Problemes de

FONAMENTS DE LES MATEMÀTIQUES

Agustí Reventós[1]

2014-2015

[1]Molts d'aquests problemes povenen de llibre *Introducció a l'àlgebra abstracta amb elements de matemàtica discreta*, de R. Antoine, R. Camps i J. Moncasi. Jo en vaig escriure la solució durant els cursos 2012-14. Alguns d'ells, com ara els 1 a), 1 b), 1 c), 4, 7, 23, 40, 67, 85, ... els resoldrem aquest curs a Teoria.

Llista 1

Inducció

1. Demostreu que per a tot nombre natural $n \in \mathbb{N}$ es compleix

(a) $1 + 2 + \cdots + n = \dfrac{n(n+1)}{2}$.

(b) $1^2 + 2^2 + \cdots + n^2 = \frac{1}{6}n(n+1)(2n+1)$.

(c) $1^3 + 2^3 + \cdots + n^3 = \frac{n^2(n+1)^2}{4}$.

(d) $n(n^2+5)$ és divisible per 6.

(e) $8^n - 3^n$ és divisible per 5.

(f) $n^2 - 1$ és divisible per 8, quan n és un enter senar.

(g) $n^3 - n$ és divisible per 6.

(h) $2n^3 + 3n^2 + n$ és divisible per 6.

(i) $n! > 2^n$ per a tot $n \geq 4$.

(j) L'expressió decimal de 6^n acaba en 6.

(k) $1 + \dfrac{1}{\sqrt{2}} + \cdots + \dfrac{1}{\sqrt{n}} > 2(\sqrt{n+1} - 1)$.

(l) $\sum_{k=1}^{n}(2k-1)3^k = (n-1)3^{n+1} + 3$.

(m) $1 + \dfrac{1}{4} + \dfrac{1}{9} + \cdots + \dfrac{1}{n^2} \leq 2 - \dfrac{1}{n}$.

(n) $\frac{1}{1\cdot 3} + \frac{1}{3\cdot 5} + \frac{1}{5\cdot 7} + \cdots + \frac{1}{(2n-1)\cdot(2n+1)} = \frac{n}{2n+1}$.

(o) $1 + 4 + 7 + \cdots + (3n-2) = \frac{n(3n-1)}{2}$.

(p) $(1 + 2 + 3 + \cdots + n)(1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{n}) \geq n^2 + n - 1, \quad n \geq 3$.

(q) $9 \cdot 2^n$ és pot escriure, per a tot $n \in \mathbb{N}$, com suma de tres quadrats.

(r) $1 + 3 + 5 + \cdots + (2n+1) = (n+1)^2$.

Solució: *El cas $n = 1$ el deixem sempre al lector.*

(a) Per H.I. tenim

$$1 + 2 + \cdots + (n-1) + n = \left[\frac{(n-1)((n-1)+1)}{2}\right] + n = \frac{n(n+1)}{2}.$$

Una altra manera elegant d'obtenir aquest resultat és contar els signes $*$ i $+$ de la taula següent:

$$\begin{array}{cccc} * & * & * & * \\ + & * & * & * \\ + & + & * & * \\ + & + & + & * \\ + & + & + & + \end{array}$$

(b) Per H.I. tenim

$$\begin{aligned} 1^2 + 2^2 + \cdots + n^2 &= \left[\frac{1}{6}(n-1)(n-1+1)(2(n-1)+1)\right] + n^2 \\ &= \frac{1}{6}(n-1)n(2n-1) + n^2 \\ &= \frac{n((n-1)(2n-1)+6n)}{6} \\ &= \frac{n(2n+1)(n+1)}{6}. \end{aligned}$$

Una manera molt elegant d'obtenir aquest resultat és considerar la taula

$$\begin{aligned} 1^3 &= 1 \\ (1+1)^3 &= 1^3 + 3 \cdot 1^2 + 3 \cdot 1 + 1 \\ (2+1)^3 &= 2^3 + 3 \cdot 2^2 + 3 \cdot 2 + 1 \\ \vdots &= \vdots \\ (n+1)^3 &= n^3 + 3 \cdot n^2 + 3 \cdot n + 1 \end{aligned}$$

i sumar-la per columnes (els cubs de l'esquerra es cancel·len amb els cubs de la dreta). Obtenim

$$(n+1)^3 = 1 + 3\left[\Sigma_{k=1}^{n} k^2\right] + 3\frac{n(n+1)}{2} + n.$$

Aïllant el sumatori obtenim el resultat.

Encara una altra manera és escriure la fórmula com

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

i contar la suma de $+,0,x$ *que apareixen a la taula següent (pot ajudar el problema 1 (r) per comptar el número de* $0's$*).*

x	x	x	x	0	$+$	$+$	$+$	$+$	
x	x	x	x	0	$+$	$+$	$+$	$+$	
x	x	x	x	0	$+$	$+$	$+$	$+$	
x	x	x	x	0	$+$	$+$	$+$	$+$	
x	x	x	0	0	0	$+$	$+$	$+$	
x	x	x	0	0	0	$+$	$+$	$+$	
x	x	x	0	0	0	$+$	$+$	$+$	
x	x	0	0	0	0	0	$+$	$+$	
x	x	0	0	0	0	0	$+$	$+$	
x	0	0	0	0	0	0	0	$+$	

(c) Per H.I. tenim

$$1^3+2^3+\cdots+n^3=\frac{(n-1)^2n^2}{4}+n^3=\frac{n^2(n-1)^2+4n^3}{4}=\frac{n^2(n+1)^2}{4}.$$

(d) Sense inducció és molt simple:

$$n(n^2+5)=n(n^2+6-1)=\dot{6}+n(n^2-1)=\dot{6}+(n-1)n(n+1)$$

i al multiplicar tres números consecutius sempre hi ha un múltiple de dos i un múltiple de tres de manera que $(n-1)n(n+1)=\dot{6}$ *i hem acabat.*

Aquesta darrera observació (que $(n-1)n(n+1)=\dot{6}$*) la podem provar per inducció així:*

$$(n-1)n(n+1)=(n-1)n(n-2+3)=(n-2)(n-1)n+3(n-1)n=\dot{6}+3(n-1)n$$

però el producte de don números consecutius sempre és parell, i hem acabat.

