Apunts de
FONAMENTS MATEMÀTICS

amb exercicis

Part 2

Rafel Farré

30/08/2022

- Els exercicis en color negre són per fer a les classes de teoria.
- Els exercicis en color blau són per fer a les classes de taller. Els marcats amb (R) són recomanats.
- Els exercicis en color verd està resolts al document *Exercicis Resolts*.

4. FUNCIONS

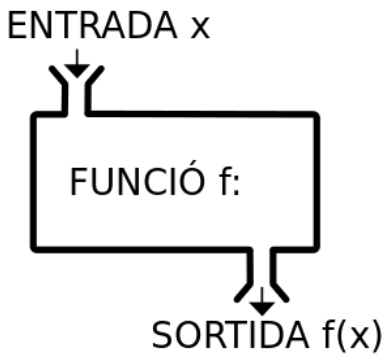
Una **funció** (també en diem **aplicació**) f consta d'un conjunt "d'origen" A, un conjunt de "destí" B i una "regla" que associa a cada element $x \in A$ un únic element $y \in B$. Més formalment, la "regla" és una relació $R \subseteq A \times B$ que satisfà:

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

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:

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

Quan aquestes dues condicions es compleixen direm que f **està ben definida.**
Intuïtivament: la "regla" és com un programa, A és el conjunt de les entrades possibles i i B és un conjunt que conté totes les sortides possibles (potser és més gran que el conjunt de totes les sortides!). Si ho pensem en termes d'especificació de programes A seria la *precondició* i B la *postcondició*. Més precisament, A és el conjunt d'objectes que satisfan la *precondició* del programa. B és el conjunt d'objectes que satisfan la *postcondició* del programa.



Exemple: Les funcions hash. Les funcions hash són funcions que a paraules binàries de longitud arbitrària els hi assignen de manera eficient paraules binàries de longitud fixa. Un dels aspectes importants de les "funcions hash" és que són

funcions: si dues entrades tenen hash diferent és que són diferents: (si $h(x) \neq h(y)$ llavors $x \neq y$). Per exemple, $MD5$ (Message Digest 5) és una funció que, a cada paraula binària (de qualsevol longitud) li fa correspondre una paraula binària (el seu hash o resum criptogràfic) de 128 bits.

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

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

Notació:

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

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.

Exemples 1:

A. $f: \mathbb{R} \to \mathbb{R}$ definida per $f(x) = e^x$.
B. $f: \mathbb{Z} \to \mathbb{N}$ definida per $f(x) = |x|$.
C. $f: \mathbb{Q} \to \mathbb{Q}$ definida per $f(x) = \frac{3x-5}{4}$.
D. $f: \mathbb{Q} \to \mathbb{R}$ definida per $f(x) = \frac{3x-5}{4}$.
E. $f: \mathbb{R} \to \mathbb{R}$ definida per $f(x) = \frac{3x-5}{4}$.
F. $f: \{1,2,3\} \to \{a,b,c,d\}$ definida per $f(1) = d$, $f(2) = d$, $f(3) = c$.
G. La identitat en A, que denotem per I_A, és la funció $I_A: A \to A$ definida per $I_A(x) = x$.
H. $h: \{0,1\}^* \to \{0,1\}$ definida per $h(b_1 b_2 \cdots b_n) = b_1 + b_2 + \cdots + b_n \, mod \, 2$, el residus de la divisió de $b_1 + b_2 + \cdots + b_n$ per 2. Aquí $\{0,1\}^*$ denota el conjunt de paraules binàries. Observeu que $h(b_1 b_2 \cdots b_n)$ és un *bit de paritat*: val 0 quan $b_1 + b_2 + \cdots + b_n$ és parell i val 1 quan $b_1 + b_2 + \cdots + b_n$ és senar.
I. Si considerem $f: \mathbb{R} \to \mathbb{R}$ definida per $f(x) = \frac{x+1}{x-1}$ no està ben definida perquè $f(1)$ no existeix. Això es pot arreglar fàcilment posant $f: \mathbb{R} - \{1\} \to \mathbb{R}$.
J. Si definim $f: \mathbb{R} \to \mathbb{R}$, fent-li correspondre a x un element $y \in \mathbb{R}$ tal que $y^2 = x$ no està ben definida. Si $x < 0$ no hi ha un tal y, mentre que si $x > 0$ n'hi ha dos: $\pm\sqrt{x}$. En canvi si prenem $f: [0,\infty) \to [0,\infty)$ definida: fent-li correspondre a x un element $y \in [0,\infty)$ tal que $y^2 = x$, sí que està ben definida.
K. Si considerem $f: \mathbb{R} \to \mathbb{Q}$ amb $f(x) = \frac{3x-5}{4}$ no està ben definida perquè $\frac{3x-5}{4}$ no sempre és racional. Per exemple, $f(\frac{4\sqrt{2}+5}{3}) = \sqrt{2}$ és irracional.

Observacions importants:

I. Tot element $x \in A$ té <u>una única</u> imatge que denotem per $f(x)$.
II. Si $y \in B$, les antiimatges de y són els $x \in A$ tals que $f(x) = y$. Cada $y \in B$ pot no tenir antiimatges, pot tenir-ne una de sola o tenir-ne moltes.

Exemples 2:

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

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 $f, g: A \to B$:

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

Exemples 3:

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

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

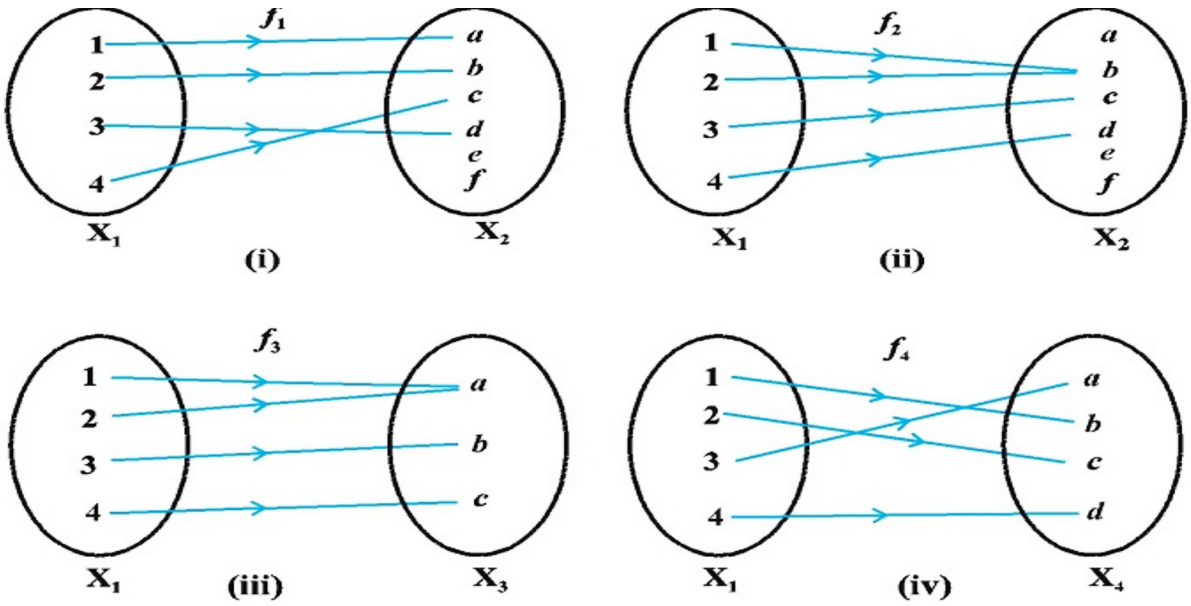


Fig 1.2 (i) to (iv)

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.

Exemples/Exercicis:

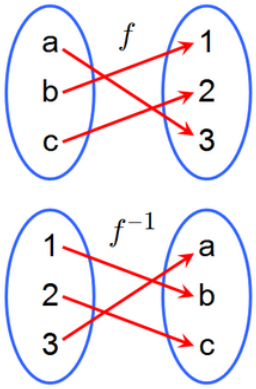
1. Estudieu la injectivitat, exhaustivitat i bijectivitat de les funcions definides per $f(x) = |x|$, segons f va de $\mathbb{Z}, \mathbb{N}$ en $\mathbb{Z}, \mathbb{N}$ (hi ha 4 funcions diferents).
2. Considerem la funció $f: \mathbb{N} \to \mathbb{Z}$ definida per $f(x) = -x/2$ si x és parell; $f(x) = \frac{x+1}{2}$ si x és senar. Demostreu que f és bijectiva.
3. (difícil) Siguin A, B, C conjunts tals que $A, B \subseteq C$. Definim $f: P(C) \to P(A) \times P(B)$ així: $f(x) = (x \cap A, x \cap B)$.
   a. Demostreu que està ben definida.
   b. Demostreu que és injectiva $\Leftrightarrow A \cup B = C$.
   c. Demostreu que és exhaustiva $\Leftrightarrow A \cap B = \emptyset$.
   d. Quan $A \cap B = \emptyset$ i $A \cup B = C$ calculeu la inversa.
4. (R) Determineu si les funcions de $\mathbb{Z}$ en $\mathbb{Z}$ següents són injectives, exhaustives i/o bijectives.
   a. $n \to n - 1$.
   b. $n \to n^2 + 1$.
   c. $n \to n^3$.
   d. $n \to E(n/2)$.

   Aquí E indica la funció part entera inferior.
5. (R) Sabem que $f: \mathbb{N} \to \mathbb{N}$ és injectiva. Considerem la funció $g: \mathbb{N} \to \mathbb{N}$ definida per $g(x) = 2f(x) + 3$. Demostreu que g és injectiva i no exhaustiva.
6. Siguin A, B conjunts on B no és buit. Demostreu que la funció $f: A \times B \to A$ definida per $f(x, y) = x$ és exhaustiva.
7. Considerem la funció $f: \mathbb{N} \to \mathbb{N}$ definida per $f(x) = x/2$ si x és parell; $f(x) = x$ si x és senar. Demostreu que f és exhaustiva però no és injectiva.
8. Siguin A, B conjunts i $b \in B$. Demostreu que la funció $f: A \to A \times B$ definida per $f(x) = (x, b)$ és injectiva.
9. (R) Sabem que $f: \mathbb{Z} \to \mathbb{Z}$ és exhaustiva. Considerem la funció $g: \mathbb{Z} \to \mathbb{Z}$ definida per $g(x) = f(x + 1) - 3$. Demostreu que g és exhaustiva.
10. En els Exemples 1: la A és injectiva i no exhaustiva, B és exhaustiva i no injectiva, C és bijectiva, D és injectiva i no exhaustiva, E és bijectiva, E és no injectiva i no exhaustiva, F és bijectiva, G és exhaustiva no injectiva.
11. $f: \mathbb{Z} \to \mathbb{N}$ definida per $f(x) = 2x - 1$, si $x > 0$, $f(x) = -2x$, si $x \leq 0$ és

bijectiva.

12. Considerem la funció $f: \mathbb{N} \to \mathbb{N}$ definida per $f(n) = n + 1$ si n és parell; $f(n) = 2n$ si n és senar. Demostreu que f és injectiva però no és exhaustiva.
13. 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.
14. Sabem que $f: \mathbb{Z} \to \mathbb{N}$ és exhaustiva. Considerem la funció $g: \mathbb{Z} \to \mathbb{N}$ definida per $g(x) = E(f(x)/2)$. Demostreu que g és exhaustiva pero no injectiva. Aquí E indica la funció part entera inferior.

Funció inversa



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

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

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.

