1}\overline{a}\cdot\overline{c} \Rightarrow \overline{b} = \overline{c}$. □

b ⇒ c). Per RA. Si existís $\overline{d} \neq \overline{0}$ tal que $\overline{a}\cdot\overline{d} = \overline{0}$, tindriem que $\overline{a}\cdot\overline{d} = \overline{a}\cdot\overline{0} \Rightarrow b)$ $\overline{d} = \overline{0}$, contradicció. □

c ⇒ a). Per contrarecíproc: Si $mcd(a,m) > 1$, hem de trobar $\overline{d} \neq \overline{0}$ tal que $\overline{a}\cdot\overline{d} = \overline{0}$. Prenem $d = m/mcd(a,m)$. Com que $mcd(a,m) > 1$, $0 < d < m$ i per tant $\overline{d} \neq \overline{0}$. Ara bé, $\overline{a}\cdot\overline{d} = \overline{a}\cdot\overline{m/mcd(a,m)} = \overline{a\cdot\frac{m}{mcd(a,m)}} = \overline{\frac{a}{mcd(a,m)}\cdot m} = \overline{\frac{a}{mcd(a,m)}}\cdot\overline{m} = \overline{\frac{a}{mcd(a,m)}}\cdot\overline{0} = \overline{0}$. □

Exercici 16. *Sigui $n \geq 1$. Demostreu si a, n són primers entre si, l'aplicació $f : \mathbb{Z}_n \to \mathbb{Z}_n$ donada per $f(\overline{x}) = \overline{a}\cdot\overline{x}$ és bijectiva i doneu la inversa.*

Solució: com que a, n són primers entre si, existeix $\overline{a}^{-1}$ i es té:

$$f(\overline{x}) = \overline{a}\cdot\overline{x} = \overline{y} \quad \Leftrightarrow \quad \overline{x} = \overline{a}^{-1}\cdot\overline{y}\,.$$

Per tant donat $\overline{y} \in \mathbb{Z}_n$ qualsevol, existeix un únic $\overline{x} \in \mathbb{Z}_n$ tal que $f(\overline{x}) = \overline{y}.$ Això significa que f és bijectiva, i, a més, la funció inversa ve donada per $f^{-1}(\overline{x}) = \overline{a}^{-1}\cdot\overline{x}.$ □

Exercici 17. Resoleu el sistema

$$x \equiv 2\ (\ mod\ 4)\,, \quad x \equiv 1\ (\ mod\ 6) \quad x \equiv 1\ (\ mod\ 7)\,.$$

Solució: busquem tots els enters x tals que $x = 2 + 4r = 1 + 6s = 1 + 7t,$ per a certs enters $r, s, t.$

$2 + 4r = 1 + 6s \ \Leftrightarrow\ 6s - 4r = 1,$ que no té solució donat que $mcd(6, 4) = 2$ no divideix $1.$ Per tant els sistema de congruències no té solució.

Exercici 18. Resoleu el sistema

$$x \equiv 1\ (\ mod\ 3),\quad x \equiv 3\ (\ mod\ 4),\quad x \equiv 4\ (\ mod\ 7\ ),\quad x \equiv 7\ (\ mod\ 11\ )\,.$$

Solució: Per trobar les solucions del sistema resoldrem successivament 3 equacions diofàntiques.

1. $x = 1 + 3r = 3 + 4s \Leftrightarrow 3r - 4s = 2$, que té solució donat que $3, 4$ són primers entre si. Una solució particular (a ull, tenim números petits) és $(r, s) = (2, 1),$ per tant $r = 2 + 4t,$ amb t enter. Així, tindrem $x = 1 + 3r = 7 + 12t.$
2. $x = 7 + 12t = 4 + 7u \ \Rightarrow\ 7u - 12t = 3$, que té solució donat que $7, 12$ són primers entre si. Una solució particular (a ull) és $(u, t) = (-3, -2),$ per tant $u = -3 + 12v,$ amb v enter. Així, tindrem $x = 4 + 7u = -17 + 84v.$
3. $x = -17 + 84v = 7 + 11w \ \Leftrightarrow\ 84v - 11w = 24$, que té solució donat que $84, 11$ són primers entre si. Aquí, una solució particular ve donada per la identitat de Bézout: $84\cdot(-3) - 11\cdot(-23) = 1.$
   Per tant: $84\cdot(-72) - 11\cdot(-552) = 24$, i $(v, w) = (-72, -552),$ és una solució particular, d'on $v = -72 + 11k,$ amb k enter. Així, tindrem $x = -17 + 84v = -17 + 84(-72 + 11k) = -6065 + 924k.$
4. Solució final del sistema de congruències: $x = -6065 + 924k,$ amb k un enter qualsevol. Alternativament ho podríem expressar així: $x \equiv 403\ (mod\ 924)\,.$

Exercici 19. 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?

