4- FUNCIONS

Una **funció** (també en diem **aplicació**) f consta d'un conjunt "d'origen" A, un conjunt de "destí" B i una "regla" que associa a cada element $x \in A$ un únic element $y \in B$. Més formalment, la "regla" és una relació $R \subseteq A \times B$ que satisfà:

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

A l'únic $y \in B$ tal que $(x, y) \in R$ li diem **la imatge** de x i el denotem per $f(x)$. Així, les dues propietats anteriors les podem expressar:

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

Notació:

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

Terminologia:

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

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

$x \rightarrow y = f(x) = e^x$

$\forall x \in \mathbb{R} \;\; \exists! \, y \in \mathbb{R} \,, \; y = e^x$

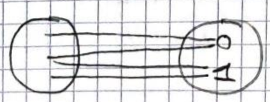
conjunto de todas las palabras binarias de cualquier longitud

$H: \{0,1\}^* \rightarrow \{0,1\}$

$b_1, b_2 \ldots b_n \rightarrow h(b_1 - b_n) = \begin{cases} 0 & \text{bit} - \text{bit}_n = \text{par} \\ 1 & \text{bit} - \text{bit}_n = \text{impar} \end{cases}$

$1011 \text{ —— } h(1011) = 1$

$11110 \text{ —— } h(11110) = 0$



Igualtat entre funcions

Dues funcions són iguals quan tenen el mateix domini, el mateix codomini i la mateixa “regla”. Si el domini o el codomini són diferents, les funcions es consideren diferents.

Si tenim dues funcions amb el mateix domini i mateix codomini llavors n’hi ha prou que tinguin la mateixa “regla”:

Donades $f, g: A \to B$:

$$\boxed{f = g \quad \text{si i només si} \quad \forall x \epsilon A \;\; f(x) = g(x)}$$

Propietats que *poden tenir* les funcions

$$f: A \to B$$

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

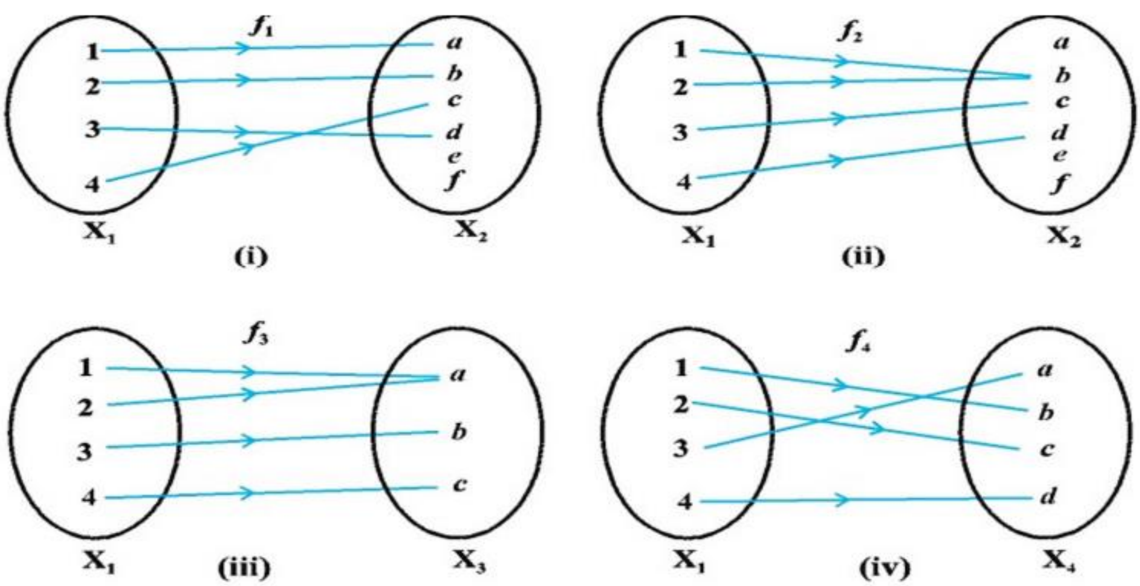


Fig 1.2 (i) to (iv)

Notem que:

Donada $f: A \to B$:

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

1- $f(x) = |x|$ a) $\mathbb{N} \to \mathbb{N}$

$0 \to 0$
$1 \to 1$
$2 \to 2$

$f(x) = x$

Inyectiva $\to |x_1| = |x_2| \to x_1 = x_2$
exhaustiva $\to f(y) = |y| = y$

Biyectiva

b) $\mathbb{N} \to \mathbb{Z}$

$0 \to 0$
$1 \to 1$
$2 \to 2$

Inyectiva $\xrightarrow{\checkmark} |x_1| = |x_2| \to x_1 = x_2$
exhaustiva $\xrightarrow{X} y = -3 \to \nexists x \in \mathbb{N} \ f(x) = -3$

c) $\mathbb{Z} \to \mathbb{N}$

$-2 \to 2$
$-1 \to 1$
$0 \to 0$
$1 \to 1$

inyectiva $\xrightarrow{X} |x_1| \neq |x_2|$, $x_1 = 1, x_2 = -1$
exhaustiva $\to f(x) = y$
$x = y$, $x = -y$ $\to y$

d) $\mathbb{Z} \to \mathbb{Z}$ No inyectiva, No exhaustiva

2- $f: \mathbb{N} \to \mathbb{Z}$

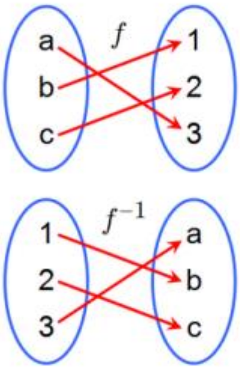
$$x \to f(x) = \begin{cases} -\frac{x}{2} & \text{si } x \text{ par} \\ \frac{x+1}{2} & \text{si } x \text{ impar} \end{cases}$$

f es inyectiva : $f(x_1) = f(x_2) \to x_1 = x_2$

- Si x_1, x_2 pares $\frac{-x_1}{2} = \frac{-x_2}{2} \xrightarrow{\checkmark} x_1 = x_2$
- Si x_1, x_2 impar $\frac{x_1+1}{2} = \frac{x_2+1}{2} \xrightarrow{\checkmark} x_1 = x_2$

Si tenen diferent $\frac{-x_1}{2} = \frac{x_2+1}{2} \xrightarrow{X} -x_1 = x_2 + 1$

Funció inversa



Si $f: A \to B$ és <u>bijectiva:</u>

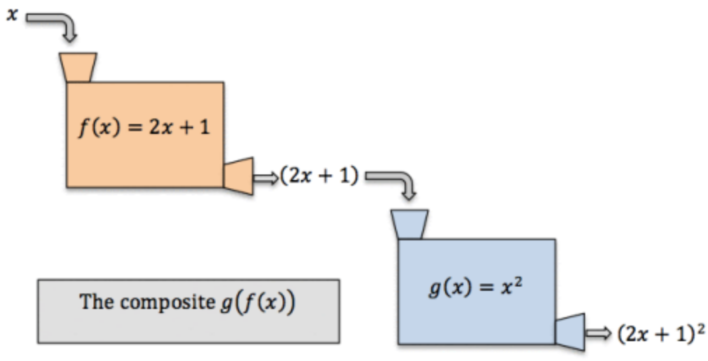
$$f^{-1}: B \to A$$
$$f^{-1}(y) \text{ és l'únic } x \in A \ \ tal\,que\ \ f(x) = y$$

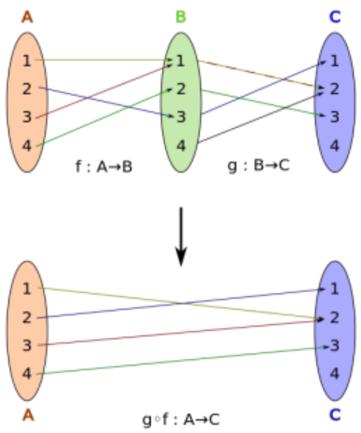
$$f^{-1}(y) = x \quad \Leftrightarrow \quad f(x) = y$$

Notem que:

- Cal que f sigui bijectiva, sinó la inversa no existeix.