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

15. $f: [5/3, \infty) \to [0, \infty)$ definida per $f(x) = \sqrt{\frac{3x-5}{4}}$.
16. $f: \mathbb{R} - \{1\} \to \mathbb{R} - \{0\}$ definida per $f(x) = \frac{1}{x-1}$.
17. (R) $f: (-\infty, 3) \to \mathbb{R}$ definida per $f(x) = ln(6 - 2x)$.
18. (R) Siguin $X = \{1, 2, 3, 4, \ldots, 99, 100\}$ i $f: X \to X$ definida per $f(x) = 2x$, si $1 \leq x \leq 50$, $f(x) = 2(x - 51) + 1$, si $51 \leq x \leq 100$. Demostreu que està ben definida, és bijectiva i calculeu la inversa.
19. $f: [-\pi/2, \pi/2] \to [-1, 1]$ definida per $f(x) = sin(x)$.
20. $f: [10, 11] \to [10, 11]$ definida per $f(x) = cos(\pi x - 10\pi)/2 + 21/2$.
21. $f: \mathbb{Q} \to \mathbb{Q}$, definida per $f(x) = \frac{3x-5}{4}$.
22. $f: \mathbb{R} - \{1/3\} \to \mathbb{R} - \{2/3\}$ definida per $f(x) = \frac{2x+5}{3x-1}$.
23. $f: \mathbb{Z} \to \mathbb{N}$ definida per $f(x) = 2x - 1$, si $x > 0$, $f(x) = -2x$, si $x \leq 0$.
24. $f: \mathbb{R} \to (1, \infty)$ definida per $f(x) = 2e^{x-1} + 1$.

Propietat:

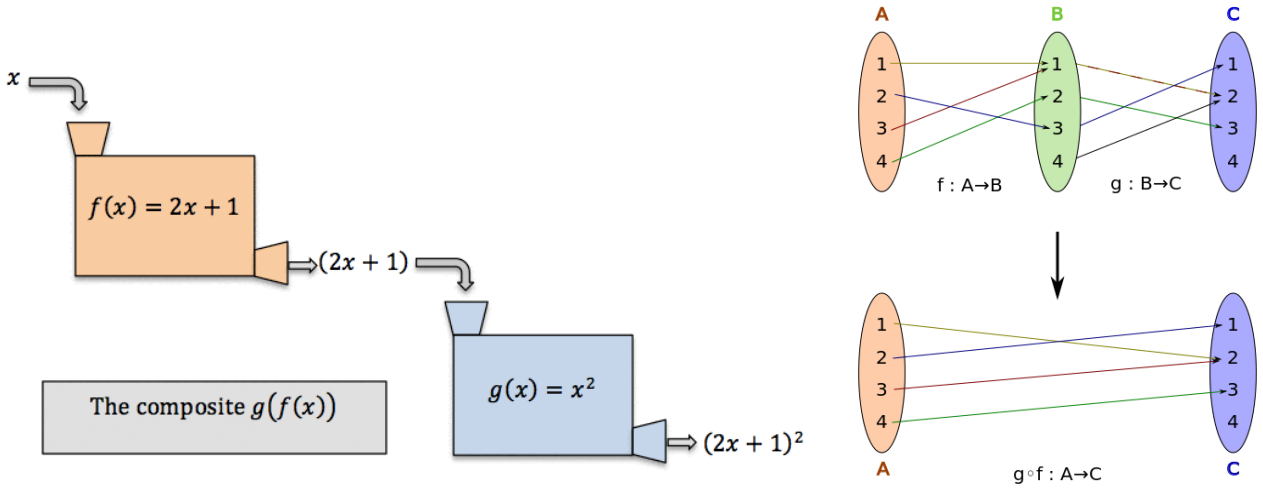
Si f és bijectiva llavors f^{-1} també és bijectiva i $(f^{-1})^{-1} = f$.

Demo: Com que $(f^{-1})^{-1}, f: A \to B,$ hem de veure que $(f^{-1})^{-1}(x) = f(x)$ per a tot $x \in A$. Ara bé:

$(f^{-1})^{-1}(x) = f(x) \Leftrightarrow [Def.\ f^{-1}]\ f^{-1}(f(x)) = x \Leftrightarrow [Def.\ f^{-1}]\ f(x) = f(x).$

I aquesta última igualtat és òbviament certa.

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:

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

Notem que:

- No sempre es pot composar, només quan el codomini de la primera funció està contingut al domini de la segona.
- Diem f composada amb g, però ho denotem $g \circ f$.

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

25. $f: \mathbb{R} \to \mathbb{R}$ definida per $f(x) = x + 1$, $g: \mathbb{R} \to \mathbb{R}$ definida per $g(x) = x^2$.
26. $f: \mathbb{Z} \to \mathbb{N}$ definida per $f(x) = x \bmod 5$, $g: \mathbb{N} \to \mathbb{R}$ definida

$g(x) = ln(x + 1)$.

27. $f: \mathbb{R} \to \mathbb{R}$ definida per $f(x) = e^x$, $g: \mathbb{R} \to \mathbb{R}$ definida per $g(x) = 2x$.

28. $f: \mathbb{Z} \to \mathbb{Z}$ 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 $x \leq 0$.

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

Propietats:

I. Associativa: si $f: A \to B$, $g: B \to C$, $h: C \to D$ llavors $h \circ (g \circ f) = (h \circ g) \circ f$.

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 $f = g^{-1}$.

Demostració de IX: Com que $f^{-1} \circ f, I_A: A \to A$, cal veure que per a tot $x \in A$, $(f^{-1} \circ f)(x) = I_A(x)$. Ara bé:

$(f^{-1} \circ f)(x) = I_A(x) \quad \Leftrightarrow [Def \circ, I_A] \quad f^{-1}(f(x)) = x \quad \Leftrightarrow [Def, f^{-1}]$
$f(x) = f(x)$. □

Demostració de X: que f i g són bijectives surt de IV. i VI. Veiem ara que $g^{-1} = f$. Sigui $x \in A$ qualsevol, hem de veure que $g^{-1}(x) = f(x)$. Per la definició de g^{-1}, això és equivalent a $g(f(x)) = x$. I això és cert perquè $g \circ f = I_A$. □

Exemples:

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

Exercicis:

29. Demostreu les propietats II., V. i VII. anteriors.
30. Siguin $f: A \to B$, $g: B \to B$ amb f exhaustiva i satisfent $g \circ f = f$. Demostreu que $g = I_B$.
31. Si $f \circ h = g \circ h$ i h és exhaustiva llavors $f = g$.
32. Sigui $f: A \to A$ satisfà $f \circ f = f$. Demostreu que són equivalents:
    a. f és injectiva.
    b. f és exhaustiva.
    c. f és bijectiva.
    d. $f = I_A$.
33. Siguin $f: A \to B$, $g: B \to A$ satisfent $g \circ f = I_A$.

a. Demostreu que si f és exhaustiva llavors $f \circ g = I_B$.

b. Demostreu que si g és injectiva llavors $f \circ g = I_B$.

c. Doneu un exemple on $f \circ g \neq I_B$.

34. Sigui $f: A \to A$.

a. Demostreu que si $f \circ f = f$ llavors $f \circ f \circ f = f \circ f$.

b. Definim $f: \mathbb{Z} \to \mathbb{Z}$ així: $f(x) = x$ si x és múltiple de 3, $f(x) = x + 1$ altrament. Demostreu que aquesta funció f compleix $f \circ f \circ f = f \circ f$, en canvi $f \circ f \neq f$.

35. (R) Sigui $f: \mathbb{N} \to \mathbb{N}$ definida per $f(x) = x$, si x és parell, $f(x) = x + 1$, altrament. Demostreu que $f \circ f = f$.

36. Demostreu les propietats IV.(R) i VIII.(R) . anteriors.

37. (R) Sigui $f: \mathbb{N} \to \mathbb{N}$ definida per $f(x) = x - 2$, si x és de la forma $3k + 2$; $f(x) = x + 1$, altrament. Demostreu que $f \circ f \circ f = I_{\mathbb{N}}$. Deduïu que f és bijectiva i que $f \circ f$ és la inversa. Demostreu que $f \circ f(x) = x + 2$, si x és múltiple de 3; $f \circ f(x) = x - 1$ altrament.

38. Si $f: A \to B$ és bijectiva i $g: B \to C$ és bijectiva llavors $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$. Pista: feu servir la propietat X.

39. $f: A \to B$ és bijectiva $\Leftrightarrow$ existeix $g: B \to A$ tal que $g \circ f = I_A$ i $f \circ g = I_B$. En aquest cas cada una és la inversa de l'altre: $g = f^{-1}$ i $f = g^{-1}$.

40. Sigui $f: A \to B$ $g: B \to C$ tals que $g \circ f$ és bijectiva. Demostreu que són equivalents:

a. f és exhaustiva.

b. f és bijectiva.

c. g és injectiva.

d. g és és bijectiva.

41. Si $f: A \to A$ satisfà $f \circ f = I_A$, què podem dir de f?

42. Sigui $f: A \to B$ i $g: B \to C$. Demostreu que si $g \circ f$ és injectiva i f és exhaustiva llavors g és injectiva.

43. (R) Siguin $f, g: A \to B$ i $h: A \to B$. Demostreu que si $h \circ f = h \circ g$ i h és

injectiva llavors $f = g$.

44. Siguin $f: A \to A$, $g: A \to B$ amb g injectiva i satisfent $g \circ f = g$. Demostreu que $f = I_A$.

45. Sigui $f: A \to A$. Demostreu que són equivalents:
    a. $f \circ f = f$.
    b. Existeix $B \subseteq A$ tal que $f(A) \subseteq B$ i $f(x) = x$ per tot $x \in B$.

46. Siguin $f: A \to B$, $g: B \to A$ amb g injectiva i satisfent $g \circ f = I_A$. Demostreu que $f \circ g = I_B$.

47. Sigui $f: A \to B$. Demostreu que són equivalents:
    a. f és injectiva
    b. Existeix $g: B \to A$ tal que $g \circ f = I_A$.

48. Sigui $f: A \to A$ satisfent $f \circ f \circ f = I_A$. Definim una relació R en A així: $xRy \Leftrightarrow x = y \vee x = f(y) \vee x = f(f(y))$. Demostreu que és relació d'equivalència i que $\overline{x} = \{x, f(x), f(f(x))\}$.

49. Demostreu les propietats I., III. i VI. anteriors.

50. 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.

51. 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.

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

RECEPTES: Demostracions amb funcions

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

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

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:

$a \mid b \iff$ existeix un enter q tal que $b = aq$

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

Exemples:

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

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: $a \mid b \iff (a = b = 0) \ \vee \ (a \neq 0 \ \wedge \ b/a \in \mathbb{Z})$.

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>:** $a \mid b,\ a \mid c \quad \Rightarrow \quad a \mid ub + vc.$

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

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

Exercicis:

1. Demostreu les propietats I. i IV. anteriors.
2. Demostreu que si $a \mid a + b$ llavors $a \mid b$.
3. Demostreu que $0 \mid a \iff a = 0$.
4. Demostreu que $a \mid 1 \iff a = \pm 1$.
5. Demostreu que les úniques solucions enteres de l'equació $xy = x + y$ són $x = y = 0$, $x = y = 2$. Pista: proveu que x, y es divideixen mútuament i useu XI.
6. (difícil) Demostreu que si $b^2 = ac$ llavors $(a + b + c) \mid (a^2 + b^2 + c^2)$.
7. Demostreu que si $x \mid y$ i $y \mid 2x$ llavors o bé $|y| = |x|$ o bé $|y| = |2x|$.
8. Demostreu les propietats II., V. (R), VIII. i IX. anteriors.
9. Demostreu que si $a \mid a'$ i $b \mid b'$ llavors $ab \mid a'b'$.
10. (R) Demostreu que si $a \mid (b - 1)$ i $a \mid (c - 1)$ llavors $a \mid (bc - 1)$.
11. A $\mathbb{Z}$ definim la relació següent. Donats a, b enters:

$$aRb \iff a \mid b^n,\ b \mid a^n \text{ per a un cert } n \geq 1.$$

Demostreu que és una relació d'equivalència.

12. (difícil) Siguin a, b enters no nuls. Demostreu que són equivalents:
    a. Per a tot $n \geq 0$, $e \mid ca^n + db^n$.
    b. $e \mid c + d$, $e \mid ca + db$.
    c. $e \mid c + d$, $e \mid c(a - b)$.
    d. $e \mid c + d$, $e \mid d(a - b)$.
13. Demostreu que si $(a + b + c) \mid abc$ llavors $(a + b + c) \mid (a^3 + b^3 + c^3)$.
    (Pista: calculeu $(a + b + c)(a^2 + b^2 + c^2 - ab - ac - bc)$).
14. Demostreu les propietats III., VI., VII., XI. i XII. anteriors.
15. Demostreu que $a \mid b$ implica $a^n \mid b^n$.