Solució: Si x és el mínim nombre de monedes d'or, x és l'enter positiu més petit solució del sistema de congruències següent:

$$x \equiv 8 \ (mod\ 13), \quad x \equiv 3 \ (mod\ 11) \quad x \equiv 5 \ (mod\ 8).$$

Per trobar les solucions del sistema resoldrem successivament 2 equacions diofàntiques.

1. $x = 8 + 13r = 3 + 11s \Leftrightarrow 13r - 11s = -5$, que té solució donat que $13, 11$ són primers entre si. Una solució particular (a partir de Bézout) és $(r, s) = (25, 30)$, per tant $r = 25 + 11t$, amb t enter. Així, tindrem $x = 8 + 13r = 333 + 143t$.
2. $x = 333 + 143t = 5 + 8u \Leftrightarrow 8u - 143t = 328$, que té solució donat que $8, 143$ són primers entre si. Una solució particular (a partir de Bézout) és $(u, t) = (5904, 328)$, per tant $u = 5904 + 143v$, amb v enter. Així, tindrem $x = 5 + 8u = 5 + 8(5904 + 143v) = 47237 + 1144v$.
3. Solució final del sistema de congruències: $x = 47237 + 1144k$, amb k un enter qualsevol.
4. Es té $47237 = 1144 \cdot 41 + 333$, per tant el nombre de monedes d'or buscat és 333.

Exercici 20. Calculeu $3^{247} \ (mod\ 17)$.

Solució: com que 17 és primer, pel teorema petit de Fermat, es té $\overline{3}^{16} = \overline{1}$ a $\mathbb{Z}_{17}$, i tenim: $\overline{3}^{247} = \overline{3}^{16 \cdot 15 + 7} = (\overline{3}^{16})^{15} \cdot \overline{3}^{7} = \overline{1} \cdot \overline{3}^{7} = \overline{3}^{7} = \overline{2187} = \overline{11}$. Per tant $3^{247} \equiv 11 \ (mod\ 17)$.

Exercici 21. Calculeu $34773^{4969} \ (mod\ 151)$.

Solució: com que 151 és primer, i $\overline{34773} = \overline{43}$ a $\mathbb{Z}_{151}$, pel teorema petit de Fermat, es té $\overline{34773}^{150} = \overline{43}^{150} = \overline{1}$ a $\mathbb{Z}_{151}$, i tenim: $\overline{43}^{4969} = \overline{43}^{150 \cdot 33 + 19} = (\overline{43}^{150})^{33} \cdot \overline{43}^{19} = \overline{1} \cdot \overline{43}^{19} = \overline{43}^{19} = \overline{43^{19}} = \overline{36}$. Per tant

$34773^{4969} \equiv 36 \ (mod\ 151)$.

Exercici 22. Calculeu, usant Fermat i l'última propietat de les congruències: $11^{1234} \ (mod\ 14)$.

Solució: ara el mòdul $14 = 2 \cdot 7$ no és primer, per tant, per poder aplicar l'última propietat de les congruències, buscarem un enter k tal que $11^{1234} \equiv k \ (mod\ 2)$ i $11^{1234} \equiv k \ (mod\ 7)$, per poder concloure que $11^{1234} \equiv k \ (mod\ 14)$. Procedim:

1. $11^{1234} \equiv 1^{1234} \equiv 1 \ (mod\ 2)$.
2. $11^{1234} \equiv 4^{1234} \equiv 4^{6 \cdot 205+4} \equiv (4^6)^{205} \cdot 4^4 \equiv 1^{205} \cdot 4 \equiv 4 \ (mod\ 7)$.
3. Ara hem de trobar un k tal que $1 \equiv k \ (mod\ 2)$ i $4 \equiv k \ (mod\ 7)$, és a dir, $k = 1 + 2r = 4 + 7s$, que és una diofàntica. A ull veiem que podem prendre $k = 1 + 2 \cdot 5 = 4 + 7 \cdot 1 = 11$.
4. Final: tenim $11^{1234} \equiv 11 \ (mod\ 2)$ i $11^{1234} \equiv 11 \ (mod\ 7)$, per tant $11^{1234} \equiv 11 \ (mod\ \ mcm(2, 7) = 14)$, que és el que ens demanaven.

Exercici 23. Calculeu, usant Fermat i l'última propietat de les congruències: $1800^{1800} \ (mod\ 77)$.