Una altra manera és veure, fent petites manipulacions, que

$$n(n^2+5)=(n-1)((n-1)^2+5)+3n^2-3n+6$$

El primer terme de la dreta és múltiple de 6 *(per H.I.) i* $3n^2-3n+6$ *també ho és.*

(e) Per H.I. tenim

$$8^{n-1}-3^{n-1}=\dot{5}.$$

Així

$$8^n=8(3^{n-1}+\dot{5})=8\cdot3^{n-1}+\dot{5}.$$

Per tant

$$8^n-3^n=8\cdot3^{n-1}+\dot{5}-3^n=3^{n-1}(8-3)+\dot{5}=\dot{5}.$$

(f) *Si $n = 2k+1$, $n^2-1 = 4k(k+1)$ i el producte de dos nombres consecutius és sempre parell. Si es volgués demostrar per inducció que $k(k+1)$ és múltiple de dos podem escriure $(k-1)k = (k+1-2)k = k(k+1) - \dot{2}$.*

(g) *Observem que $n^3 - n = n(n^2-1) = n(n+1)(n-1)$ i apliquem l'apartat (d).*

(h) *El polinomi donat es pot escriure com $2n(n+1)(n+\frac{1}{2})$ de manera que tot està en demostrar que*

$$n(n+1)(n+\frac{1}{2}) = \dot{3}.$$

Però

$$n(n+1)(n+\frac{1}{2}) = n(n+1)(n+2-\frac{3}{2}) = n(n+1)(n+2) - \frac{3}{2}n(n+1).$$

Però com que el producte de tres nombres consecutius és múltiple de 6 i el producte de dos nombres consecutius és parell, hem acabat.

Una altra manera on la inducció és veu molt clara és adonar-se que

$$2n^3 + 3n^2 + n = \left[2(n-1)^3 + 3(n-1)^2 + (n-1)\right] + 6n^2.$$

(i) *El nombre natural més petit que compleix $n! > 2^n$ és $n = 4$. Per H.I. tenim*

$$n! = n(n-1)! > n2^{n-1}$$

i ara ens preguntem si $n2^{n-1} > 2^n$. Igualtat certa per a $n \geq 3$, però com estem treballant només amb $n \geq 4$, aquesta igualtat és certa.

(j) *Per H.I.*

$$6^{n-1} = 6 + \dot{10}.$$

Per tant

$$6^n = 6^{n-1} \cdot 6 = (6 + \dot{10})6 = 36 + \dot{10} = (6 + \dot{10}) + \dot{10} = 6 + \dot{10}.$$

(k) *Per H.I. tenim*

$$1 + \frac{1}{\sqrt{2}} + \cdots + \frac{1}{\sqrt{n-1}} > 2(\sqrt{n} - 1).$$

Per tant,

$$1 + \frac{1}{\sqrt{2}} + \cdots + \frac{1}{\sqrt{n-1}} + \frac{1}{\sqrt{n}} > 2(\sqrt{n} - 1) + \frac{1}{\sqrt{n}}.$$

I ara hem de veure que

$$2(\sqrt{n} - 1) + \frac{1}{\sqrt{n}} > 2(\sqrt{n+1} - 1). \tag{1.1}$$

Multiplicant per $\sqrt{n}$ ens queda

$$2n + 1 > 2\sqrt{n}\sqrt{n+1}$$

I elevant al quadrat

$$1 + 4n > 4n.$$

Com aquesta igualtat és certa, la igualtat (1.1) també ho és.

(l) Per H.I. tenim

$$\sum_{k=1}^{n}(2k-1)3^k = (n-2)3^n + 3 + (2n-1)3^n = (n-1)3^{n+1} + 3.$$

(m) Per H.I. tenim

$$1 + \frac{1}{4} + \frac{1}{9} + \cdots + \frac{1}{n^2} \leq 2 - \frac{1}{n-1} + \frac{1}{n^2}.$$

I ara hem de veure que

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

Simplificant el 2 *i manipulant una mica, aquesta igualtat resulta ser equivalent a*

$$\frac{n^2-1}{n^2} \leq 1$$

la qual és certa.

(n) Per H.I. tenim

$$\frac{1}{1\cdot 3} + \frac{1}{3\cdot 5} + \frac{1}{5\cdot 7} + \cdots + \frac{1}{(2n-1)\cdot(2n+1)} = \frac{n-1}{2(n-1)+1} + \frac{1}{(2n-1)\cdot(2n+1)} = \frac{n}{2n+1}.$$

(o) Per H.I. tenim

$$1 + 4 + 7 + \cdots + (3n-2) = \frac{(n-1)(3(n-1)-1)}{2} + 3n - 2 = \frac{n(3n-1)}{2}.$$

(p) Com el mètode d'inducció és molt fàcil d'aplicar quan hi ha sumes 'de 1 *fins a* n*' reescrivim l'enunciat així:*

$$1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{n} \geq \frac{2(n^2+n-1)}{n(n+1)}$$

Per H.I. tenim

$$1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{n} \geq \frac{2((n-1)^2+(n-1)-1)}{(n-1)n} + \frac{1}{n}$$

Equivalentment

$$1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{n} \geq \frac{2n^2-n-3}{(n-1)n}$$

Per tant, tan sols hem de veure que

$$\frac{2n^2-n-3}{(n-1)n} \geq \frac{2(n^2+n-1)}{n(n+1)}$$

Simplificant es veu immediatament que aquesta desigualtat és equivalent a

$$n^2 \geq 5,$$

la qual és certa per a $n \geq 3$*, com volíem veure.*

(q) *Suposarem primer que n és parell. Hem d'escriure $9 \cdot 2^{2k}$ com suma de tres quadrats. Per H.I. (sobre k) tenim*

$$9 \cdot 2^{2k} = 9 \cdot 2^{2(k-1)} \cdot 2^2 = (a^2 + b^2 + c^2)2^2 = (2a)^2 + (2b)^2 + (2c)^2.$$

Si n és senar, per H.I. (sobre k) tenim

$$9 \cdot 2^{2k+1} = 9 \cdot 2^{2(k-1)+1+2} = 9 \cdot 2^{2(k-1)+1}2^2 = (a^2 + b^2 + c^2)2^2 = (2a)^2 + (2b)^2 + (2c)^2.$$

El punt central ha estat notar que $9 = 1 + 4 + 4$ i $18 = 1 + 1 + 16$. En canvi 18 no és 9 per un quadrat.

(r) *Per H.I tenim*

$$1 + 3 + 5 + \cdots + (2n + 1) = n^2 + (2n + 1) = (n + 1)^2.$$

Una manera elegant de veure aquest resultat és observar el dibuix següent i calcular l'àrea de dues maneres diferents.

7	*7*	*7*	*7*
5	*5*	*5*	*7*
3	*3*	*5*	*7*
1	*3*	*5*	*7*

2. Digueu on falla la demostració del teorema següent:

Teorema. *Tots els alumnes de la classe es diuen igual.*

Demostració. Apliquem el principi d'inducció sobre el nombre n d'alumnes que hi ha a classe.
Si $n = 1$, clarament tots els alumes es diran igual.
Suposem, per inducció, que el resultat és cert quan la classe té $n - 1$ alumnes.
Considerem ara que la classe té n alumnes. Demanem a un alumne que surti al carrer i tindrem una classe amb $n - 1$ alumnes que, per hipòtesi d'inducció es diuen igual (independentment de si són nois o noies), direm que es diuen *Joan*. Així tenim que tota la classe es diu Joan, excepte, potser, el noi de fora. El fem entrar i en fem sortir un altre. De nou tenim una classe amb $n - 1$ alumnes que per inducció es diuen igual, però ja sabem que tots es deien Joan, per tant el primer noi que havia sortit també es diu Joan. □

Solució: *Penseu la següent reformulació: Si en una classe de n alumnes n'hi un que es diu Joan, tots es diuen Joan. Penseu llavors en una classe de dos alumnes.*