Nombres primers

Definició:

p és **primer** $\iff p \geq 2$ 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.

Exemples:

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

Resultats

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.

Demostracions.

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

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

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

III. Per Reducció a l'absurd. Si no, siguin $p_1, p_2, p_3, \ldots, p_n$ tots els primers. Per I, $p_1 p_2 p_3 \ldots p_n + 1$ ha de tenir algun divisor primer, posem p_i. De $p_i \mid p_1 p_2 p_3 \ldots p_n + 1$ i

$p_i \mid p_1 p_2 p_3 \ldots p_n$, per linealitat tenim que $p_i \mid 1$, absurd. □

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).

Exemple : És primer el nombre 102941?

Necessitem la llista de tots els primers fins $\sqrt{102941} = 320,8\ldots$ La fem fins al 400. Aquesta llista la faren utilitzant un algorisme anomenat **Garbell d'Eratóstenes**. Comencem fent una llista de tots enters des de 2 fins a 400 (en aquest cas). A continuació marquem el 2 com a primer i eliminem tots el múltiples de 2(excepte el 2). En tots els passos posteriors agafem el primer enter de la llista ni marcat ni eliminat. El marquem com a primer i a continuació eliminem tots els seus múltiples (excepte l'esmentat nombre). Pel test de primalitat només caldrà fer-ho fins al 20. Tots els enters que quedin a la llista són primers. En aquest link es pot fer la seva execució en viu. Ara, provant divisors resulta que…. Resposta. Si volem fer la llista de tots el primers fins a n executarem aquest procediment fins que arribem a $\sqrt{n}$.

Màxim comú divisor

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

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

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

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**: $mcd(a, b) = mcd(a + ub, b)$.

Demostracions:

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

II. Surt de 1. □

III. Els únics divisors positius de p són $1, p$. Com que p no divideix b, l'únic divisor positiu comú és 1. □

IV. Ja que la divisibilitat no depèn del signe. □

V. Posem $d_1 = mcd(a, b)$, $d_2 = mcd(a + ub, b)$. Hem de veure $d_1 = d_2$ i això ho farem demostrant que $d_1 \leq d_2$ i $d_2 \leq d_1$. Com que $d_1 \mid a$ i $d_1 \mid b$, per linealitat $d_1 \mid a + ub$. Així d_1 és un divisor comú de $a + ub$, b i per tant ≤ que el seu mcd. Així $d_1 \leq d_2$. Per a l'altra desigualtat, com que $d_2 \mid a + ub$, $d_2 \mid b$ i tenint en compte que $a = (a + ub) - ub$, per linealitat deduïm que $d_2 \mid a$. Com que d_2 divideix b resulta que $d_2 \leq d_1$. □

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 ⇔ no tenen cap divisor primer comú.

Demostració: Denotem $d = mcd(a, b)$. Les dues implicacions les fem per contrarecíproc.

⇒) Si a, b tenen algún divisor primer p comú, llavors $d \geq p \geq 2$.

⇐)Si $d \neq 1$ hi ha dos casos. Si $d = 0$, a i b han de ser zero ambdós i qualsevol primer és divisor comú. Si $d \geq 2$ llavors d té algun divisor primer p. De $p \mid d$ i $d \mid a$ deduïm $p \mid a$. Anàlogament $p \mid d$ i per tant d és un divisor primer comú. □

Exercicis:

16. Demostreu que $mcd(n, n + 2) = 2 \ si \ \ 2 \mid n \, , \ \ 1 \ altrament.$
17. Calculeu $mcd(a^2 - 1, \ a^3 - 1)$.
18. Calculeu $mcd(32k + 12, 12k + 4)$.
19. Trobeu tots els enters a tals que $(a - 1) \mid a$. Pista: Qui és $mcd(a, a - 1)$?
20. Demostreu que si $a + c = 1$ llavors $mcd(a, c) = 1$.
21. La successió de Fibonacci és defineix així: $F_0 = 0, F_1 = 1, F_n = F_{n-1} + F_{n-2}$

per a $n \geq 2$. Demostreu que $mcd(F_n, F_{n-1}) = 1$ per a tot $n \geq 1$. Pista: feu inducció simple i useu T. Euclides.

22. Demostreu que si $c \mid a$ i $mcd(a, b) = 1$ llavors $mcd(c, b) = 1$.
23. Demostreu que si $a + b \mid a$ llavors $a = -b \pm mcd(a, b)$. Pista: Qui és $mcd(a, a + b)$?
24. Demostreu que si $a \mid c$ i $b \mid d$ llavors $mcd(a, b) \leq mcd(c, d)$ [1].
25. Calculeu $mcd(a + b, a^2 - b^2)$.
26. (R) Calculeu el $mcd(a, b)$ en els casos següents:
    a. $b = ca$.
    b. $b = a^n$ $(n \geq 1)$.
    c. b és primer.
    d. $b = 2a - 1$.
27. Demostreu que $mcd(4k + 14, 6k + 20) = 2$.
28. Calculeu $mcd(a^2 - 1, a^3 + 1)$.
29. Demostreu que si $ab + c = 1$ llavors $mcd(a, c) = mcd(b, c) = 1$.
30. (R) Demostreu que $mcd(2k + 9, 3k + 15) = 3$ si $3 \mid k$, 1 $altrament$.
31. Trobeu tots els enters a tals que $(a + 2) \mid a$. Pista: Qui és $mcd(a, a + 2)$?
32. Demostreu que si per a cada $j \in \{1,..., m\}$ hi ha un $i \in \{1,..., n\}$ tal que $a_i \mid b_j$ llavors $mcd(a_1,..., a_n) \leq mcd(b_1,..., b_m)$.
33. Demostreu que $mcd(\pm 1, b, c,..) = 1$.
34. Demostreu que $mcd(a) = |a|$.
35. Demostreu que si $b \mid a$ llavors $mcd(a, b, c,..) = mcd(b, c,..)$.
36. Demostreu que $mcd(0, b, c,..) = mcd(b, c,..)$.
37. Demostreu que $mcd(a, b, c,..) = mcd(a + ub, b, c,..)$.
38. (En aquest exercici introduïm un algorisme eficient per calcular el mcd de diversos enters positius). Demostreu que el següent algorisme acaba i calcula $mcd(a_1, a_2,..., a_n)$. Comencem reemplaçant cada enter pel seu valor absolut. Apliquem successivament les operacions següents: mentre hi hagi zeros, suprimir-los; mentre hi hagi més d'un enter reemplaçar el més gran dels enters pel residu de la seva divisió entre el menor d'ells. Quan només quedi un sol

[1] De fet mcd(a,b) divideix mcd(c,d), però de moment no ho podem demostrar.

enter, acabar i respondre aquest enter. (pista: useu exercicis anteriors).

39. Calculeu el $mcd(a, b)$ en els casos següents:
    a. $b = 2a$.
    b. $b = a + 1$.
    c. $b \mid a$.
    d. $b = mcd(a, c)$.
40. Demostreu que $mcd(2k + 5, 3k + 7) = 1$.
41. Calculeu $mcd(a^2 + 1,\ a^3 + 1)$.
42. Demostreu que si p, q són primers i $p \mid q$ llavors $p = q$.
43. (*) Demostreu que si $ab + cd = 1$ llavors $mcd(a, c) = mcd(a, d) = mcd(b, c) = mcd(b, d) = 1$.

Divisió euclidiana

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

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

---

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

Demostració:

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

Prenem el quocient q i el residu r així:

$$\boxed{\begin{array}{c} q = sig(b)E(a/|b|) \\ \hline r = a - bq = a - |b|E(a/|b|) \end{array}}$$

Com que

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

multiplicant per $|b|$, obtenim:

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

i restant $|b|E(a/|b|)$: $0 \leq r < |b|$.

Per veure la unicitat prenem dues possibles solucions q, r i q', r' i veiem que són la mateixa, és a dir: $q = q'$ i $r = r'$. Comencem veient, per RA, que $r = r'$. En efecte, de $a = bq + r = bq' + r'$, deduïm que $b(q - q') = r' - r$ i per tant $b \mid (r' - r)$. Si $r \neq r'$, per la propietat 9 de la divisibilitat, $|b| \leq |r' - r|$. Suposem per comoditat que $r \leq r'$. Llavors $|b| \leq |r' - r| = r' - r$ implica que $r' = |b| + r \geq |b|$, contradicció. Això demostra que $r' = r$. Però llavors $bq + r = bq' + r'$ implica que $bq = bq'$; i com que $b \neq 0$, resulta que $q' = q$. □

Notem que:

- a i b poden ser negatius!
- Si $b \neq 0$ llavors:

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

Exemples:

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

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

$$mcd(a, b) = mcd(a - bq, b) = mcd(r, b),$$

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

Aplicant successivament la fórmula

$$mcd(a, b) = mcd(b, r)$$

per tal de calcular el mcd, anem obtenint una successió de nombres ≥ 0 decreixent $a \geq b > r >$... En algun moment arribarem a 0. El mcd serà l'últim element no nul de la successió (l'últim residu no nul), ja que $mcd(a, 0) = |a|$.

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

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

$r_0 = a, \quad r_1 = b, \quad r_i = q_{i+1} r_{i+1} + r_{i+2}, \quad 0 \leq r_{i+2} < r_{i+1}, \quad i = 0 \ldots n-2$

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

Anem a "acotar" el nombre de passos que fa l'algorisme d'Euclides. La raó d'or és el nombre $\phi = \frac{1+\sqrt{5}}{2}$, que satisfà $\phi^2 = \phi + 1$.

Lema

Siguin $a > b > 0$. Si el nombre de passos (divisions) en l'algorisme d'Euclides és n llavors $a \geq \phi^n$ i $b \geq \phi^{n-1}$.

Demostració: Per inducció simple. Quan $n = 1$ (pas base) és clar, ja que

$$a \geq 2 > \phi \quad \text{i} \quad b \geq 1 = \phi^0.$$

Si $n > 1$ (pas inductiu), fent la divisió Euclidiana de a per b obtenim $a = bq + r$, on q és el quocient i r el residus. Observem que $r > 0$ ja que $n > 1$. Com que el nombre de passos al fer Euclides amb $b > r > 0$ és $n - 1$, per HI tindrem que

$$b \geq \phi^{n-1} \text{ i } r \geq \phi^{n-2}.$$

Llavors, com que $q \geq 1$, tenim:

$$a \geq b + r \geq \phi^{n-1} + \phi^{n-2} = \phi^{n-2}(\phi + 1) = \phi^{n-2}\phi^2 = \phi^n. \qquad \square$$

Aplicant logaritmes: $n \leq 1 + log_\phi b$. És a dir:

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

$$1 + log_\phi b.$$

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

Com que $log_\phi b = log_\phi 2 \, log_2 b < 1.44 \cdot log_2 b$ resulta que ho podem escriure:

$$n < 1 + 1.44 \cdot log_2 b$$

i per tant el nombre de passos sempre és com a molt $1,44$ vegades el nombre de xifres binàries de b.

També $log_\phi b = log_\phi 10 \, log_{10} b < 4,78 \cdot log_{10} b$ resulta que ho podem escriure:

$$n < 1 + 4,78 \cdot log_{10} b$$

i per tant el nombre de passos sempre és com a molt $4,78$ vegades el nombre de xifres decimals de b.

Identitats de Bézout

q		50	5	2		
r	14001	279	51	24	3	0

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

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

24 = **279** + **51**(-5) ⇒ **3** = **51** + **(279** + **51**(-5) **)**(-2) = **279**(-2) + **51** (11)

51 = **14001** + **279**(-50) ⇒ **3** = **279**(-2) + **(14001** + **279**(-50) **)** (11) =

= **14001**(11) + **279**(-552)

Hem arribat a l'expressió següent:

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

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

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

$$mcd(a, b) = ax + by.$$

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

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

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

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

Si ho posem a la taula anterior ampliant-la:

i	*0*	*1*	*2*	*3*	*…*	*n-1*	*n*	
x	1	0	x_2	x_3	…	x_{n-1}	x_n	
y	0	1	y_2	y_3	…	y_{n-1}	y_n	
q		q_1	q_2	q_3	…	q_{n-1}		
r	$r_0 = a$	$r_1 = b$	r_2	r_3	…	r_{n-1}	r_n	0

Aplicat a l'exemple anterior:

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

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

Exercicis.