Composició de funcions





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

$$g \circ f: A \to C$$
$$(g \circ f)(x) = g(f(x))$$

• Asociativa

$$\begin{tikzcd}
A \arrow[r, "f"] \arrow[d, "h\circ f"'] \arrow[dr, "g\circ f"] & B \arrow[d, "g"] \arrow[dl, "h\circ g"'] \\
D & C \arrow[l, "h"]
\end{tikzcd}$$

$f: A \to B$
$\quad x \to f(x)$

$g: B \to C$
$\quad x \to g(x)$

$h: C \to D$
$\quad x \to h(x)$

$$\boxed{h\cdot(g\cdot f) = (h\cdot g)\cdot f}$$

$g\cdot f: A \to C$
$\quad x \to (g\cdot f)\cdot(x)$

$h\cdot(g\cdot f): A \to D$

La composición no es commutativa

II. Si $f: A \to B$, llavors $I_B \circ f = f \circ I_A = f$.

propietats de la composició, injectivitat i exhaustivitat:

III. La composició de funcions injectives és injectiva.

IV. Si $g \circ f$ és injectiva llavors f és injectiva.

V. La composició de funcions exhaustives és exhaustiva.

VI. Si $g \circ f$ és exhaustiva llavors g és exhaustiva.

VII. La composició de funcions bijectives és bijectiva.

VIII. Si $g \circ f$ és bijectiva llavors f és injectiva i g és exhaustiva.

propietats de la composició i la inversa:

IX. Si $f: A \to B$ és bijectiva, llavors $f^{-1} \circ f = I_A$ i $f \circ f^{-1} = I_B$.

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

Ex

$f: \mathbb{Z} \to \mathbb{N}$

$x \to f(x) = \begin{cases} 2x-1 & x>0 \\ -2x & x \leq 0 \end{cases}$

$g: \mathbb{N} \to \mathbb{Z}$

$x \to g(x) = \begin{cases} -\frac{x}{2} & x = \text{par} \\ \frac{x+1}{2} & x = \text{imparell} \end{cases}$

1- $g \cdot f : \mathbb{Z} \to \mathbb{Z}$ $\quad g \cdot f = I_{\mathbb{Z}}$

$x \to (g \circ f)(x) = g(f(x)) = \begin{cases} g(2x-1) & x>0 \\ g(-2x) & x \leq 0 \end{cases}$

$\begin{cases} \frac{2x-1+1}{2} = x & x>0 \\ \frac{2x}{2} = x & x \leq 0 \end{cases}$

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

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

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

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

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

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

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

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

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

1a manera: f és injectiva i exhaustiva.

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

Demostració que les funcions $f, g: A \to B$ són iguals ($f = g$):

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

5. DIVISIBILITAT

Tant en aquest capítol com en el següent, treballem en els enters $\mathbb{Z}$. Si no es diu el contrari, tots el nombres que apareixen són enters.

Definició: Donats dos enters a, b:

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

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

Notem que:

- No és exactament el mateix $a \mid b$ que $b/a \in \mathbb{Z}$.
- Si $a \neq 0$ sí que és equivalent: $a \mid b \iff b/a \in \mathbb{Z}$.
- En general: $a \mid b \iff (a = b = 0) \lor (a \neq 0 \land b/a \in \mathbb{Z})$.

Propietats:

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

I. $1 \mid a$.

II. $a \mid 0$.

III. $a \mid ab$.

IV. Reflexiva: $a \mid a$.

V. Transitiva: $a \mid b\, ,\ b \mid c \quad \Rightarrow \quad a \mid c$.

VI. $a \mid b \quad \Rightarrow \quad ac \mid bc$.

VII. Simplificació: Si $c \neq 0$, $ac \mid bc \quad \Rightarrow \quad a \mid b$.

VIII. $a \mid b \quad \Rightarrow \quad a \mid bc$.

IX. No depèn del signe:

$$a \mid b \iff a \mid -b \iff -a \mid b \iff -a \mid -b \iff |a| \mid |b|.$$

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

XI. $a \mid b\, ,\ b \mid a \quad \Rightarrow \quad |a| = |b|$.

XII. **<u>Linealitat</u>:** $a \mid b\, ,\ a \mid c \quad \Rightarrow \quad a \mid ub + vc$.

Nombres primers

Definició:

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

Notem que:

- Els primers són positius i el 1 no és primer!
- Si $n \geq 2$, i no és primer (rep el nom de **compost**) llavors $n = rs$ per a uns certs enters r, s amb $1 < r < n$, $1 < s < n$.
- Per la propietat X anterior, els nombres $1, -1$ no tenen divisors primers. De fet veurem que són els únics enters que no tenen divisors primers.