3. Trobeu una fórmula per a la suma d'angles d'un polígon de n costats i demostreu-la.

Solució: *Aplicant el teorema de les 'tourning tangents', o menys pedantment mirant que fa un misto quan li fem donar una volta al voltant del polígon tenim que*

$$\sum_i (\pi - \alpha_i) = 2\pi$$

on α_i *són els angles interiors. Per tant,*

$$n\pi - S(n) = 2\pi,$$

on $S(n) = \sum_i \alpha_i$ *és la suma dels angles interiors. És a dir*

$$S(n) = (n-2)\pi.$$

També es pot demostrar per inducció de la manera següent.
Explicitem primer el resultat que volem demostrar: La suma dels angles interns d'un polígon de n costats val $S(n) = (n-2)\pi$.
Si $n = 3$ *aquest enunciat diu:* La suma dels angles interns d'un triangle val $S(3) = (3-2)\pi = \pi$, *resultat que sabem cert (en geometria euclidiana).*
H.I: Suposem el resultat cert fins a $n-1$*:* La suma dels angles interns d'un polígon de $n-1$ costats val $S(n-1) = (n-1-2)\pi$.
Considerem ara un polígon de n *costats i el polígon de* $n-1$ *costats que obtenim en unir dos vèrtexs alterns (per exemple, l'*1 *i el* 3 *si orientem el vèrtexs a favor o en contra del rellotge). Llavors*

$$S(n) = S(n-1) + \pi$$

ja que els angles del triangle format pels vèrtex $1, 2, 3$ *sumen* π*. Així*

$$S(n) = (n-3)\pi + \pi = (n-2)\pi.$$

4. Sigui $\{a_n\}_{n\in\mathbb{N}}$ una successió de nombres reals.

(a) $\{a_n\}_{n\in\mathbb{N}}$ es diu aritmètica si existeix un $d \in \mathbb{R}$ tal que per a tot $i \geq 1$, $a_{i+1} = a_i + d$.

(b) $\{a_n\}_{n\in\mathbb{N}}$ es diu geomètrica si existeix un $r \in \mathbb{R}$ tal que per a tot $i \geq 1$, $a_{i+1} = r.a_i$.

Per a cadascun dels casos trobeu una fórmula per la suma dels n primers termes de la successió $S_n = a_1 + a_2 + \cdots + a_n$, i demostreu-la per inducció.

Solució: *Estudiem només el cas de les progressions geomètriques. Tenim*

$$S(n) = a_1 + \cdots + a_n = a_1(1 + r + r^2 + \cdots + r^{n-1}),$$

de manera que

$$rS(n) = a_1(r + r^2 + r^3 + \cdots + r^n).$$

Així

$$S(n) - rS(n) = a_1(1 - r^n)$$

i per tant

$$S(n) = \frac{a_1(1 - r^n)}{1 - r}.$$

Si la volem demostrar per inducció observem que aquesta fórmula és certa per a $n = 1$. Suposem-la certa fina a $n - 1$, és a dir

$$S(n-1) = \frac{a_1(1 - r^{n-1})}{1 - r}.$$

Llavors tenim

$$S(n) = a_1 + \cdots + a_{n-1} + a_n = S(n-1) + a_n = \frac{a_1(1 - r^{n-1})}{1 - r} + r^{n-1}a_1 = \frac{a_1(1 - r^n)}{1 - r}.$$

5. (*Nombres de Fibonacci*) Denotem per F_n, $n \geq 1$, els nombres de Fibonacci que es defineixen de la manera següent:

(i) $F(1) = 1$, $F(2) = 1$.

(ii) $F(n) = F(n-1) + F(n-2)$ si $n \geq 3$.

Així doncs tenim els nombres següents:

$$1, 1, 2, 3, 5, 8, 13, 21, \ldots$$

Aquest nombres són la pera, però aquí només veurem algunes propietats.

1. Per a tot $n \geq 1$, F_{3n} és parell.
2. Per a tot $n \geq 1$, F_{4n} és divisible per 3.
3. Més generalment, proveu que si $k \mid n$ aleshores $F_k \mid F_n$.
4. Proveu per inducció la fórmula general dels nombres de Fibonacci:

$$F_n = \frac{1}{\sqrt{5}}\left(\frac{1+\sqrt{5}}{2}\right)^n - \frac{1}{\sqrt{5}}\left(\frac{1-\sqrt{5}}{2}\right)^n.$$

Solució: *1) Per H.I. tenim que $F_{3(n-1)}$ és parell. Així*

$$F_{3n} = F_{3n-1} + F_{3n-2} = (F_{3n-2} + F_{3n-3}) + F_{3n-2} = 2F_{3n-2} + F_{3n-3}$$

i per tant F_{3n} és parell.

2) Per H.I. $F_{4n-4} = \dot{3}$. *Llavors*

$$\begin{aligned} F_{4n} &= F_{4n-1} + F_{4n-2} = (F_{4n-2} + F_{4n-3}) + (F_{4n-3} + F_{4n-4}) \\ &= (F_{4n-3} + F_{4n-4} + F_{4n-3}) + (F_{4n-3} + F_{4n-4}) \\ &= 3F_{4n-3} + 2F_{4n-4} = \dot{3}. \end{aligned}$$

3) Suposem $n = km$. *Per H.I. sobre* m *tenim* $F_{k(m-1)} = \dot{F}_k$. *Llavors*

$$\begin{aligned} F_n &= F_{n-1} + F_{n-2} = 2F_{n-2} + F_{n-3} \\ &= 3F_{n-3} + 2F_{n-4} = 5F_{n-4} + 3F_{n-5} \\ &= 8F_{n-5} + 5F_{n-6} \end{aligned}$$

Veiem que sempre apareixen dos nombres de Fibonacci consecutius afectats d'uns coeficients que tornen a ser justament nombres de Fibonacci. Continuant el desenvolupament anterior k *vegades obtenim*

$$F_n = \alpha F_{n-k+1} + \beta F_{n-k}$$

però justament $\alpha = F_k$ *i per tant* $F_n = \dot{F}_k$ *com volíem.*

(4) Denotem $\tau = (1+\sqrt{5})/2$ *i* $\sigma = (1-\sqrt{5})/2$. *Observem que* τ *és la raó d'or, i per tant, tant* τ *com* σ *són arrels de l'equació* $1 + x = x^2$. *Hem de demostrar que*

$$F_n = \frac{1}{\sqrt{5}} \left(\tau^n - \sigma^n\right).$$

Per H.I. forta tenim

$$\begin{aligned} F_n &= F_{n-1} + F_{n-2} = \frac{1}{\sqrt{5}} \left((\tau^{n-1} + \tau^{n-2}) - (\sigma^{n-1} + \sigma^{n-2})\right) \\ &= \frac{1}{\sqrt{5}} \left(\tau^{n-2}(\tau+1) - \sigma^{n-2}(\sigma+1)\right) \\ &= \frac{1}{\sqrt{5}} \left(\tau^{n-2} \cdot \tau^2 - \sigma^{n-2} \cdot \sigma^2\right) \\ &= \frac{1}{\sqrt{5}} \left(\tau^n - \sigma^n\right) \end{aligned}$$

6. Siguin F_n els números de Fibonacci tal i com estan definits a l'exercici anterior.

1. Proveu per inducció que $1 < \frac{F_{n+1}}{F_n} < 2$ per a tot $n > 2$.
2. Proveu que $F_n^2 = F_{n-1}F_{n+1} + (-1)^{n+1}$.