44. (R algun) Executeu l'algorisme d'Euclides estès per a les parelles de la taula següent. A les columnes de la dreta hi ha les solucions.

a	b
5548	1727
3614	7752
1084	4904
7084	3563
-7084	3563
7084	-3563
-7084	-3563

$mcd(a,b)$	x	y
1	80	-257
2	1435	-669
4	-95	21
7	-85	169
7	85	169
7	-85	-169
7	85	-169

45. (R) Demostreu que la funció $f: \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ definida per $f(x,y) = 5548x + 1727y$ és exhaustiva.

46. Calculeu el mcd i una identitat de Bézout per a les parelles següents: $(512, 88)$, (Solució: $x = 5, y = -29$) $(-512, 88)$ i $(1234, -221)$.

47. Demostreu que la funció $f: \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ definida per $f(x, y) = 1004x + 189y$ és exhaustiva.

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

$$ax + by = a(x + t\tfrac{b}{mcd(a,b)}) + b(y - t\tfrac{a}{mcd(a,b)}).$$

Lemes de Gauss i Euclides

Lema de Gauss:

Si $a \mid bc$ i $mcd(a, b) = 1$ llavors $a \mid c$.

Lema Euclides:

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

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

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

Demostracions:

Lema de Gauss. Com que $mcd(a, b) = 1$, per Bézout sabem que existeixen x, y enters satisfent: $1 = ax + by$.

Multiplicant per c obtenim: $c = acx + bcy$.

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

Lema d'Euclides. Hem de veure que si p no divideix b llavors p divideix c. En efecte: al ser primer, si p no divideix b resulta que $mcd(p, b) = 1$. Aplicant el lema de Gauss tenim que $p|c$. □

Exercicis:

48. Demostreu que si $n \geq 0$, $m > 0$ llavors a^n i $a^m - 1$ són primers entre si.
49. Demostreu que si a, b son primers entre si, llavors $mcd(a, bc) = mcd(a, c)$.
    Pista: Useu el Lema de Gauss.

50. Trobeu tots els enters a tals que $(a+1) \mid a$. Pista: Qui és $mcd(a, a+1)$?

51. Demostreu que els coeficients d'una identitat de Bézout són primers entre sí. *Pista:* dividiu pel mcd i useu l'exercici (*) del tema anterior (o linealitat).

52. Demostreu que si $mcd(a,b) = 1$ llavors $mcd(a^3 + b^2, a^2 b^3) = 1$.

53. (difícil) Demostreu que si a, b són relativament primers, $b \neq 0$ i $\frac{a}{b}$ és un zero del polinomi $c_0 x^n + c_1 x^{n-1} + \cdots + c_{n-1} x + c_0$, llavors $a \mid c_0$ i $b \mid c_n$. (Pista: traieu denominadors i useu el Lema de Gauss i linealitat)

54. (R) Definim el conjunt $M_a = \{ x \in \mathbb{Z} \mid a \mid x \}$.

   a. Si p, q són primers diferents, demostreu que $M_p \cap M_q = M_{pq}$.

   b. Val $M_p \cap M_q = M_{pq}$ per a p, q enters qualssevol? Justifiqueu-ho.

55. (difícil) Demostreu que $\{x + y \mid x \in M_a,\ y \in M_b\} = M_{mcd(a,b)}$. (Pista: useu linealitat i identitats de Bézout).

56. (R algun) Suposem que p és primer. Demostreu que són equivalents:

   a. $p \mid a$.

   b. $mcd(p, a) = p$.

   c. $p \mid a^2$.

   d. $p^2 \mid a^3$.

   Pista: Useu el Lema d'Euclides.

57. Demostreu que si a, b son primers entre si, llavors $mcd(a^3 - b^3, a^4 b^2) = 1$. Pista: useu el Lema d'Euclides i linealitat.

58. Demostreu per inducció que si $p \mid b_1 \cdots b_n$ i p és primer llavors $p \mid b_1$ o $p \mid b_2$ o $\cdots$ o $p \mid b_n$.

59. Demostreu que si $(a+b+c) \mid a^3 + b^3 + c^3$ i $a+b+c$ no és múltiple de 3 llavors $(a+b+c) \mid abc$. Pista: calculeu

$$(a+b+c)(a^2 + b^2 + c^2 - ab - ac - bc)$$

i useu el Lema de Gauss i linealitat.

60. (R) Demostreu que si a i b són primers entre sí, llavors a^4 i $5a^2 + b^3$ també són primers entre sí. Pista: useu el Lema d'Euclides i linealitat.

61. (difícil) Demostreu que hi ha identitats de Bézout per a tres o més enters: Donats $a_1,\ldots,a_n$ existeixen $x_1,\ldots,x_n$ tals que $mcd(a_1,\ldots,a_n) = a_1x_1 + a_2x_2 + \cdots + a_nx_n$ (pista: feu inducció sobre n).

62. (difícil) Donats $a_1,\ldots,a_n$ primers entre si dos a dos, demostreu que existeixen $x_1,\ldots,x_n$ tals que $1 = \sum_{i=1}^{n} x_i \prod_{j\neq i} a_j$. Val el recíproc?

63. (difícil) Donats $a_1,\ldots,a_n$ enters no tots nuls, considerem el conjunt $A = \{a_1x_1 + a_2x_2 + \cdots + a_nx_n \mid x_i \in \mathbb{Z},\ a_1x_1 + a_2x_2 + \cdots + a_nx_n > 0\}$. Demostreu que:
    a. A és no buit.
    b. Demostreu que tot divisor comú de $a_1,\ldots,a_n$ divideix cada element de A. (Pista: linealitat)
    c. El mínim de A divideix cada a_i (Pista: feu la divisió Euclidiana i observeu que el residus també pertany a A).
    d. Deduiu que el mínim de A és $mcd(a_1,\ldots,a_n)$. (Pista: useu b. i c.)
    e. Deduiu que tot divisor comú de $a_1,\ldots,a_n$ divideix $mcd(a_1,\ldots,a_n)$. (Pista: useu b. i e.)

64. Donats $a_1,\ldots,a_n$ enters, demostreu que $\{a_1x_1 + a_2x_2 + \cdots + a_nx_n$: cada x_i és enter $\} = \{x \mid mcd(a_1,\ldots,a_n) \mid x\}$. Pista: useu Linealitat i l'exercici anterior.

65. Demostreu que si a és relativament primer amb cada un dels $b_1,\ldots,b_n$ llavors a és relativament primer amb el seu producte: $b_1\cdots b_n$. Val el recíproc?

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

67. (R) Demostreu que si $a^2 = 5b^2$ llavors tant a com b són múltiples de 5.

68. (R) Demostreu que a, b són primers entre si $\Leftrightarrow$ existeixen x, y tals que $1 = ax + by$.

69. Demostreu que la funció $f: \{0, 1, 2,\ldots, 53, 54\} \times \{0, 1, 2,\ldots, 12, 13\} \to \mathbb{Z}$ definida per $f(x, y) = 14x + 55y$ és injectiva (Pista: Useu el Lema de

Gauss).

70. Demostreu que $mcd(a,b) = 1$ i $mcd(a,c) = 1 \Leftrightarrow mcd(a, bc) = 1$.
71. 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. $mcd(p^2, a) = p^2$.
    e. $p^2 \mid mcd(p^2, a)$.
    f. $p^2 \mid mcd(p^3, a)$.
    g. $p^2 \mid mcd(p^{10}, a)$.

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

Demostració. L'existència ja l'hem fet per inducció completa sobre n. Ara demostrarem, per inducció sobre k, que si tenim primers $p_1, p_2, \dots, p_k, q_1, \dots, q_r$ que estan ordenats en forma creixent: $p_1 \leq p_2 \leq \dots \leq p_k$, $q_1 \leq q_2 \leq \dots \leq q_r$ llavors

$$p_1 p_2 \cdots p_k = q_1 q_2 \cdots q_r \quad \Rightarrow \quad k = r, p_1 = q_1, \dots, p_r = q_r.$$

Si $k = 1$ és obvi, ens centrem en el cas inductiu($k > 1$).
Com que resulta que $p_1 | q_1 q_2 \ldots q_r$, pel Lema d'Euclides, $p_1 | q_j$ per algun j i $q_j | p_i$ per algun i. Com que son primers tenim que $p_1 = q_j \geq q_1$ i per tant $p_1 \geq q_1$. Anàlogament podem veure que $q_1 \geq p_1$ i per tant $p_1 = q_1$. Ara, dividint per $p_1 = q_1$ obtenim que $p_2 \ldots p_k = q_2 \ldots q_r$. Per Hipòtesi d'inducció tenim que $k - 1 = r - 1$, $p_2 = q_2, \ldots, p_r = q_r$. Per tant, $k = r, p_1 = q_1, \ldots, p_r = q_r$. □

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

Descomposició en factors primers amb signe i exponents possiblement nuls.
Tot nombre enter $n \neq 0$ té una descomposició de la forma següent:

$$n = \varepsilon p_1^{e_1} p_2^{e_2} \ldots p_k^{e_k}, \quad \text{on } \varepsilon = \pm 1, \text{ cada } p_i \text{ és primer i cada } e_i \geq 0.$$

Notem que: En aquesta última factorització tant ε com els exponents són únics. Això vol dir que si $\varepsilon p_1^{e_1} p_2^{e_2} \ldots p_k^{e_k} = \varepsilon' p_1^{f_1} p_2^{f_2} \ldots p_k^{f_k}$ llavors $\varepsilon = \varepsilon'$ i $e_i = f_i$ per a cada i. Però ni el k ni els $p_1, \ldots, p_k$ són únics, ja que sempre podem afegir un nou primer amb l'exponent 0. Per exemple

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

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

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

Càlcul del mcd a partir de la factorització i conseqüències

Divisibilitat i càlcul del mcd a partir de la factorització.

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 $(e_1 + 1)(e_2 + 1)\cdots(e_k + 1)$.