Resultats

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

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

Màxim comú divisor

Definició:

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

Observem que

- $mcd(a_1, a_2, \dots a_n) \geq 0$.
- $mcd(a_1, a_2, \dots a_n) = 0 \quad \Leftrightarrow \quad a_1 = a_2 = \dots = a_n = 0$.

Propietats:

I. **Si** $a \mid b$ **llavors** $mcd(a, b) = |a|$.

II. $mcd(a, 0) = |a|$.

III. Si p és primer i no divideix b, llavors $mcd(p, b) = 1$.

IV. El mcd no depèn del signe:
$mcd(a, b) = mcd(a, -b) = mcd(-a, b) = mcd(-a, -b)$.

V. **Teorema d'Euclides**: $mcd(a, b) = mcd(a + ub, b)$.

Definició:

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

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

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

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

Solució: Utilitzem el Teorema d'Euclides diverses vegades:

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

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. $\square$

Divisió euclidiana

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

$$\boxed{\begin{array}{l} a = bq + r, \\ 0 \leq r < |b| \end{array}}$$

---

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

Algorisme d'Euclides

Volem calcular $mcd(a, b)$. Com que el mcd no depèn del signe ni de l'ordre podem començar suposant que $a \geq b > 0$ i fem la divisió Euclidiana de a per b:

$$a = bq + r$$

Observació: Pel teorema d'Euclides tenim que

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

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

Aplicant successivament la fórmula

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

Exemple:

$mcd(14001, 279) = mcd(279, 51) = mcd(51, 24) = mcd(24, 3) = 3.$

Això ho organitzem en una taula de la manera següent:

q		50	5	2		
r	14001	279	51	24	3	0

on r_n és l'últim residu no nul. Llavors $mcd(a, b) = r_n$.

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

Nombre de passos de l'algorisme d'Euclides

Si $a > b > 0$, el nombre de passos (divisions) en l'algorisme d'Euclides és com a molt

$$1 + log_{\phi} b. \qquad \phi = \frac{1+\sqrt{5}}{2},$$

Nota: el nombre de passos també el podem acotar per $log_{\phi} a$.

Descomposició en factors primers.

Unicitat de la descomposició en factors primers:.

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

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

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

Això vol dir que si demanem que $p_1 < p_2 < \cdots < p_k$, el nombre k, els $p_1, \dots, p_k$ i els $e_1, \dots, e_k$ són únics.

Exemple: $84 = 2^2 3^1 7^1, 90 = 2^1 3^2 5^1, 264 = 2^3 3^1 11^1$

Càlcul del mcd a partir de la factorització i conseqüències

Divisibilitat i càlcul del mcd a partir de la factorització.

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

I. $a \mid b \quad \Leftrightarrow \quad e_i \leq f_i$ per a cada i.

II. $mcd(a, b) = p_1^{min(e_1, f_1)} p_2^{min(e_2, f_2)} \dots p_k^{min(e_k, f_k)}$.

III. La fórmula del mcd val amb més nombres agafant el mínim dels exponents.

IV. Els divisors positius de a son tots els nombres de la forma $p_1^{g_1} p_2^{g_2} \dots p_k^{g_k}$ amb $0 \leq g_i \leq e_i$. El nombre de tals divisors és $(e_1 + 1)(e_2 + 1)\cdots(e_k + 1)$.