Solució: *1) Per H.I. tenim*

$$1 < \frac{F_n}{F_{n-1}} < 2$$

Invertint

$$1 > \frac{F_{n-1}}{F_n} > \frac{1}{2}.$$

Sumant 1,

$$2 > 1 + \frac{F_{n-1}}{F_n} > \frac{3}{2} > 1.$$

Per altra banda

$$\frac{F_{n+1}}{F_n} = \frac{F_n + F_{n-1}}{F_n} = 1 + \frac{F_{n-1}}{F_n}$$

quantitat que acabem de veure que està estrictament entre 1 *i* 2.

2) Per H.I. tenim

$$F_{n-1}^2 = F_{n-2}F_n + (-1)^n.$$

Ara bé,

$$\begin{aligned} F_n^2 &= F_{n-1}^2 + F_{n-2}^2 + 2F_{n-1}F_{n-2} \\ &= F_{n-2}F_n + (-1)^n + F_{n-2}^2 + 2F_{n-1}F_{n-2} \end{aligned}$$

Tenint en compte que $F_{n-2} = F_n - F_{n-1}$ *ens queda*

$$F_n^2 = (F_n - F_{n-1})F_n + (-1)^n + (F_n - F_{n-1})^2 + 2F_{n-1}(F_n - F_{n-1})$$

Simplificant

$$\begin{aligned} F_n^2 &= 2F_n^2 - F_{n-1}^2 - F_nF_{n-1} + (-1)^n \\ &= 2F_n^2 - F_{n+1} \cdot F_{n-1} + (-1)^n \end{aligned}$$

Equivalentment

$$F_n^2 = F_{n+1} \cdot F_{n-1} - (-1)^n = F_{n+1} \cdot F_{n-1} + (-1)^{n+1}$$

com volíem.

7. Sigui τ la raó d'or. Demostreu que

$$\tau = 2\cos\frac{\pi}{5},$$

i que també

$$\tau = \sqrt{1 + \sqrt{1 + \sqrt{1 + \sqrt{1 + \ldots}}}}.$$

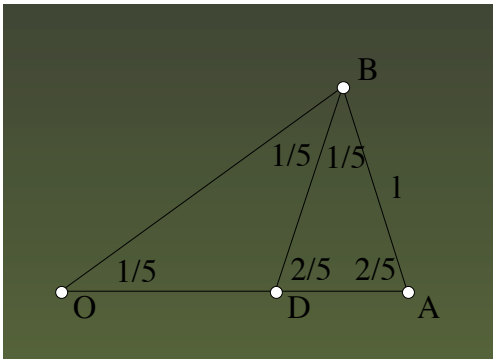
Demostreu a continuació que el quocient entre termes consecutius F_n i F_{n-1} de la succesió de Fibonacci es va apropant a la raó àuria:

$$\lim_{n\to\infty} \frac{F_n}{F_{n-1}} = \tau.$$

Solució: *Recordeu que una de les maneres d'obtenir la raó d'or τ és com*

$$\tau = \frac{c}{b}$$

on c és la longitud dels costats iguals en un triangle isòsceles d'angles $\frac{2\pi}{5}, \frac{2\pi}{5}, \frac{1\pi}{5}$ i base b. A la figura $c = OB = OA$, $b = AB$.



Observem $AD = c - b$, ja que els triangles $\triangle DOB$ i $\triangle BDA$ són isòsceles. Llavors com que els triangles $\triangle OAB$ i $\triangle BDA$ són semblants, tenim

$$\frac{c}{b} = \frac{b}{c-b}.$$

Equivalentment

$$\tau = \frac{1}{\tau - 1},$$

d'on

$$\tau = \frac{1+\sqrt{5}}{2}$$

(no considerem l'arrel negativa).
Per tant, considerant l'altura des de O, tenim

$$\cos\frac{2\pi}{5} = \frac{b/2}{c}$$

és a dir

$$\cos\frac{2\pi}{5} = \frac{1}{2\tau}.$$

Per la fórmula de l'angle doble tenim

$$\frac{1}{2\tau} = \cos\frac{2\pi}{5} = 2\cos^2\frac{\pi}{5} - 1$$

d'on

$$2\cos^2\frac{\pi}{5} = \frac{1}{2\tau} + 1 = \frac{\tau^2}{2}$$

i per tant (recordem que $\tau^2 = \tau + 1$)

$$\tau = 2\cos\frac{\pi}{5}.$$

Per demostrar que

$$\tau = \sqrt{1+\sqrt{1+\sqrt{1+\sqrt{1+\ldots}}}}$$

només cal observar que posant

$$a = \sqrt{1+\sqrt{1+\sqrt{1+\sqrt{1+\ldots}}}}$$

i elevant al quadrat els dos termes d'aquesta igualtat obtenim

$$a^2 = 1+\sqrt{1+\sqrt{1+\sqrt{1+\ldots}}}$$

Però com que hi ha infinits termes, aquesta igualtat també es pot escriure com

$$a^2 = 1 + a$$

i per tant a és arrel del polinomi $x^2 - x - 1$, i.e. $a = \tau$.
Finalment, l'apartat 4 del problema 5 ens diu que

$$F_n = \frac{1}{\sqrt{5}}(\tau^n - (-\frac{1}{\tau})^n)$$

Com $\lim_{n\to\infty} \frac{1}{\tau^n} = 0$ tenim

$$\lim_{n\to\infty}\frac{F_n}{F_{n-1}} = \lim_{n\to\infty}\frac{\tau^n - (-\frac{1}{\tau})^n}{\tau^{n-1} - (-\frac{1}{\tau})^{n-1}} = \tau.$$

8. Tenim peces formades per quadrats vermells 1×1 i rectangles grocs 2×1 que suposem situats horitzontalment. Quantes tires (rectangles $n\times 1$) diferents (en algun lloc no tenen el mateix color) de longitud n podem formar?

Solució: *Les tires de longitud n es formen o bé afegint un quadrat vermell a les tires de longitud $n-1$, o bé afegint dos quadrats grocs a les tires de longitud $n-2$. Per tant, denotant per L_n les tires diferents de longitud n tenim*

$$L_n = L_{n-1} + L_{n-2}.$$

Per tant L_n és el terme general de la successió de Fibonacci que comença amb $L_1 = 1$ i $L_2 = 2$ (un rectangle groc o dos quadrats vermells).

9. Denotarem per D_n les diferents maneres de cobrir una quadrícula de mida $2 \times n$ amb peces de dominó de mida 2×1. Observeu que $D_1 = 1$, $D_2 = 2$, $D_3 = 3$. Trobeu una fórmula general per a D_n.