Demostracions:

I. $\Rightarrow$) Si $a|b$ resulta $b = ad$, per a un cert $d = \varepsilon_3 p_1^{g_1} p_2^{g_2} \dots p_k^{g_k}$. Llavors $\varepsilon_2 p_1^{f_1} p_2^{f_2} \dots p_k^{f_k} = \varepsilon_1 \varepsilon_3 p_1^{e_1+g_1} p_2^{e_2+g_2} \dots p_k^{e_k+g_k}$. Per la unicitat dels exponents de la descomposició tenim que $f_i = e_i + g_i$. Com que $g_i \geq 0$ obtenim $f_i \geq e_i$. $\Leftarrow$) Recíprocament, si $f_i \geq e_i$ per a cada i resulta que $b = ad$, on $d = \varepsilon_1 \varepsilon_2 p_1^{f_1-e_1} p_2^{f_2-e_2} \dots p_k^{f_k-e_k}$. □

II. El mcd és el nombre més gran possible de la forma $p_1^{g_1} p_1^{g_2} \dots p_1^{g_k}$ tal que $g_i \leq e_i$ i $g_i \leq f_i$ per a cada i. Aquest nombre s'obté fent $g_i = min(e_i, f_i)$. □

III. Es fa igual que 2. □

IV. Surt de 1. □

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

Exercicis:

72. Demostreu que a no divideix b $\Leftrightarrow$ existeixen p primer i $e > 0$ tals que p^e divideix a però p^e no divideix b.
73. Escrivim $n = p_1^{e_1} p_2^{e_2} \dots p_k^{e_k}$ amb cada p_i primer i cada $e_i \geq 0$. Demostreu que: $\sqrt{n}$ és racional $\Leftrightarrow$ tots els e_i són parells.
74.
    a. Demostreu que tot nombre racional $r \neq 0$ es pot escriure de la forma $r = \varepsilon\, p_1^{e_1} p_2^{e_2} \dots p_k^{e_k}$ amb $\varepsilon = \pm 1$, cada e_i enter i cada p_i primer.
    b. Demostreu que tant ε com els e_i són únics.
    c. Demostreu que el criteri de l'exercici anterior també és cert per als racionals.
75. Demostreu que:
    a. $mcd(a^n, b^n) = mcd(a, b)^n$ $(n \geq 0)$ (Pista: useu la descomposició en factors primers).
    b. Si $m \leq n$ llavors $mcd(a, b)^m \mid mcd(a^n, b^m) \mid mcd(a, b)^n$ (pista: useu l'apartat anterior).
    c. Si $m \leq n$ llavors $mcd(a, b)^m \leq mcd(a^n, b^m) \leq mcd(a, b)^n$.
76. Demostreu que si $c \neq 0$ i $a^n \mid b^n c$ per a tot $n \geq 0$ llavors $a \mid b$. Val el recíproc?
77. (R) Si p, q, r són tres nombres primers diferents 2 a 2, calculeu tots el divisors positius de pq^2r^3.
78. Suposem que p és primer, $n \geq 2$ i r, s són enters tals que $n - 1 < r/s \leq n$. Demostreu que són equivalents:
    a. $p^n \mid a$.
    b. $p^r \mid a^s$.
    c. $mcd(p^n, a) = p^n$.
    d. $p^n \mid mcd(p^n, a)$.
    e. $p^n \mid mcd(p^{n+m}, a)$ $(m \geq 0)$.
79. Aquest exercici és continuació d'un exercici anterior, en el qual es demanava

demostrar que la relació en els enters: $aRb \Leftrightarrow a \mid b^n$, $b \mid a^n$ per a un cert $n \geq 1$, és d'equivalència.

a. Demostreu que si $a \neq 0$, $a \mid b^n$ per a un cert $n \geq 1$ si i només si tots els factors primers de a ho són de b.
b. Descriviu la classe d'un enter a.
c. (Difícil) Demostreu que hi ha una bijecció entre $\mathbb{Z} - \{0\}/R$ i el conjunt dels subconjunts finits de nombres primers.

80. Trobeu tots els divisors de 600.
81. Si $mcd(a, b) = p$, on p és primer, raoneu i justifiqueu quins són els possibles valors de:
    a. $mcd(a^2, b)$.
    b. $mcd(a^3, b)$.
    c. $mcd(a^2, b^3)$.
82. Si $mcd(a, b) = p^3$, on p és primer, calculeu $mcd(a^2, b^2)$.
83. Tenim 1000 rajoles quadrades. De quantes maneres es poden disposar de manera que formin un rectangle?

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.

Demostracions: En aquestes demostracions suposem que $a \neq 0, b \neq 0$ i $c \neq 0$, els casos en que $a = 0$ o $b = 0$ o $c = 0$ són trivials i es fan apart. Posem $a = \varepsilon_1 p_1^{e_1} p_2^{e_2} \dots p_k^{e_k}$, $b = \varepsilon_2 p_1^{f_1} p_2^{f_2} \dots p_k^{f_k}$, $c, d = \varepsilon_3 p_1^{g_1} p_2^{g_2} \dots p_k^{g_k}$. Sabem que

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

I. $d \mid a$ i $d \mid b \Leftrightarrow$ per a cada i $g_i \leq e_i$ i $g_i \leq f_i \Leftrightarrow$ per a cada i $g_i \leq min(e_i, f_i) \Leftrightarrow d \mid mcd(a,b)$. □

II. Surt de l'associativitat del mínim:
$min(min(e_i, f_i), g_i) = min(e_i, min(f_i, g_i)) = min(e_i, f_i, g_i)$. □

III. Surt de $min(g_i + e_i, g_i + f_i) = g_i + min(e_i, f_i)$. □

IV. Si posem $c = mcd(a,b)$ i apliquem III: $c = mcd(a,b) = mcd(c\,a/c,\ c\,b/c) = c\,mcd(a/c, b/c)$. Simplificant per $c \neq 0$, obtenim $1 = mcd(a/c, b/c)$. □

V. Es fan igual que en el cas de dos. □

Nota: Una manera de calcular $mcd(a_1, a_2, \dots, a_n)$ sense factoritzar consisteix en aplicar l'associativitat del mcd i en cada pas, calcular el mcd de dos nombres mitjançant l'algorisme d'Euclides.

Exercicis:

84. Demostreu que si $a \mid c$ i $b \mid d$ llavors $mcd(a,b) \mid mcd(c,d)$.

85. Demostreu que si d divideix a i b llavors $mcd(a/d, b/d) = \frac{mcd(a,b)}{|d|}$.

86. Demostreu que si per a cada $j \in \{1,\dots,m\}$ hi ha un $i \in \{1,\dots,n\}$ tal que $a_i \mid b_j$ llavors $mcd(a_1,\dots,a_n) \mid mcd(b_1,\dots,b_m)$.

87. Sigui a enter positiu. Demostreu que si $\sqrt{a}$ és racional llavors a és un quadrat (és igual al quadrat d'un altre nombre enter)

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).

Exemples:

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

De la primera equació és fàcil endevinar solucions. Per exemple, com que $10 - 6 = 4$veiem que $x = 1, y = 1$ és una solució. De fet en podem trobar moltes més, per exemple $x = -2, y = -4$ o també $x = 4, y = 6$. La segona, en canvi no té solució ja que la part esquerra és múltiple de 3 i la dreta no.

En aquest exemple hem trobat un nombre, el 3, que divideix $10 - 6$, però en canvi no divideix 4. Això passa perquè $mcd(3, 6)$ no divideix 5.

Acabem d'observar que si $d = mcd(a, b)$ no divideix c, l'equació (1) no té solució.

Recíprocament, si $d \mid c$, prenent una identitat de Bézout per a, b tenim u, v tals que $au + bv = d$. Multiplicant per $\frac{c}{d}$ queda $a(u\frac{c}{d}) + b(v\frac{c}{d}) = d\frac{c}{d} = c$ i per tant $x = u\frac{c}{d}, y = v\frac{c}{d}$ és una solució. Hem vist, doncs:

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.

Ara anem a veure com son totes les solucions. Suposem que ja hem trobat una solució (x_0, y_0). Si (x, y) és una altre solució $\Rightarrow ax + by = ax_0 + by_0 \Rightarrow$ $a(x - x_0) = b(y_0 - y) \quad \Rightarrow [dividint\ per\ d]$

$$\frac{a}{d}(x - x_0) = \frac{b}{d}(y_0 - y). \qquad (2)$$

Ara, com que $mcd(\frac{a}{d}, \frac{b}{d}) = 1$, pel Lema de Gauss, això implica que $\frac{b}{d}$ divideix $x - x_0$, és a dir ,$x - x_0 = \frac{b}{d}\, t$ per a algun enter t. Substituint a (2) queda $\frac{a}{d}\,\frac{b}{d}\, t = \frac{b}{d}(y_0 - y)$ i simplifican obtenim $y_0 - y = \frac{a}{d}\, t$. Tot plegat, aïllant x, y queda

$$x = x_0 + \frac{b}{d}\, t, \quad y = y_0 - \frac{a}{d}\, t, \quad \text{per a un cert enter } t. \qquad (3)$$

Recíprocament: veiem que una parella (x, y) de la forma (3) satisfà l'equació:
$ax + by = a(x_0 + \frac{b}{d}\, t) + b(y_0 - \frac{a}{d}\, t) = ax_0 + by_0 + \frac{ab}{d}\, t - \frac{ab}{d}\, t = c.$
Tot plegat, hem vist que:

Solució general.

Si x_0, y_0 és una solució particular de l'equació $ax + by = c$, totes les solucions són de la forma:

$$x = x_0 + \frac{b}{d}\,t, \quad y = y_0 - \frac{a}{d}\,t, \quad \text{per a un cert enter } t.$$

Usant notació vectorial, ho podem posar:

$$(x, y) = (x_0, y_0) + \frac{1}{d}\,(b, -a)t \quad \text{amb } t \in \mathbb{Z}$$

Exemple/Exercici: *Trobeu totes les solucions de* $14.001x + 279y = 21$.

Solució: Com que ja tenim una solució particular $x_0 = 77, y_0 = -3.864$ només hem d'aplicar la fórmula: $x = 77 + \frac{279}{3}t, y = -3.864 - \frac{14.001}{3}t$ i queda:

$$x = 77 + 93t, y = -3.864 - 4.667t.$$

Un cop resolta la equació diofàntica, és fàcil verificar les solucions substituint-les a l'equació. En el nostre exemple:

$14.001x + 279y = 14.001(77 + 93t) + 279(-3.864 - 4.667t) =$

$14001 \cdot 77 - 279 \cdot 3.864 + 14001 \cdot 93\,t - 279 \cdot 4.667\,t = 21.$

Això sol no ens assegura que hàgim donat totes les solucions, només que les que hem donat són solucions. Per saber que no ens n'hem deixat cap cal verificar que els coeficients del paràmetre són primers entre sí: $mcd(93, 4667) = 1$.

Verificació de solucions.

l'expressió $x = x_0 + \lambda t,\ y = y_0 + \mu t$ proporciona totes les solucions de l'equació $ax + by = c \Leftrightarrow$ es compleixen dues condicions:

a. Totes les parelles de la forma $x = x_0 + \lambda t, y = y_0 + \mu t$ són solució.

b. $mcd(\lambda, \mu) = 1$

Exercicis:

88. Li demaneu a un amic que multipliqui el dia que va néixer per 12 i el número del mes per 31 i que us digui el resultat de la suma d'aquestes quantitats. El resultat é 500. Esbrineu la data del seu aniversari.
89. (difícil) Demostreu el criteri de verificació de solucions.
90. Un firaire anunciava entrades a 1 € a un recinte sota l'oferta de lliurar 50 € a aquell que li'n donés 5 €. Un cop dins el recinte els explicava que l'única condició era que els 5 € havien de ser amb 20 monedes de 50, 20 o 5 cèntims (i que si no tenien monedes li podien apuntar en un paper la distribució). Al cap d'una estona i per tal que el públic no s'empipés, oferia els 50 € a canvi de 3 €, amb idèntiques condicions. I fins i tot els arribava a oferir en una tercera oportunitat pels assistents, a canvi de 2 €.
    a. Com és que podria oferir 50 € a canvi de 5, 3 o 2? Per quin motiu no els ofereix per 4 €?
    b. Quines combinacions de 20 monedes de 50, 20 i 5 cèntims sumen 4 €?
91. Digueu si les equacions diofàntiques següents tenen solució. Si en tenen, trobeu totes les solucions.
    - (R) $512x + 88y = 20$, $512x + 88y = 40$, $-512x - 88y = 40$ $-512x + 88y = 40$, $512x - 88y = 40$.
    - $1234x + 221y = 20$, $-1234x + 221y = 40$, $-1234x - 221y = 40$.
92. Trobeu la solució (x, y) de les equacions anteriors que tingui la y màxima que sigui menor o igual que -3.
93. (R) Els graus Fahrenheit F i Celsius C estan relacionats per la fórmula: $F = \frac{9}{5}C + 32$. Trobeu totes les solucions enteres d'aquesta equació. Heu de tenir en compte que el zero absolut correspon a $-273.15\,^{\circ}C$.
94. S'ha de començar a jugar un partit de futbol i només disposem de dos rellotges de sorra que mesuren 6 i 11 minuts. És possible mesurar exactament els 45 minuts que ha de durar cada part? Trobeu totes les possibles maneres de fer-ho.
95. Digueu si les equacions diofàntiques següents tenen solució. Si en tenen,

trobeu totes les solucions.

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

96. Trobeu la solució (x, y) de les equacions anteriors que tingui la x positiva mínima.
97. Descomponeu de totes les maneres possibles la fracció $230/247$ en suma de dues fraccions positives de denominadors 19 i 13.