IDENTITAD DE BEZOUT (IB)

$\forall a,b \in \mathbb{Z} \quad \exists x,y \in \mathbb{Z} \,//\, ax+by = mcd(a,b)$

Ex:

1 0	0 1	1 -50	-5 251	11 -552	x y
	50 (cociente)	5	2	8	
14001	279	51	24	3	
51 (Residu)	24	3	0		

$x = x_{n-2} - (x_{n-1} \cdot q)$

$1 = 1 - (0 \cdot 50)$

$-50 = 0 - (1 \cdot 50)$

Lema de Gaus

$$\left.\begin{array}{l} a \mid b \cdot c \\ mcd(a,b) = 1 \end{array}\right\} a \mid c$$

Dem: $a \mid b \cdot c \rightarrow \left.\begin{array}{l} a \mid a \rightarrow a \mid a \cdot c \cdot x \\ a \mid b \cdot c \cdot y \end{array}\right\} \rightarrow acx + bcy \rightarrow a \mid c$

Lema de Euclides

p = primo

$p \mid b \cdot c \rightarrow p \mid b \vee p \mid c$

Si $p \nmid b \rightarrow p \mid c \qquad \left.\begin{array}{l} mcd(p,b) = 1 \\ p \mid b \cdot c \end{array}\right\} \rightarrow p \mid c$

Altres propietats de mcd.

I. **Tot divisor comú de a, b divideix $mcd(a, b)$. De fet:**

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

II. Associativitat mcd:

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

III. $$mcd(ca, cb) = |c|\, mcd(a, b).$$

IV. **Si** $d = mcd(a, b) \neq 0$ **llavors** $mcd(\, a/d,\ b/d\,) = 1$.

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

Equacions diofàntiques

Les equacions diofàntiques són equacions a coeficients enters de les quals busquem les solucions enteres. Nosaltres ens centrarem en les lineals amb dues variables:

$$ax + by = c \qquad (1)$$

Denotem $d = mcd(a, b)$ i suposem que $d \neq 0$(és a dir, a o b no son zero).

Existencia de solucions.

$$ax + by = c \text{ té solució} \quad \Leftrightarrow \quad d \mid c$$

multiplicant una identitat de Bézout de (a, b) per $\frac{c}{d}$ obtenim una solució particular.

Exemple/Exercici: *Esbrineu si* $14.001x + 279y = 21$ *té solució i trobeu-ne una en cas que la tingui.*

Solució: Comencem fent Euclides amb els coeficients per tal de calcular el mcd:

q		50	5	2		
r	14.001	279	51	24	3	0

Veiem que $mcd(14.001, 279) = 3$ per tant, l'equació té solució ja que $3 \mid 21$.
Ara, per trobar una solució, executem euclides estès:

x	1	0	1	-5	11	
y	0	1	-50	251	-552	
q		50	5	2		
r	14.001	279	51	24	3	0

i obtenim la identitat de Bézout: $14.001(11) + 279(-552) = 3.$
Multiplicant per 7 queda: $14.001(77) + 279(-3.864) = 21,$
i per tant $x = 77, y = -3.864$ és una solució.

Mínim comú múltiple

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

Definició:

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

Propietats immediates:

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

Propietats del mcm:

I. Càlcul eficient del mcm: $mcd(a, b)\, mcm(a, b) = |ab|$.

II. Tot múltiple comú de a, b és múltiple de $mcm(a, b)$. De fet:

$$a \mid c \text{ i } b \mid c \quad \Leftrightarrow \quad mcm(a, b) \mid c.$$

III. Associativitat: $mcm(\, mcm(a, b), c) = mcm(a, mcm(b, c)\,) = mcm(a, b, c)$.
IV. Les propietats anteriors valen també amb més enters excepte la propietat 1.

$$\boxed{mmcm(a,b) = \frac{a \cdot b}{mcd(a,b)}}$$

6. CONGRUÈNCIES

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

Definició:

Donat $m \geq 1$

$$a \equiv b \ (mod\, m) \iff m \mid b - a$$
$$\iff b = a + km \text{ per un cert } k$$
$$\iff a \text{ i } b \text{ tenen el mateix residu al dividir per } m$$

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

Quan $a \equiv b \ (mod\, m)$ es diu que a **és congruent amb** b **mòdul** m**.**

Exemples:

- $7 \equiv 15 \ (mod\, 4)$, $7 \not\equiv 12 \ (mod\, 4)$
- $a \equiv b \ (mod\, 1)$
- $a \equiv 0 \ (mod\, 2) \iff a$ és parell
- $a \equiv 1 \ (mod\, 2) \iff a$ és senar
- $a \equiv b \ (mod\, 2) \iff a$ i b tenen la mateixa paritat

---

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

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

Classes modulars

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

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

$\overline{0} = \{x\epsilon\mathbb{Z} \mid x \equiv 0\ (mod\ 5)\ \} = \{5k \mid k\epsilon\mathbb{Z}\ \}$

$\overline{1} = \{x\epsilon\mathbb{Z} \mid x \equiv 1(mod\ 5)\ \} = \{1 + 5k : k\epsilon\mathbb{Z}\ \}$

$\overline{2} = \{x\epsilon\mathbb{Z}\colon x \equiv 2\ (mod\ 5)\ \} = \{2 + 5k : k\epsilon\mathbb{Z}\ \}$

$\overline{3} = \{x\epsilon\mathbb{Z}\colon x \equiv 3\ (mod\ 5)\ \} = \{3 + 5k : k\epsilon\mathbb{Z}\ \}$

$\overline{4} = \{x\epsilon\mathbb{Z}\colon x \equiv 4\ (mod\ 5)\ \} = \{4 + 5k : k\epsilon\mathbb{Z}\ \}$

El conjunt quocient és doncs:

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

Fets:

A $\mathbb{Z}_m$ tenim:

I. $\overline{a} = \{x \in \mathbb{Z} : x \equiv a\ (mod\ m)\} = \{a + km : k \in \mathbb{Z}\ \}$.

II. $\overline{a} = \overline{b} \quad \Leftrightarrow \quad a \equiv b\ (mod\ m)$.

III. $\mathbb{Z}_m = \{\overline{0}, \overline{1}, \overline{2}, ..., \overline{m - 1}\}$.

Propietat 2:

$$\left| \begin{array}{l} a \equiv a'\ (mod\ m\ ) \\ b \equiv b'\ (mod\ m\ ) \end{array} \right. \quad \Rightarrow \quad \left| \begin{array}{l} a + b \equiv a' + b'\ (mod\ m) \\ ab \equiv a'b'\ (mod\ m) \end{array} \right.$$

Altres propietats de les congruències:

I. Si $a \equiv b \ (mod\ m)$ i $d \mid m$ llavors $a \equiv b \ (mod\ d)$.

II. Si $k > 0$ **llavors:**

$$ka \equiv kb \ (mod\ km) \quad \Leftrightarrow \quad a \equiv b \ (mod\ m).$$

III. Si $mcd(k, m) = 1$ **llavors:**

$$ka \equiv kb \ (mod\ m) \quad \Leftrightarrow \quad a \equiv b \ (mod\ m)$$

IV. $a \equiv b \ (mod\ m_1),..,\ a \equiv b \ (mod\ m_n) \ \Leftrightarrow \ a \equiv b \ (\ mod\ \ mcm(m_1,..., m_n)\ ).$

Aritmètica modular

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

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

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

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

Això ens permet "triar el representant" que més ens convingui. Sempre és millor "reduir" abans d'operar. Per exemple, a $\mathbb{Z}_{3000}$:

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

Propietats:

I. De la suma:

A. Commutativa: $\overline{a} + \overline{b} = \overline{b} + \overline{a}$

B. Associativa: $(\overline{a} + \overline{b}) + \overline{c} = \overline{a} + (\overline{b} + \overline{c})$

C. Element neutre: $\overline{a} + \overline{0} = \overline{a}$

D. Element invers: $\overline{a} + \overline{-a} = \overline{0}$

E. $n\overline{a} = \overline{na}$ per a tot $n \geq 1$.

II. Del producte:

A. Commutativa: $\overline{a}\cdot\overline{b} = \overline{b}\cdot\overline{a}$

B. Associativa: $(\overline{a}\cdot\overline{b})\cdot\overline{c} = \overline{a}\cdot(\overline{b}\cdot\overline{c})$

C. Element neutre: $\overline{a}\cdot\overline{1} = \overline{a}$

D. $\overline{a}^{n} = \overline{a^{n}}$ per a tot $n \geq 1$.

III. Distributiva: $\overline{a}\cdot(\overline{b} + \overline{c}) = \overline{a}\cdot\overline{b} + \overline{a}\cdot\overline{c}$