Solució: *Podem passar d'una solució $2 \times (n-1)$ a una solució $2 \times n$ simplement afegint una peça de dominó verticalment al final. Podem passar d'una solució $2 \times (n-2)$ a una solució $2 \times n$ simplement afegint dues peces de dominó horitzontalment al final. A més, tota solució $2 \times n$ es construeix d'aquesta manera. Per tant*

$$D_n = D_{n-1} + D_{n-2},$$

i D_n és el terme general de la successió de Fibonacci que comença amb $D_1 = 1$ i $D_2 = 2$.

10. Sigui x un nombre real i n un nombre natural. Deduïu una fórmula per al producte

$$(1+x) \cdot (1+x^2) \cdot (1+x^4) \cdot (1+x^8) \cdot \cdots \cdot (1+x^{2^n})$$

i demostreu-la per inducció.

Solució: *Observem que*

$$(1+x)(1+x^2) = 1 + x + x^2 + x^3.$$

Això suggereix que

$$(1+x) \cdot (1+x^2) \cdot (1+x^4) \cdot (1+x^8) \cdot \cdots \cdot (1+x^{2^n}) = 1 + x + x^2 + \cdots + x^a,$$

on $a =$ grau del polinomi, és a dir

$$a = 1 + 2 + 2^2 + 2^3 + \cdots + 2^n = 2^{n+1} - 1.$$

Demostrem ara aquesta fórmula per inducció. Suposem-la certa fins a $n-1$. llavors tenim

$$\begin{aligned}
& (1+x) \cdot (1+x^2) \cdots (1+x^{2^{n-1}})(1+x^{2^n}) \\
= & \sum_{k=1}^{2^n-1} x^k \cdot (1+x^{2^n}) \\
= & \sum_{k=1}^{2^n-1} x^k + \sum_{k=1}^{2^n-1} x^{k+2^n} \\
= & \sum_{k=1}^{2^n-1} x^k + \sum_{j=2^n}^{2^{n+1}-1} x^j \\
= & \ 1 + x + x^2 + \cdots + x^a.
\end{aligned}$$

11. Demostreu que per a tot nombre real positiu $a \geq 0$ i per a tot número natural n, es compleix que

$$\sqrt{a+1+\sqrt{a+2+\cdots+\sqrt{a+n}}} < a+3.$$

Observeu que en particular tenim, per a tot nombre natural n,

$$\sqrt{1+\sqrt{2+\cdots+\sqrt{n}}} < 3.$$

Solució: *Per H.I. suposem que per tot $a \geq 0$ i per tot $n \in \mathbb{N}$ tenim*

$$\sqrt{a+1+\sqrt{a+2+\cdots+\sqrt{a+n-1}}} < a+3.$$

Com això és cert per tot $a \geq 0$ ho apliquem a $a+1$ i tenim

$$\sqrt{a+2+\sqrt{a+3+\cdots+\sqrt{a+n}}} < a+4.$$

Per tant

$$\sqrt{a+1+\sqrt{a+2+\cdots+\sqrt{a+n}}} < \sqrt{a+1+a+4}$$

Però ara és fàcil veure (elevant al quadrat) que

$$\sqrt{2a+5} < a+3$$

i hem acabat.

12. Sigui $X = \{x_1, \ldots, x_n\}$ un conjunt amb n elements.

1. $\mathcal{P}(X)$ denota el conjunt de les parts de X. Proveu que $|\mathcal{P}(X)| = 2^n$.
2. Per a qualsevol $0 \leq k \leq n$, $\mathcal{P}(X,k)$ denota els subconjunts de X amb k elements. Proveu que
$$|\mathcal{P}(X,k)| = \frac{n!}{(n-k)!k!}.$$
Aquests números s'anomenen números binomials o combinatoris i es denoten per $\binom{n}{k}$.

Solució: *1) Sigui $Y = \{x_1, \ldots, x_{n-1}\}$. Per H.I., $|\mathcal{P}(Y)| = 2^{n-1}$. Els subconjunts de X, o bé no contenen x_n, i llavors són subconjunts de Y, o contenen x_n i llavors són de la forma $A \cup x_n$ amb $A \subset Y$. Per tant i ha el doble de subconjunts de X que de Y. És a dir, $|\mathcal{P}(X)| = 2 \cdot |\mathcal{P}(Y)| = 2 \cdot 2^{n-1} = 2^n$.*
2) Els subconjunts de k elements de X són els subconjunts de k elements de Y (que per H.I, n'hi ha $\binom{n-1}{k}$) més els subconjunts de $k-1$ elements de Y (que per H.I, n'hi ha $\binom{n-1}{k-1}$) ja que

a cadascun d'aquests últims subconjunts hi podem afegir x_n per obtenir un subconjunt de k elements de X diferent als ja considerats.
Tenim doncs

$$|\mathcal{P}(X,k)| = \binom{n-1}{k} + \binom{n-1}{k-1}.$$

Però el càlcul directa demostra que

$$\binom{n-1}{k} + \binom{n-1}{k-1} = \binom{n}{k},$$

i hem acabat.

13. [**Binomi de Newton**] Proveu, utilitzant que

$$\binom{n}{k} + \binom{n}{k-1} = \binom{n+1}{k}, \tag{1.2}$$

que

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

Solució: *La fórmula és certa per a $n = 1$. Suposem-la certa fins a $n-1$. Llavors*

$$\begin{aligned}
(a+b)^n &= (a+b)(a+b)^{n-1} \\
&= (a+b)\left(a^{n-1} + \binom{n-1}{1}a^{n-2}b + \binom{n-1}{2}a^{n-3}b^2 + \cdots + \binom{n-1}{n-2}ab^{n-2} + b^{n-1}\right) \\
&= a^n + \binom{n-1}{1}a^{n-1}b + \binom{n-1}{2}a^{n-2}b^2 + \cdots + \binom{n-1}{n-2}a^2b^{n-2} + ab^{n-1} \\
&+ a^{n-1}b + \binom{n-1}{1}a^{n-2}b^2 + \binom{n-1}{2}a^{n-3}b^3 + \cdots + \binom{n-1}{n-2}ab^{n-1} + b^n
\end{aligned}$$

Agrupant els termes amb el mateixos exponents a a i b, i utilitzant la igualtat (1.2) *(provada a l'exercici anterior), tenim el resultat.*

14. Proveu que per a tot enter positiu n, existeix un enter positiu d'n xifres, A, format només amb els dígits 1 i 2, que és divisible per 2^n.