Mínim comú múltiple

El mínim comú múltiple dels nombres enters $a_1, a_2, \ldots, a_n$ és el més petit de tots els múltiples comuns **positius** (> 0) de $a_1, a_2, \ldots, a_n$, 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 $a_1, a_2, \ldots, a_n$ el denotarem per $mcm(a_1, a_2, \ldots, a_n)$.

Definició:

- Si algun $a_i = 0$, $mcm(a_1, a_2, \ldots, a_n) = 0$.
- Si tots el $a_i \neq 0$, el $mcm(a_1, a_2, \ldots, a_n)$ 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:
$mcm(a, b) = mcm(a, -b) = mcm(-a, b) = mcm(-a, -b)$.

Demostracions:

I. Si $a = 0$ o $b = 0$ resulta que $mcm(a, b) = 0$, $|b| = 0$. Si ambdós a, b són no nuls, $|b|$ és un múltiple comú positiu de a, b. I és el màxim, ja que si m' és un múltiple comú positiu de a, b en particular és múltiple de b i per tant $|b| \leq |m'| = m'$.

II. Ja que la divisibilitat no depèn del signe.

Càlcul del mcm a partir de la factorització i conseqüències

Càlcul del mcm a partir de la factorització.

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

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

Aquesta fórmula també val amb més nombres agafant el màxim dels exponents.

Demostració: El mcm és el nombre més petit possible de la forma $p_1^{g_1} p_2^{g_2} \dots p_k^{g_k}$ tal que $g_i \geq e_i$ i $g_i \geq f_i$ per a cada i. Aquest nombre s'obté fent $g_i = max(e_i, f_i)$. □

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

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.

Demostracions: En aquestes demostracions suposem que $a \neq 0$, $b \neq 0$ i $c \neq 0$, els casos en que $a = 0$ o $b = 0$ o $c = 0$ són trivials i es fan apart. Si posem $a = \varepsilon_1 p_1^{\ e_1} p_2^{\ e_2} \dots p_k^{\ e_k}$, $b = \varepsilon_2 p_1^{\ f_1} p_2^{\ f_2} \dots p_k^{\ f_k}$, $c = \varepsilon_3 p_1^{\ g_1} p_2^{\ g_2} \dots p_k^{\ g_k}$, sabem:

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

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

I. $min(e_i, f_i) + max(e_i, f_i) = e_i + f_i$. □

II. $a \mid c$ i $b \mid c \Leftrightarrow e_i \leq g_i$ i $f_i \leq g_i \Leftrightarrow max(e_i, f_i) \leq g_i \Leftrightarrow mcm(a,b) \mid c$. □

III. $max(max(e_i, f_i), g_i) = max(e_i, max(f_i, g_i)) = max(e_i, f_i, g_i)$. □

IV. Es fan igual que en el cas de dos. La **propietat 1 no val** amb 3 o més enters en general: $mcd(a_1, a_2, \dots, a_n)\ mcm(a_1, a_2, \dots, a_n) \neq |a_1, a_2, \dots, a_n|$

Un contraexemple senzill: $mcd(2,2,1) = 1,\ mcm(2,2,1) = 2$

Nota: El càlcul eficient de $mcm(a_1, a_2, \dots, a_n)$ es pot fer usant l'associativitat del mcm i, en cada pas, calcular el mcm de dos mitjançant la fórmula $mcd(a,b)\ mcm(a,b) = |ab|$ i l'algorisme d'Euclides. El càlcul de $mcm(a_1, a_2, \dots, a_n)$ no passa pel de $mcd(a_1, a_2, \dots, a_n)$!!!

Exercicis:

98. Suposem que p és primer. Demostreu que són equivalents:
    a. $p \mid a$.
    b. $mcm(p, a) = |a|$.
    c. $p \mid a^2$.
    d. $p^2 \mid a^3$.
99. Demostreu que si $a_1, \ldots, a_n$ són relativament primers entre si dos a dos, llavors $mcm(a_1, \ldots, a_n) = |a_1 \cdots a_n|$.
100. Demostreu que $mcm(ca, cb) = |c| mcm(a, b)$.
101. (R) Calculeu tots els enters positius a, b tals que $a + b = 57$ i $mcm(a, b) = 680$.
102. Definim el conjunt $M_a = \{ x \in \mathbb{Z} \mid a \mid x \}$. Demostreu que:

$$M_a \cap M_b = M_{mcm(a,b)}.$$

Val aquesta propietat per a tres o més enters? Per a quins enters a, b es compleix $M_a \cap M_b = M_{ab}$?

103. (R algunes) Suposem que p és primer. Demostreu que són equivalents:
    a. $p^2 \mid a$.
    b. $p^4 | a^2$.
    c. $p^3 | a^2$.
    d. $mcm(p^2, a) = |a|$.
    e. $p^2 \mid mcm(p, a)$.
104. Demostreu que si per a cada $i \in \{1,\ldots, n\}$ hi ha un $j \in \{1,\ldots, m\}$ tal que $a_i \mid b_j$ llavors $mcm(a_1,\ldots, a_n) \mid mcm(b_1,\ldots, b_m)$.
105. Demostreu que si d divideix a i b llavors $mcm(\frac{a}{d}, \frac{b}{d}) = \frac{mcm(a,b)}{|d|}$.
106. Suposem que p és primer , $n \geq 2$ i que r, s són enters tals que $n - 1 < r/s \leq n$. Demostreu que són equivalents:
    a. $p^n \mid a$.
    b. $p^r | a^s$.

c. $mcm(p^n, a) = |a|$.

d. $p^n \mid mcm(p, a)$.

e. $p^n \mid mcm(p^{n-1}, a)$.

107. (difícil) Siguin $a_1, a_2, \ldots, a_n$ enters i $n \geq 3$. Demostreu que són equivalents:

a. $mcd(a_1, a_2, \ldots, a_n)\, mcm(a_1, a_2, \ldots, a_n) = |a_1, a_2, \ldots, a_n|$.

b. $a_1, a_2, \ldots, a_n$ són primers entre si dos a dos.

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

109. Demostreu que si $a \neq 0$ i $b \neq 0$, llavors $mcm(a, b) = |ab|$ si i només si a i b són primers entre si.

110. Demostreu que si a, b són primers entre sí i $a \mid c$, $b \mid c$ llavors $ab \mid c$.

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 $m \geq 1$

$a \equiv b \,(mod\, m) \quad \Leftrightarrow \quad m \mid b - a$

$\Leftrightarrow \quad b = a + km$ per un cert k

$\Leftrightarrow \quad a$ i b 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:

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

---

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

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

Classes modulars

La classe de a per la relació de congruència mòdul m es denota per $\overline{a}$ 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:

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

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

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

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

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

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:

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

Demostració: Per linealitat:

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

□

En particular: si $a \equiv a' \,(mod\ m\ )$ llavors $a^n \equiv a'^n \,(mod\ m\ )$ i $ka \equiv ka' \,(mod\ m\ )$.

Exemple 1: Quin és el residu de dividir 58*79 mòdul 11? Hi ha dues maneres de fer-ho. La primera consisteix en efectuar la multiplicació 58*79=4582 i a continuació calcular el residus de 4582. L'altra consisteix en usar que $58 * 79 \equiv 3 * 2 = 6$. Aquí usem que $58 \equiv 3 \,(mod\, 11)$ i $79 \equiv 2 \,(mod\, 11)$ implica que $58 * 79 \equiv 3 * 2 \,(mod\, 11)$. Aquesta segona manera consisteix en "reduir abans de operar". Això sempre simplifica les operacions.

Exemple 2: Calculem les dues últimes xifres de $2^{1000000}$ a mà (no necessitem calculadora). Treballem mòdul 100. Comencem calculant els residus de les primeres potències de 2:

$2^2 = 4,\ \ 2^3 = 8,\ \ \ 2^4 = 16,\ \ \ 2^5 = 32,\ \ \ 2^6 = 64,\ \ \ 2^7 = 128 \equiv 28\ (mod\ 100),$

$2^8 = 2 * 2^7 \equiv 2 * 28 \equiv 56\ (mod\ 100),$

$2^9 = 2 * 2^8 \equiv 2 * 56 \equiv 112 \equiv 12\ (mod\ 100),$

$2^{10} = 2 * 2^9 \equiv 2 * 12 \equiv 24\ (mod\ 100),$

$2^{11} = 2 * 2^{10} \equiv 2 * 24 \equiv 48\ (mod\ 100),$

$2^{12} = 2 * 2^{11} \equiv 2 * 48 \equiv 96 \equiv -4\ (mod\ 100),$

$2^{13} = 2 * 2^{12} \equiv 2 * (-4) \equiv -8\ (mod\ 100),$

… … …

$2^{20} \equiv -24\ (mod\ 100),\ \ 2^{21} \equiv -48\ (mod\ 100),\ \ 2^{22} \equiv 4\ (mod\ 100).$

Aquí ens aturem i observem que hem trobat un primer valor que es repeteix: $2^{22} \equiv 2^2\ (mod\ 100)$

Per tant, també tenim que:

$2^2 \equiv 2^2 2^{20} \equiv 2^2 2^{20} 2^{20} \equiv 2^2 2^{20} 2^{20} 2^{20} \equiv 2^2 2^{20} 2^{20} 2^{20} 2^{20} \equiv \cdots \equiv 2^{2+20k} (mod\ 100)$

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

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

Per tant les dues últimes xifres de $2^{1000000}$ són 76. Observeu que tots aquests càlculs els hem fet sense usar calculadora.

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

Demostracions:

I. $d \mid m$, $m \mid b - a \Rightarrow [transitivitat]$ $d \mid b - a$. □

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

III. ⇒) Si $m \mid b - a$ òbviament $m \mid k(b - a)$.

⇐) Si $m \mid k(b - a)$ i $mcd(k, m) = 1$, pel Lema de Gauss, $m \mid b - a$. □

IV. $m_1 \mid b - a$, … , $m_n \mid b - a \Leftrightarrow mcm(m_1,\dots, m_n) \mid b - a$. □

Exemple: Resolem les congruències:

A. $5x \equiv 10\ (mod\ 9)$

B. $3x \equiv 6\ (mod\ 9)$

C. $15x \equiv 30\ (mod\ 9)$

D. $8x \equiv 28\ (mod\ 6)$

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

B: La segona, simplificant-la per 3 queda $x \equiv 2\ (mod\ 3)$ i per tant, les solucions són de la forma $x = 2 + 3k$ amb $k \epsilon \mathbb{Z}$.

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

D: Simplificant per 2, és equivalent a $4x \equiv 14\ (mod\ 3)$. Com que $mcd(2, 3) = 1$, poden simplificar per 2 i queda equivalent a $2x \equiv 7\ (mod\ 3)$. Aquesta la podem transformar en una diofàntica: $7 = 2x + 3y$, de la que només ens interessa la x.

Resolent-la queda: $x = 2 + 3k$ amb $k \in \mathbb{Z}$.

Exercicis:

1. Demostreu que per a tot $n \geq 0$, $2^4 \cdot 7^{n+1} + (6 \cdot 9^n)^2$ és múltiple de 148 usant inducció i congruències.
2. Demostreu que $ax \equiv b \,(mod\, m)$ té solució $\Leftrightarrow$ $mcd(a, m) \mid b$ (Pista: transformeu la congruència en una equació diofàntica).
3. (R) Sigui p un nombre primer. Demostreu que:
   a. Si $a^2 \equiv b^2 (mod\, p)$ llavors $a \equiv b \ (mod\, p)$ o $a \equiv -b \ (mod\, p)$.
   b. Deduïu que les solucions de la congruència $x^2 \equiv 1 \,(mod\, p)$ són els enters tals que $x \equiv 1 \,(mod\, p)$ o $x \equiv -1 \,(mod\, p)$.
   c. És cert b. si p no és primer?
4. Demostreu que per a tot $n \geq 0$, $15 \cdot 2^{3n+2} + 8(-9)^n$ és múltiple de 68 usant inducció i congruències.
5. (difícil) Demostreu que son equivalents:
   a. $a \equiv b \,(mod\, m)$
   b. $a/mcd(a, b) \equiv b/mcd(a, b) \ (\, mod \ \ m/mcd(a, b, m)\,)$.
6. Demostreu que són equivalents:
   a. $a^n c \equiv b^n d \,(mod\, m)$ per a tot $n \geq 0$.
   b. $c \equiv d \,(mod\, m),\ ac \equiv bd \,(mod\, m)$.
7. Demostreu que $2 \cdot 5^{2n+1} + 8 \cdot 7^n$ és múltiple de 18 per a tot $n \geq 0$. (Pista: useu inducció i congruències)
8. Demostreu que per a $n \geq 0$, $8^{n+1} - 8 - 56n$ és múltiple de 392 usant congruències i inducció.
9. Demostreu que:
   $ka \equiv kb \,(mod\, m) \quad \Leftrightarrow \quad a \equiv b \,(\, mod \ \ m/mcd(k, m)\,)$.
10. Demostreu que:
    $ac \equiv bc \,(mod\, m) \quad \Rightarrow \quad a^n c \equiv b^n c \,(mod\, m) \ \ (n \geq 1)$.