---

b) $n = \overset{\circ}{9}$

$$n = d_4 \cdot 10^4 + d_3 \cdot 10^3 + d_2 \cdot 10^2 + d_1 \cdot 10^1 + d_0 \cdot 10^0$$

$$\frac{n}{9} = \frac{d_4}{9} \cdot \overline{1} + \frac{d_3}{9} \cdot \overline{1} + \frac{d_2}{9} \cdot \overline{1} + \frac{d_1}{9} \cdot \overline{1} + \frac{d_0}{9} \cdot \overline{1}$$

$$\frac{n}{9} = \frac{d_4 + d_3 + d_2 + d_1 + d_0}{9} \cdot \overline{1}$$

Invers modular

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

Existència d'inversos modulars:

$$\overline{a} \text{ té invers a } \mathbb{Z}_m \quad \Leftrightarrow \quad mcd(a, m) = 1$$

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:

$$\overline{39}^{-1} = \overline{-31} = \overline{1.179} \quad \text{a } \mathbb{Z}_{1.210}.$$

Definició:

Un **cos** és un anell on tot element, llevat del 0 (el neutre de la suma), té invers.

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

---

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

Sistemes de congruències

Un sistema de congruències és un sistema d'equacions del tipus:

$$x \equiv a_1 \,(mod\, m_1) ,..., \; x \equiv a_n \,(mod\, m_n)$$

Comencem veient que si tenim una solució particular d'un sistema de congruències, ja sabem com son totes les solucions.

---

totes les solucions d'un sistema.
Si x_0 és una solució particular del sistema $x \equiv a_1 \,(mod\, m_1) ,..., \; x \equiv a_n \,(mod\, m_n)$, llavors totes les solucions són de la forma:

$$x \equiv x_0 \,(\,mod \;\; mcm(m_1,.., m_n)\,)$$

Un exemple. Considerem el sistema:

$$x \equiv 0\,(\,mod \;\; 3), \quad x \equiv 1\,(\,mod \;\; 4), \; x \equiv 2\,(\,mod \;\; 5).$$

Com que $-\ 3$ és una solució, el sistema és compatible i totes les solucions són de la forma:

$$\boxed{x \equiv -\ 3\,(\,mod \;\; mcm(3, 4, 5)\,)}$$

Per tant, totes les solucions del sistema són:

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

Ara donarem un mètode per saber si té solució i trobar una solució particular. Comencem amb dues. Si tenim un sistema de dues congruències:

$$x \equiv a_1\,(\,mod \;\; m_1), \;\; x \equiv a_2\,(\,mod \;\; m_2) \qquad (1)$$

i x és una solució llavors $x = a_1 + m_1 y = a_2 + m_2 z$ per a uns certs y, z enters. Per tant

$$m_1 y - m_2 z = a_2 - a_1 \qquad (2)$$

Així, l'equació diofàntica (2) en les variables y, z té solució. Recíprocament, si y, z és una solució de l'equació diofàntica (2), fent $x = a_1 + m_1 y = a_2 + m_2 z$ tenim que x és una solució del sistema xinès. Això ens dona un mètode per resoldre un

Existència de solucions.

El sistema (1) té solució si i només si $mcd(m_1, m_2) \mid a_2 - a_1$.

El Teorema petit de Fermat

Teorema de Fermat.

Si p és primer i $\overline{a} \neq \overline{0}$ a $\mathbb{Z}_p$ llavors $\overline{a}^{p-1} = \overline{1}$

Això es pot expressar en termes de congruències de la manera següent:

Si p és primer i no divideix a llavors $a^{p-1} \equiv 1\ (mod\ p)$.

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

$$43^{3221} \equiv 4^{3221} (mod\ 13)$$

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

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

El Teorema de Fermat es pot expressar de la manera següent, més útil a la pràctica:

Teorema de Fermat (2a versió).

Si $n, m \geq 1$ llavors:

$$n \equiv m\ (mod\ p-1) \quad \Rightarrow \quad a^n \equiv a^m\ (mod\ p)$$