Solució: *Per H.I. existeixen $n-1$ números $a_0, a_1, \ldots, a_{n-2} \in \{1,2\}$ i un altre número $\lambda \in \mathbb{N}$ tals que*

$$A = \sum_{k=0}^{n-2} a_k 10^k = \lambda \cdot 2^{n-1}.$$

Considerem ara

$$B = x \cdot 10^{n-1} + A, \quad \text{amb } x = 2 \text{ si } \lambda \text{ és parell, i } x = 1 \text{ si } \lambda \text{ és senar.}$$

Per exemple, si $A = 112$, llavors $112 = 2^3 \cdot 14$, de manera que $\lambda = 14$, i per tant B es construeix posant un 2 devant de les xifres de A, i.e., $B = 2112$ (divisible per 16). Si $A = 12$, llavors $12 = 2^2 \cdot 3$, de manera que $\lambda = 3$, i per tant B es construeix posant un 1 devant de les xifres de A, i.e., $B = 112$ (divisible per 8).
Tornant al cas general estudiem les dues possibilitats, λ parell o senar.
λ parell.

$$B = 2 \cdot 10^{n-1} + A = 2 \cdot 10^{n-1} + 2^{n-1}2k = 2^n(5^{n-1} + k),$$

i B és divisible per 2^n.
λ senar.

$$B = 10^{n-1} + A = 10^{n-1} + 2^{n-1}(2k+1) = 2^n \cdot k + 2^{n-1}(5^{n-1} + 1),$$

però $5^{n-1} + 1$ és clarament parell, de manera que $B = 2^n \cdot \mu$, per a un cert $\mu \in \mathbb{N}$, és a dir, B és divisible per 2^n.

15. Demostreu que amb segells de 4 i 5 cèntims podem enviar qualsevol paquet postal de 12 cèntims o més.

Solució: *Suposem que per a $n-1$, amb $n \geq 12$, existeixen números α i β tals que*

$$4\alpha + 5\beta = n - 1.$$

Si $\alpha \geq 1$, prenem $\gamma = \alpha - 1$, i $\delta = \beta + 1$ i tenim

$$4\gamma + 5\delta = n.$$

Si $\alpha = 0$, observem que ha de ser $\beta \geq 3$. Això permet prendre $\gamma = 4$ i $\delta = \beta - 3$ i tenim

$$4\gamma + 5\delta = n.$$

16. Quants talls hem de fer a una rajola de xocolata (un rectangle $a \times b$ amb $n = ab$) que conté n petites peces per separar-les totes?

Solució: *Demostrem per inducció que la resposta és que hem de fer $n-1$ talls. Tallem el rectangle donat fent un tall vertical de manera que obtinguem dues tauletes de xocolata. Una serà un rectangle $(a-1) \times b$ i l'altre un rectangle $1 \times b$. Per H.I., ens calen $(a-1)b - 1$ talls per separar les peces de xocolata de la primera rajola i $b-1$ per separar les peces de xocolata de la segona rajola. En total haurem fet doncs*

$$[(a-1)b - 1] + (b-1) + 1 = ab - 1 = n - 1$$

talls, com volíem demostrar.

17. Trobeu totes les funcions $f : \mathbb{N} \to \mathbb{N}$ tals que

1. $f(2) = 2$.
2. $f(n+1) = 1 + 1f(1) + 2f(2) + \cdots + nf(n)$, per a tot $n \geq 1$.

Solució: *Com* $2 = f(2) = f(1+1) = 1 + 1f(1)$ *tenim que* $f(1) = 1$. *Anàlogament*

$$f(3) = f(2+1) = 1 + 1f(1) + 2f(2) = 1 + 1 + 2^2 = 6.$$

$$f(4) = f(3+1) = 1 + 1f(1) + 2f(2) + 3f(3) = 1 + 1 + 2^2 + 3.6 = 4.6$$

$$f(5) = f(4+1) = 1 + 1f(1) + 2f(2) + 3f(3) + 4f(4) = 4.6 + 4^2.6 = 20.6$$

Si no veiem una relació clara podem fer el següent. Observem que

$$f(n+1) - nf(n) = f(n)$$

és a dir

$$f(n+1) = (n+1)f(n).$$

I com que aquesta igualtat és certa per a tot n *tenim*

$$f(n+1) = (n+1)nf(n-1) = (n+1)n(n-1)f(n-2) = (n+1)n(n-1)\ldots 2f(1) = (n+1)!$$

És a dir

$$f(n) = n!, \qquad \forall n \geq 1.$$

Si volem procedir per inducció, comprovem la fórmula per a $n = 1$, *suposem cert* $f(n) = n!$, *i veiem que*

$$f(n+1) = f(n) + nf(n) = (n+1)f(n) = (n+1)n! = (n+1)!.$$

18. [**El joc del NIM**]. Es disposen uns quants objectes sobre la taula. Hi ha dos jugadors. Cada jugador pot agafar un, dos, o tres objectes. El jugador que elimina l'últim objecte, perd. Demostreu que el primer jugador té una estratègia guanyadora si i només si el número d'objectes n sobre la taula **no** és igual a $4k+1$, per algun $k \in \mathbb{N}$.

Solució: *La H.I. forta ens diu el següent: Suposem que hi ha* m *objectes sobre la taula amb* $m \leq n-1$. *Si podem escriure* m *de la forma* $4k+1$ *per a algun* $k \in \mathbb{N}$ *el jugador que mou primer perd. Si, pel contrari,* $m = 4k, 4k+2, 4k+3$ *per a algun* $k \in \mathbb{N}$ *(observeu que no hi ha més casos) el primer jugador guanya.*
Suposem ara que tenim n *objectes sobre la taula. Hi ha 4 casos.*

1) $n = 4k+1$. *Veiem que el primer jugador perd. En efecte, podem suposar que sobre la taula hi ha 5 o més objectes. El primer jugador pot treure 1,2 o 3 objectes. Si treu 1 objecte, queden* $4k$ *objectes per al segon jugador. Per H.I. aquest segon jugador (que ara seria el primer) guanya. I per tant el primer perd. Si treu 2 objectes, queden* $4k-1$ *objectes per al segon jugador. Per H.I., ja que* $4k-1 = 4(k-1)+3$, *aquest segon jugador (que ara seria el primer) guanya. I per tant el primer perd. Finalment si treu 3 objectes, queden* $4k-2$ *objectes per al segon jugador.*

Per H.I., ja que $4k-2 = 4(k-1)+2$, aquest segon jugador (que ara seria el primer) guanya. I per tant el primer perd.

2) $n = 4k$. Veiem que el primer jugador guanya. En efecte, només ha de treure 3 objectes, ja que llavors queden $4k-3 = 4(k-1)+1$ objectes i, per H.I., el segon jugador (que ara és el primer) perd.

3) $n = 4k+2$. Veiem que el primer jugador guanya. En efecte, només ha de treure 1 objecte, ja que llavors queden $4k+1$ objectes i, per H.I., el segon jugador (que ara és el primer) perd.

4) $n = 4k+3$. Veiem que el primer jugador guanya. En efecte, només ha de treure 2 objectes, ja que llavors queden $4k+1$ objectes i, per H.I., el segon jugador (que ara és el primer) perd.

19. Proveu que $n^n > (n+1)!$; $\quad \forall n \geq 3$.
Indicació: Escriviu la hipòtesi d'inducció per a $n-1$ i proveu que $n^n > (n+1)(n-1)^{(n-1)}$. Per a això, podeu considerar els tres primers termes de Newton de $(n-1+1)^n$.