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:

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

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

Quan tenim dues operacions $+, \cdot$ que satisfan totes aqueste propietats es diu tenim un **anell**. Així, $\mathbb{Z}_m$, amb aquestes operacions, és un anell i podem efectuar càlculs de manera anàloga a com ho fem amb els nombres enters. El neutre de la suma és $\overline{0}$, el neutre del producte és $\overline{1}$ i l'invers per la suma de $\overline{a}$ és $\overline{-a}$. Una diferència important respecte a l'aritmètica dels enters és que no podem "simplificar" en general. De de $\overline{a}\cdot\overline{b} = \overline{a}\cdot\overline{c}$ no podem deduir $\overline{b} = \overline{c}$ encara que $\overline{a} \neq \overline{0}$. Per exemple, a $\mathbb{Z}_6$, $\overline{2}\cdot\overline{2} = \overline{2}\cdot\overline{5}$ en canvi $\overline{2} \neq \overline{5}$. Això és degut a que podem tenir $\overline{a}\cdot\overline{b} = \overline{0}$ encara que $\overline{a} \neq \overline{0}, \overline{b} \neq \overline{0}$. Per exemple, a $\mathbb{Z}_6$ $\overline{2}\cdot\overline{3} = \overline{0}$ encara que $\overline{2} \neq \overline{0}, \overline{3} \neq \overline{0}$.

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

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

+	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{0}$	$\overline{1}$
$\overline{3}$	$\overline{3}$	$\overline{4}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{4}$	$\overline{4}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$

Taula del producte a $\mathbb{Z}_5$:

*	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{4}$	$\overline{1}$	$\overline{3}$
$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{1}$	$\overline{4}$	$\overline{2}$
$\overline{4}$	$\overline{0}$	$\overline{4}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

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

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

*	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{4}$	$\overline{0}$	$\overline{2}$	$\overline{4}$
$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{0}$	$\overline{3}$
$\overline{4}$	$\overline{0}$	$\overline{4}$	$\overline{2}$	$\overline{0}$	$\overline{4}$	$\overline{2}$
$\overline{5}$	$\overline{0}$	$\overline{5}$	$\overline{4}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

Observem que les úniques classes que tenen invers són $\overline{1}$ i $\overline{5}$**.**

Exercicis:

11. Demostreu que no hi ha cap enter n tal que $7n + 2$ sigui un cub.
12. Demostreu que per a tot $n \geq 0$, $15 \cdot 2^{3n+2} + 8(-9)^n$ és múltiple de 68.
13. Quina xifra s'ha de posar en el lloc de z perquè el nombre $9z86$ en dividir-lo per 11 tingui residu 5?
14. Demostreu el criteri de divisibilitat següent: n és múltiple de 4 si i només si el nombre format pels dos últims dígits de n és múltiple de 4.
15. Demostreu els criteris de divisibilitat següents:
    a. (R) n és múltiple de 5 si i només si acaba en 0 o en 5.
    b. (R) n és múltiple de 9 si i només si la suma dels dígits de n és múltiple de 9.
16. Quines xifres s'han de posar en el lloc de a, b perquè el nombre $40a9b$ sigui divisible per $2, 3, 5, 11$?
17. (R) Demostreu que no hi ha cap enter n tal que $6n + 5$ sigui un quadrat.
18. Sigui $A_n = 2^n + 2^{2n} + 2^{3n}$.
    a. Demostreu que per a tot $n \geq 0$ el nombre $A_{n+3} - A_n$ és múltiple de 7.
    b. Calculeu el residu de dividir A_{2019} per 7.
19. (R) Demostreu que per a tot $n \geq 0$, $2 \cdot \left(6^{n+1}\right)^2 + 12 \cdot \left(2^{n+1}\right)^3$ és múltiple de 168 usant classes modulars (no cal inducció). Pista: primer treieu factor comú i simplifiqueu.
20. Demostreu que per a tot $n \geq 0$ el nombre $3^{2n+2} - 8n - 9$ és múltiple de 64 usant classes modulars i inducció.
21. Demostreu les propietats I., II. i III. de la suma i el producte a $\mathbb{Z}_m$.
22. Demostreu per inducció que $\overline{a}^{-n} = \overline{a^n}$ per a tot $n \geq 1$.
23. Demostreu que per a tot $m, n \geq 0$ $5^n + 2 \cdot 3^m + 1$ és múltiple de 4.
24. Demostreu que per a tot $n \geq 0$ $19^n + 3^{2n+2}$ acaba en 0 usant classes modulars.
25. Demostreu que tot enter positiu és congruent mòdul 3 amb la suma dels seus dígits en base 10.

26. Demostreu el criteri de divisibilitat següent: n és múltiple de $11 \Leftrightarrow$ la suma dels dígits de n que ocupen un lloc parell menys la suma dels que ocupen un lloc senar és múltiple de 11.
27. Proveu que no hi ha cap enter n tal que $5n + 3$ és un quadrat.

Complement a 2

El complement a 2 s'utilitza per a representar els nombre enters (naturals amb signe). Per exemple, si tenim 3 bits, podem representar els 8 nombres següents:

$$-4, -3, -2, -1, 0, 1, 2, 3.$$

El que es fa senzillament, és pensar aquests 8 nombres a $\mathbb{Z}_8 = \{\overline{0}, \overline{1}, \overline{2},..., \overline{7}\} = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{-4}, \overline{-3}, \overline{-2}, \overline{-1}\}$. La representació mitjançant el complement a 2 consisteix en prendre la representació binària del representant canònic:

nombre	-4	-3	-2	-1	0	1	2	3
representant canònic	4	5	6	7	0	1	2	3
representació complement a 2	100	101	110	111	000	001	010	011

Si, per exemple tenim 8 bits podem representar els nombres:

$$-128, -127,..., -2, -1, 0, 1, 2,... 127.$$

treballant mòdul $2^8 = 256$:

$$\mathbb{Z}_{256} = \{\overline{0}, \overline{1}, \overline{2},..., \overline{127}, \overline{128}, \overline{129},,... \overline{254}, \overline{255}\}$$
$$= \{\overline{0}, \overline{1}, \overline{2},..., \overline{127}, \overline{-128}, \overline{-127},... \overline{-3}, \overline{-2}, \overline{-1}\}$$

Llavors la representació mitjançant complement a 2 de -46 és la representació binària de $256 - 46 = 210$, que és: 11010010.

En general, si tenim N bits podem representar els nombres:

$$-2^{N-1}, \ldots. -1, 0, 1, \ldots, 2^{N-1}-1$$

La representació mitjançant complement a 2 d'un nombre d'aquest, serà la representació binària del representant canònic mòdul 2^N.

$$\mathbb{Z}_{2^N} = \{\overline{0}, \overline{1}, \overline{2}, \ldots, \overline{2^N - 1}\} = \{\overline{-2^{N-1}}, \overline{-2^{N-1}+1}, \ldots \overline{0}, \overline{1}, \overline{2}, \ldots, \overline{2^{N-1}-1}\}.$$

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:

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

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

Ara trobem l'invers modular de $\overline{227}$ a $\mathbb{Z}_{2.292}$. Observeu que el valor de la x no ens importa i no l'hem calculat.

	1	0			x
	0	1	-10	101	-313
q		10	10	3	
r	2.292	227	22	7	1

$1 = 2.292x + 227(-313) \quad \Rightarrow \quad \overline{1} = \overline{2.292x} + \overline{227}\cdot\overline{(-313)} \quad \Rightarrow$
$\overline{1} = \overline{0x} + \overline{227}\,\overline{-313} \quad \Rightarrow \quad \overline{1} = \overline{227}\,\overline{-313}$ i per tant l'invers de $\overline{227}$ a $\mathbb{Z}_{2292}$ és $\overline{-313} = \overline{1.979}$. Això es pot escriure així:

$$\overline{227}^{-1} = \overline{1.979}$$

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

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

Observació: A $\mathbb{Z}_m$ tota classe $\overline{a}$, o bé té invers respecte a la multiplicació o bé hi ha una altre classe $\overline{b} \neq \overline{0}$ tal que $\overline{a}\cdot\overline{b} = \overline{0}$. En el primer cas podrem "simplificar" per $\overline{a}$. En el segon no.

Exercicis:

28. Resoleu l'equació $\overline{5x} - \overline{3} = \overline{29}$ a $\mathbb{Z}_{13}$.
29. Resoleu el sistema $\overline{3x} + \overline{5y} = \overline{0}$, $\overline{2x} - \overline{y} = \overline{1}$ a $\mathbb{Z}_7$ (Sol: $\overline{x} = \overline{2}$, $\overline{y} = \overline{3}$).
30. Resoleu les congruències següents:
    a. $3x \equiv 5\ (mod\ 10)$.
    b. $2x \equiv 4\ (mod\ 10)$.

c. $6x \equiv 4\ (mod\ 10)$.

d. $2x \equiv 7\ (mod\ 10)$.

31. Demostreu que a $\mathbb{Z}_m$ tota classe $\overline{a}$, o bé té invers respecte a la multiplicació o bé hi ha una altre classe $\overline{d} \neq \overline{0}$ tal que $\overline{a}\cdot\overline{d} = \overline{0}$.

32. (R) Resoleu el sistema $\overline{3x} + \overline{5y} = \overline{4}$, $\overline{4x} - \overline{2y} = \overline{2}$ a $\mathbb{Z}_{11}$ (Sol: $\overline{x} = \overline{10},\ \overline{y} = \overline{8}$).

33. Demostreu que l'invers modular, si existeix, és únic (Pista: heu de demostrar que si $\overline{b}$ i $\overline{c}$ són inversos modulars de $\overline{a}$ llavors $\overline{b} = \overline{c}$).

34. (R) Resoleu les congruències següents:

a. $22x \equiv 9\ (mod\ 15)$.

b. $21x \equiv 9\ (mod\ 15)$.

c. $21x \equiv 10\ (mod\ 9)$.

35. Considerem la funció $f: \mathbb{Z}_{29} \to \mathbb{Z}_{29}$ donada per $f(\overline{x}) = \overline{22}\cdot\overline{x} + \overline{7}$.

a. Demostreu que la funció f és bijectiva i doneu la inversa.

b. Considerem l'alfabet de 29 símbols indicat a continuació.

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

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

36. Resoleu el sistema $\overline{4x} + \overline{7y} = \overline{22},\ \overline{3x} + \overline{3y} = \overline{y} + \overline{16}$ a $\mathbb{Z}_{11}$ (Sol: $\overline{x} = \overline{1},\ \overline{y} = \overline{1}$).

37. Resoleu les congruències següents:
    a. $3x \equiv 5\ (mod\ 8)$.
    b. $2x \equiv 4\ (mod\ 8)$.
    c. $6x \equiv 4\ (mod\ 8)$.
    d. $2x \equiv 5\ (mod\ 8)$.
38. Demostreu que el producte de dues classes invertibles de $\mathbb{Z}_m$ és invertible. Qui és l'invers del producte?
39. Demostreu que a per tota classe $\overline{a}$ de $\mathbb{Z}_m$ son 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 $\overline{a}\cdot\overline{d} = \overline{0}$,
40. Sigui $n \geq 1$. Demostreu si a, n són primers entre si, la funció $f: \mathbb{Z}_n \to \mathbb{Z}_n$ donada per $f(\overline{x}) = \overline{a}\cdot\overline{x}$ és bijectiva i doneu la inversa.