Solució: el mòdul $77 = 7 \cdot 11$ no és primer, per tant, per poder aplicar l'última propietat de les congruències, trobarem un enter k tal que $1800^{1800} \equiv k \ (mod\ 7)$ i $1800^{1800} \equiv k \ (mod\ 11)$, per poder concloure que $1800^{1800} \equiv k \ (mod\ 77)$. Procedim:

1. $1800^{1800} \equiv 1^{1800} \equiv 1 \ (mod\ 7)$.
2. $1800^{1800} \equiv 7^{1800} \equiv 7^{10 \cdot 180} \equiv (7^{10})^{180} \equiv 1^{180} \equiv 1 \ (mod\ 11)$.
3. En aquest cas ja hem trobat $k = 1$. Tenim doncs: $1800^{1800} \equiv 1 \ (mod\ 7)$ i $1800^{1800} \equiv 1 \ (mod\ 11)$, per tant $1800^{1800} \equiv 1 \ (mod\ \ mcm(7, 11) = 77)$.

Exercici 24. Calculeu, usant Fermat i l'última propietat de les congruències: $12345^{12345} \ (mod\ 210)$.

Solució: el mòdul $210 = 2 \cdot 3 \cdot 5 \cdot 7$ no és primer, per tant, per poder aplicar l'última propietat de les congruències, buscarem un enter k tal que $12345^{12345} \equiv k \ (mod\ 2)$, $12345^{12345} \equiv k \ (mod\ 3)$, $12345^{12345} \equiv k \ (mod\ 5)$,

$12345^{12345} \equiv k \ (mod\ 7)$, per poder concloure que $12345^{12345} \equiv k \ (mod\ 210)$.
Procedim:

1. $12345^{12345} \equiv 1^{12345} \equiv 1 \ (mod\ 2)$.
2. $12345^{12345} \equiv 0^{12345} \equiv 0 \ (mod\ 3)$.
3. $12345^{12345} \equiv 0^{12345} \equiv 0 \ (mod\ 5)$.
4. $12345^{12345} \equiv 4^{12345} \equiv 4^{6\cdot 2057+3} \equiv (4^6)^{2057}\cdot 4^3 \equiv 1^{2057}\cdot 64 \equiv 1 \ (mod\ 7)$.
5. Ara hem de trobar un k tal que $1 \equiv k \ (mod\ 2)$, $0 \equiv k \ (mod\ 3)$, $0 \equiv k \ (mod\ 5)$, $1 \equiv k \ (mod\ 7)$.
   Agrupem: $1 \equiv k \ (mod\ 2), 1 \equiv k \ (mod\ 7) \Leftrightarrow 1 \equiv k \ (mod\ 14)$ i $0 \equiv k \ (mod\ 3), 0 \equiv k \ (mod\ 5) \Leftrightarrow 0 \equiv k \ (mod\ 15)$.
   Tindrem: $k = 1 + 14r = 15s$, que és una diofàntica. A ull veiem que podem prendre $k = 1 + 14\cdot 1 = 15\cdot 1 = 15$.
6. Final: tenim $12345^{12345} \equiv 15 \ (mod\ 2)$, $12345^{12345} \equiv 15 \ (mod\ 3)$, $12345^{12345} \equiv 15 \ (mod\ 5)$, $12345^{12345} \equiv 15 \ (mod\ 7)$, per tant: $12345^{12345} \equiv 15 \ (mod\ mcm(2,3,5,7) = 210)$, que és el que ens demanaven.

Exercici 25. Demostreu que per tot a, $\overline{a}^{17} = \overline{a}$ a $\mathbb{Z}_{255}$ (Pista: useu Fermat i l'última propietat de les congruències).
Solució: Factoritzant 255 es té $255 = 3\cdot 5\cdot 17$, i aplicarem Fermat amb 3 mòduls diferent:

1. A $\mathbb{Z}_3$, per Fermat: $\overline{a} \neq \overline{0} \Rightarrow \overline{a}^2 = \overline{1} \Rightarrow \overline{a}^{16} = \overline{1} \Rightarrow \overline{a}^{17} = \overline{a}$.
2. A $\mathbb{Z}_5$, per Fermat: $\overline{a} \neq \overline{0} \Rightarrow \overline{a}^4 = \overline{1} \Rightarrow \overline{a}^{16} = \overline{1} \Rightarrow \overline{a}^{17} = \overline{a}$.
3. A $\mathbb{Z}_{17}$, per Fermat: $\overline{a} \neq \overline{0} \Rightarrow \overline{a}^{16} = \overline{1} \Rightarrow \overline{a}^{17} = \overline{a}$.
   Per tant, per l'última propietat de les congruències en termes de classes de residus: $\overline{a}^{17} = \overline{a}$ a $\mathbb{Z}_{mcm(3,5,17)} = \mathbb{Z}_{255}$ quan $\overline{a} \neq \overline{0}$.
   Fal el cas $\overline{a} = \overline{0}$: evidentment, $\overline{0}^{17} = \overline{0}$ a $\mathbb{Z}_{255}$. □