Solució: *Per H.I. tenim $(n-1)^{n-1} > n!$. Així, si suposem demostrat que $n^n > (n+1)(n-1)^{(n-1)}$, tenim*

$$n^n > (n+1)(n-1)^{(n-1)} > (n+1)n! = (n+1)!$$

i haurem acabat. Demostrem doncs que $n^n > (n+1)(n-1)^{(n-1)}$. Per Newton tenim

$$n^n = (n-1+1)^n = (n-1)^n + n(n-1)^{n-1} + \frac{n(n-1)}{2}(n-1)^{n-2} + R$$

on R és una certa quantitat que no escrivim però que sabem que compleix $R > 0$.
Així

$$n^n > (n-1)^{n-1}\left((n-1)+n+\frac{n}{2}\right) > (n-1)^{n-1}(n+1)$$

i hem acabat.

Llista 2

Llenguatge

20. Acceptem[1] que una *proposició* és una afirmació que és vertadera o falsa, però no les dues coses a la vegada. Digueu quines de les expressions següents són proposicions?

a) Joan Sales va escriure *Incerta glòria*.

b) Surts?

c) $x = 2$.

d) 10 és un nombre imparell.

e) $6 + 6 = 13$.

f) $x + y > 5$.

g) Només hi ha vida a la Terra.

h) Ves a comprar patates.

Solució:

a) És una proposició ja que és una afirmació certa.

b) No és una afirmació, i per tant no és una proposició.

c) No és una proposició ja que és una afirmació que és certa o false segons els valors de x.

d) És una proposició ja que és una afirmació falsa.

e) És una proposició ja que és una afirmació falsa.

f) No és una proposició ja que és una afirmació que és certa o false segons els valors de x i de y.

g) És una proposició ja que és una afirmació certa o falsa.

[1] Aquests primers problemes són de *Apuntes de Lògica Matemàtica*, F.J.Gonzàlez, Universitat de Cádiz.

h) No és una afirmació, i per tant no és una proposició.

21. Considerem les proposicions P: *Està nevant*; Q: *Aniré al poble*; R: *Tinc temps.* Escriviu, utilitzant 'implicacions', 'i', 'o', 'no' les afirmacions següents.

a) Si no està nevant i tinc temps aniré al poble.

b) Aniré al poble només si tinc temps.

c) No està nevant.

d) Està nevant i no aniré al poble.

Escriviu també

e) Q⇔(R i (no P))

f) R i Q

g) (Q⇒R) i (R⇒Q)

h) no(R o Q)

Solució:

a) ((no P) i R) ⇒ Q

b) Q⇒R.

c) (no P).

d) (P i (no Q)).

També tenim

e) Aniré al poble si i només si tinc temps i no està nevant.

f) Tinc temps i aniré al poble.

g) Aniré al poble si i només si tinc temps.

h) Ni tinc temps, ni aniré al poble.

22. Escriviu la recíproca i la contrarrecíproca de cadascuna de les afirmacions següents.

a) Per a tot $n \in \mathbb{N}$, el numero $2n^3 + 3n^2 + n$ és múltiple de 6.

b) En tot triangle rectangle es compleix que la hipotenusa al quadrat és igual a la suma dels quadrats dels catets.

c) La tangent a una el·lipse forma angles iguals amb els radis vectors en el punt de contacte.

d) Tot nombre parell és suma de dos primers.

e) No hi ha cap nombre natural n tal que $n^2 = 2$

Solució:

a) *Reformulem l'enunciat així: Si el nombre natural* m es pot escriure com $m = 2n^3 + 3n^2 + n$ per a algun $n \in \mathbb{N}$, *llavors* m és múltiple de 6. *És a dir P⇒ Q amb P:* m es pot escriure com $m = 2n^3 + 3n^2 + n$ per a algun $n \in \mathbb{N}$ *i Q:* m és múltiple de 6.

El recíproc Q⇒P és doncs, si m *és múltiple de* 6 *llavors* m *es pot escriure com* $m = 2n^3 + 3n^2 + n$ *per a algun* $n \in \mathbb{N}$.

Observem que P⇒Q és certa (Exercici 9 (h)) i que Q⇒P és falsa.

El contrarrecíproc (no Q) ⇒ (no P) és doncs, si m *no és múltiple de* 6 *llavors* m *no es pot escriure com* $m = 2n^3 + 3n^2 + n$ *per a cap* $n \in \mathbb{N}$.

b) *Reformulem l'enunciat així: Sigui* T *un triangle de costats* a, b, c *i angles oposats* A, B, C *respectivament. Si* A *és recte, llavors* $a^2 = b^2 + c^2$. *És a dir, P⇒Q amb P:* A és recte, *Q:* $a^2 = b^2 + c^2$. *Tant a la definició P com a la de Q estem suposant implícitament l'existència del triangle* T *amb la notació explicada.*

El recíproc Q⇒P és doncs, si en un triangle T de costats a, b, c i angles oposats A, B, C respectivament, es compleix que $a^2 = b^2 + c^2$ llavors A és un angle recte.

El contrarrecíproc (no P)⇒ (no Q) és doncs, si A *no és recte llavors* $a^2 \neq b^2 + c^2$.

c) *Reformulem l'enunciat així: Sigui* P *un punt d'una el·lipse. Sigui* r *una recta per* P. *Afirmem que si* r *és tangent a l'el·lipse llavors* r *forma angles iguals amb es radis vectors en* P. *És a dir, P⇒Q amb P:* r és tangent a l'el·lipse, *Q:* r forma angles iguals amb els radis vectors en el punt de contacte. *Tant a la definició de P com de Q se suposa l'existència de l'el·lipse.*

El recíproc Q⇒P és doncs, si la recta r *pel punt* P *d'una el·lipse forma angles iguals amb els radis vectors, llavors* r *és tangent a l'el·lipse en aquest punt.*

I el contrarrecíproc (no Q) ⇒ (no P) si la recta r *que passa per un punt* P *d'una el·lipse no forma angles iguals amb els radis vectors en* P *llavors aquesta recta no és tangent a l'el·lipse en* P.

d) *Pel context s'entén que 'nombre' vol dir aquí nombre natural.*

Recíproc: Si un nombre és suma de dos primers, llavors és parell.

Contrarrecíproc: Si un nombre no és suma de dos primers llavors aquest nombre no és parell.

e) *Reformulem l'enunciat així: Sigui* $n \in \mathbb{R}$. *Si* $n \in \mathbb{N}$ *llavors* $n^2 \neq 2$.
Recíproc: Si $n^2 \neq 2$ *llavors* $n \in \mathbb{N}$.
Contrarrecíproc: Si $n^2 = 2$, *llavors* $n \notin \mathbb{N}$.

23. Donades[2] dues proposicions P, Q, construïu taules de veritat per a "i" i "o".

P	Q	P i Q
V	V	
V	F	
F	V	
F	F	

P	Q	P o Q
V	V	
V	F	
F	V	
F	F	

Penseu el cas particular en que les proposicions P i Q són P: *n és múltiple de* 3 i Q: *n és múltiple de* 5. Penseu altres exemples per a P i Q.