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:

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

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:

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

Demostració: com que $x_0 \equiv a_i \,(mod\, m_i)$, resulta que $x \equiv a_i \,(mod\, m_i)$ és equivalent a $x \equiv x_0 \,(mod\, m_i)$. Per la propietat IV de les congruències, el sistema $x \equiv x_0 \,(mod\, m_1)$, ..., $x \equiv x_0 \,(mod\, m_n)$, equival a $x \equiv x_0 \,(\, mod\ \ mcm(m_1,..,m_n)\,)$. □

Això ens diu que resoldre un sistema de congruències es redueix a saber si té solució i trobar-ne una en el cas en que en tingui.

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:

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

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 sistema xinès de dues congruències. A més veiem que:

Existència de solucions.

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

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

- $x \equiv 2\ (mod\ 4),\ \ x \equiv 1\ (mod\ 6)$
- $x \equiv 4\ (mod\ 5),\ \ x \equiv 5\ (mod\ 6)$

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

Exercicis: Resoleu els sistemes següents:

41. $x \equiv 1\ (mod\ 10),\ x \equiv 4\ (mod\ 15),\ \ x \equiv 5\ (mod\ 6)$.
42. $x \equiv 8\ (mod\ 10),\ x \equiv 3\ (mod\ 15),\ \ x \equiv 0\ (mod\ 6)$.
43. $3x \equiv 15\ (mod\ 18),\ 5x \equiv 6\ (mod\ 7),\ x \equiv 5\ (mod\ 8)$.
44. $x \equiv 4\ (mod\ 5),\ x \equiv 5\ (mod\ 6),\ x \equiv 7\ (mod\ 8)$.
45. (R) $x \equiv 1\ (mod\ 4),\ x \equiv 5\ (mod\ 6),\ \ x \equiv 7\ (mod\ 10)$.
46. $3x \equiv 3\ (mod\ 12),\ 15x \equiv 9\ (mod\ 18),\ 2x \equiv 12\ (mod\ 15)$.
47. $x \equiv 2\ (mod\ 4),\ x \equiv 1\ (mod\ 6),\ x \equiv 1\ (mod\ 7)$.
48. $x \equiv 1\ (mod\ 3),\ x \equiv 3\ (\ mod\ 4),\ x \equiv 4\ (mod\ 7),\ \ x \equiv 7\ (mod\ 11)$.

49. 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?

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 $a^{p-1} \equiv 1\ (mod\ p)$.

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

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

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

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

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

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

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

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:

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

Demostració: Hi ha dos casos, segons $p|a$ o no. En el primer cas, com que $n, m \geq 1$ resulta que $p|a^n$, $p|a^m$ i per tant $a^n \equiv a^m \equiv 0\ (mod\, p)$.
En el segon cas, si $n \equiv m\ (\ mod\ (p - 1)\ )$, llavors $n = m + k(p - 1)$ i per tant:
$a^n \equiv a^{m+k(p-1)} \equiv a^m (a^{p-1})^k \equiv a^m 1^k \equiv a^m\ (mod\, p)$. □

Exemple. Calculem el residu de 4^{3141} mòdul 137 reduint amb Fermat. Primer verifiquem que 137 és primer. Com que $3141 \equiv 13\ (mod\ 136)$ tenim que

$$4^{3141} \equiv 4^{13} \equiv 67108864 \equiv 99\ (mod\ 137).$$

Exercicis:

50. Calculeu:
    a. $44^{444}\ (mod\ 13)$.
51. Demostreu que per tot a, $\overline{a}^5 = \overline{a}$ a $\mathbb{Z}_{15}$. (Pista: useu Fermat i la propietat IV de les congruències).
52. Calculeu, usant Fermat i la propietat IV de les congruències:
    a. $11^{1234}\ (mod\ 14)$.
    b. $7^{1234}\ (mod\ 165)$.

53. Calculeu:

a. $19^{1976}\ (mod\ 23)$.

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

c. (R) $25^{1025}\ (mod\ 251)$.

54. Calculeu, usant Fermat i sistemes de congruències:

a. (R) $8^{1235} (mod\ 15)$

b. $1800^{1800}\ (mod\ 77)$.

c. $54321^{54321}\ (mod\ 165)$.

55. Demostreu que per tot a, $\overline{a}^{-13} = \overline{a}$ a $\mathbb{Z}_{91}$. (Pista: useu Fermat i la propietat IV de les congruències).

56. Aquí $p_1, p_2, \ldots, p_r$ són primers diferents, $n, m \geq 1$ i a és un enter qualssevol. Demostreu que:

$$n \equiv m\ (\ mod\ \ mcm(p_1 - 1, \ldots, p_r - 1)\ ) \quad \Rightarrow \quad a^n \equiv a^m\ (mod\ p_1 \cdots p_r)$$

(Pista: useu Fermat i la propietat IV de les congruències).

57. Calculeu:

a. $3^{247}\ (mod\ 17)$.

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

58. Calculeu, usant Fermat i sistemes de congruències:

a. $3^{7000}\ (mod\ 6)$.

b. $50^{810}\ (mod\ 35)$.

c. $12345^{12345}\ (mod\ 210)$.

59. Demostreu que per tot a, $\overline{a}^{-17} = \overline{a}$ a $\mathbb{Z}_{255}$ (Pista: useu Fermat i la propietat IV de les congruències).

El sistema criptogràfic RSA

El sistema criptogràfic RSA es basa en l'aritmètica modular. Hi ha tres nombres bàsics, el mòdul n, l'exponent de xifrat e i l'exponent de desxifrat d. La clau pública la formen (n, e) i el xifrat consisteix bàsicament en elevar a e mòdul n. Com que tothom coneix aquests dos nombres tothom pot xifrar un missatge. El exponent de desxifrat d només el coneix el propietari de la clau i el desxifrat consisteix en elevar a la d mòdul n. El desxifrat només el pot fer el propietari de la clau privada.

Fabricació de les claus

Per fabricar unes claus (part pública i part privada) del sistema RSA comencem triant dos nombre primers grans p, q. Treballarem en aritmètica modular i el mòdul serà $n = pq$. Cal triar p, q grans, aleatoris, de magnitud semblant però que la seva longitud difereixi una mica. La longitud de n expressat en binari rep el nom de **longitud de la clau.**

Denotem $\lambda(n) = mcm(p - 1,\ q - 1)$ (La funció Lambda de Carmichael de n). A continuació triem un nombre e, $1 < e < \lambda(n)$, que sigui relativament primer amb $\lambda(n)$. El nombre e rep el nom d'**exponent de xifrat** (o també **exponent públic**). És convenient (per tal que el xifrat sigui ràpid) triar un nombre no molt gran amb pocs uns a la seva expressió binària (pes de Hamming petit). Per aquesta raó s'agafa moltes vegades el nombre $2^{16} + 1$ (el primer de Fermat F_4), que a més és primer.

Ara calculem un invers d de e mòdul $\lambda(n)$. Sabem que d existeix perquè hem triat e relativament primer amb $\lambda(n)$. Ja hem acabat. El nombre d serà l'**exponent privat** (o també **de desxifrat**).

La **clau pública** és (n, e) y la **clau privada** és (n, d). La part privada de la informació és $p, q, d, \lambda(n)$, que cal mantenir en secret. Si algú coneix qualssevol d'aquests quatre nombres serà capaç de calcular l'exponent privat d i per tant de desxifrar tots els missatges.

Xifrat

Els missatges llargs els trenquem en blocs binaris de longitud menor que la longitud de la clau. Mitjançant l'anomenat **'padding'** (farciment), cada bloc es transforma en un nombre menor que el mòdul de la clau que anomenarem m. A continuació es calcula $m^e \ (mod\, n)$. Aquest nombre, que denotarem per c és el missatge xifrat. Aquest càlcul el fem bloc a bloc.

Desxifrat

Cada bloc rebut c el desxifrem calculant $c^d \ (mod\, n)$. Recuperem el missatge original gràcies al fet següent:

Teorema. Si p, q són primers diferents i $ed \equiv 1 \ (mod\, \lambda(n))$ llavors

$$m^{ed} \equiv m \ (mod\, pq)$$

Demostració. Per la propietat IV de les congruències, això és equivalent a que $m^{ed} \equiv m \ (mod\, p)$ i $m^{ed} \equiv m \ (mod\, q)$. Demostrem la primera congruència, la segona es fa igual. Com que $ed \equiv 1 \ (mod\, \lambda(n))$ resulta que $ed \equiv 1 \ (mod\, (p-1))$ i, per la segona versió del Teorema de Fermat tenim, $m^{ed} \equiv m \ (mod\, p)$. □

Usant el llenguatge de les funcions, el xifrat de blocs és una funció:

$$E\colon \mathbb{Z}_n \to \mathbb{Z}_n$$
$$\overline{x} \to \overline{x}^e$$

Mentre que el desxifrat és la funció:

$$D\colon \mathbb{Z}_n \to \mathbb{Z}_n$$

$$\overline{x} \rightarrow \overline{x}^{d}$$

El teorema anterior diu que $D(E(\overline{x})) = D(\overline{x}^{e}) = \left(\overline{x}^{e}\right)^{d} = \overline{x}^{ed} = \overline{x}$. De la mateixa manera $E(D(\overline{x})) = \overline{x}$. Això demostra que $D \circ E = D \circ E = I_{\mathbb{Z}_n}$ i per tant les funcions de xifrat i desxifrat són inverses l'una de l'altra.

Usant Fermat i sistemes de congruències per a accelerar el desxifrat (i/o el xifrat)

El missatge original es recupera fent $m \equiv c^{d} \ (mod\, pq)$. En lloc de calcular aquesta exponencial modular en farem dues amb mòduls p i q respectivament. Per fer això usem sistemes de congruències i el Teorema de Fermat. Per la propietat IV de les congruències, $x \equiv c^{d} \ (mod\, pq)$ és equivalent al sistema:

$$x \equiv c^{d} \ (mod\, p), \qquad x \equiv c^{d} \ (mod\, q)$$

Ara, amb ajut del Teorema de Fermat reduïm els exponents. Si d_p és el residu de d mòdul $p - 1$ i d_q és el residu de d mòdul $q - 1$ per Fermat tenim que :

$$c^{d} \equiv c^{d_p} (mod\, p) \text{ i } c^{d} \equiv c^{d_q} (mod\, q).$$

Si anomenem m_1 el residu de c^{d_p} mòdul p i m_2 el residu de c^{d_q} mòdul q, hem de resoldre el sistema xinès:

$$x \equiv m_1 \ (mod\, p) \ , \qquad x \equiv m_2 \ (mod\, q)$$

Si denotem per q_{inv} un invers de q mòdul p, és fàcil veure que:

$$m = m_2 + hq, \quad \text{on} \quad h \equiv q_{inv}(m_1 - m_2) \ (mod\, p)$$

Notes:

1. Tria de e: moltes vegades es pren $e = F_4 = 2^{2^4} + 1$, el quart número de Fermat. La raó és que F_4 és primer i hi ha només dos 1 en la seva expressió binària. Això fa que el xifrat sigui molt ràpid.
2. S'utilitzen mètodes de farciment (*padding* en anglès) per seguretat. Consisteixen en afegir informació extra al missatge per tal d'evitar certs perills. Per exemple, amb un missatge molt curt i un exponent de xifratge petit, podria passar que m^e fos menor que el mòdul n, i per tant desxifrable simplement prenent l'arrel e-èssima.
3. A l'article original, els autors (Rivest–Shamir–Adleman) usaven la funció φ d'Euler enlloc de la funció λ de Carmichael. Com que $\varphi(n) = (p-1)(q-1)$ resulta que $\lambda(n) \mid \varphi(n)$ i per tant el que hem demostrat abans per a $\lambda(n)$ també val per a $\varphi(n)$.