Solució:

P	Q	P *i* Q
V	V	V
V	F	F
F	V	F
F	F	F

P	Q	P *o* Q
V	V	V
V	F	V
F	V	V
F	F	F

24. Donades dues proposicions P, Q, construïu taules de veritat per a

a) no (P i Q);

b) (no P) o (no Q);

c) P i (no Q);

d) (no P) o Q.

Penseu el cas particular en que les proposicions P i Q són: P: *n és múltiple de* 3 i Q: *n és múltiple de* 5. Penseu altres exemples per a P i Q.

Solució:

P	Q	*no*$(P$ *i* $Q)$
V	V	F
V	F	V
F	V	V
F	F	V

P	Q	*(no* P*) o (no* Q*)*
V	V	F
V	F	V
F	V	V
F	F	V

[2]Els problemes que venen a continuació són del llibre "An Introduction to Mathematical Reasoning" de J.P. Eccles.

P	Q	P *i (no* Q*)*
V	V	F
V	F	V
F	V	F
F	F	F

P	Q	*(no* P*) o* Q
V	V	V
V	F	F
F	V	V
F	F	V

25. Considerem l'afirmació següent:

a) Les arrels del polinomi $x^3 - x^2 - x$ són positives (estrictament més grans que zero).

Quina de les afirmacions següents és la negació d'aquesta?

b) Les arrels del polinomi $x^3 - x^2 - x$ són negatives.

c) Si $a \in \mathbb{R}$ no és arrel $x^3 - x^2 - x$, llavors a és positiu.

d) Si $a \in \mathbb{R}$ és positiu, llavors a és arrel $x^3 - x^2 - x$.

e) Per algun $a \in \mathbb{R}$ no positiu es compleix que $a^3 - a^2 - a = 0$.

f) Si $a \neq 0$, llavors a no és arrel del polinomi $x^3 - x^2 - x$.

Alguna d'aquestes darreres afirmacions té el mateix significat que l'afirmació (a)? Què passa si canviem el polinomi per $x^2 + 3$?

Solució: *Com que P⇒Q vol dir (Q o (no P)), la negació de P⇒Q és (no (Q o (no P)))=(no Q) i P. Si posem P: a* és arrel del polinomi $x^3 - x^2 - x$ *i Q:* $a > 0$*, llavors la negació de P⇒Q és ((no Q) i P), és a dir,* $a \leq 0$ *i a és arrel del polinomi* $x^3 - x^2 - x$*. Equivalentment, hi ha una arrel del polinomi que és menor o igual a zero. Així doncs, la negació de* a) *és* e)*.*

26. Completeu la taula de veritat de $P \Leftrightarrow Q$ a partir de les taules per a "⇒" i "i".

P	Q	$P \Rightarrow Q$	$Q \Rightarrow P$	$P \Leftrightarrow Q$
V	V			
V	F			
F	V			
F	F			

Solució:

P	Q	$P \Rightarrow Q$	$Q \Rightarrow P$	$P \Leftrightarrow Q$
V	V	V	V	V
V	F	F	V	F
F	V	V	F	F
F	F	V	V	V

27. Usant taules de veritat proveu que les afirmacions següents són certes per a totes les afirmacions P, Q.

a) P $\Rightarrow$ (P o Q).

b) (P i Q)$\Rightarrow$ P.

Proveu també que

c) Les afirmacions 'P $\Rightarrow$ Q' i '(no Q) $\Rightarrow$ (no P)' són equivalents,

d) Les afirmacions 'P o Q' i '(no P) $\Rightarrow$ Q' són equivalents.

Solució: *a) La darrera columna de la taula està formada per V's.*

P	Q	P *o* Q	$P \Rightarrow (P$ *o* $Q)$
V	V	V	V
V	F	V	V
F	V	V	V
F	F	F	V

b) La darrera columna de la taula està formada per V's.

P	Q	P *i* Q	$(P$ *i* $Q) \Rightarrow P$
V	V	V	V
V	F	F	V
F	V	F	V
F	F	F	V

c) La tercera i quarta columna de la taula coincideixen.

P	Q	$P \Rightarrow Q$	$(no\ Q) \Rightarrow (noP)$
V	V	V	V
V	F	F	F
F	V	V	V
F	F	V	V

d) La tercera i quarta columna de la taula coincideixen.

P	Q	P *o* Q	$(no\ P) \Rightarrow Q$
V	V	V	V
V	F	V	V
F	V	V	V
F	F	F	F

28. Verifiqueu[3] l'equivalència

$$(A \Rightarrow (\text{B o C})) \Leftrightarrow ((\text{A i (no B)}) \Rightarrow C).$$

[3]Aquest problema i els següents són de *Chapter Zero*, Carol Schumacher

Solució: *Tenen les mateixes taules de veritat.*

29. Negueu: Tots els Marcians són baixos i calbs, o el meu nom no és Ot Pi.
Indicació: Considereu les afirmacions següents:

A:= Tots els Marcians són baixos i calbs.

B:= El meu nom no és Ot Pi.

C:= Tots els Marcians són baixos.

D:= Tots els Marcians són calbs.

Solució: *no (A o B) $\Leftrightarrow$ (no A) i (no B) $\Leftrightarrow$ (no(C i D) i (no B)) $\Leftrightarrow$ ((no C) o (no D)) i (no B). Així doncs la negació és "O bé algun Marcià és alt o algun Marcià té cabell, i jo em dic Ot Pi".*

30. Sigui $n \in \mathbb{N}$. És certa l'afirmació:
"El polinomi $991n^2 + 1$ no és mai un quadrat perfecte" ?

Solució:

$$379516400906811930638014896080^2 = 991(12055735790331359447442538767)^2 + 1.$$

Llista 3

Conjunts

31. Siguin $A, B \subseteq X$. De cada una de les afirmacions següents, doneu-ne una demostració (si és certa) o un contraexemple (si és falsa):

(a) $(A \cap B) \cup (A \cap B^c) = A$

(b) $A \cap (A^c \cup B) = A \cap B$

(c) $A \subseteq B$ si i només si $B^c \subseteq A^c$.

(d) $A = (A \cap B) \cup (A \setminus B)$.

(e) $A \cup B = (A \setminus B) \cup (B \setminus A) \cup (A \cap B)$.

(f) $A \setminus B = B^c \setminus A^c$

Solució: *Tota igualtat de conjunts s'ha de demostrar sempre per doble inclusió. No obstant dono només unes indicacions prou clares en cada cas.*

(a) Certa. Els elements de A estan a B o a B^c.

(b) Certa. Els elements de A i de $A^c \cup B$ són els elements de $A \cap B$.

(c) Certa. Suposem $A \subseteq B$. Si un element pertany a B^c, no pertany a B i, per tant, no pot pertànyer a A. Així doncs, pertany a A^c. La implicació en sentit contrari funciona quasi igual.

(d) Certa. A la dreta tenim els elements de A que estan a B i també els elements de A que no estan a B. Per tant, hi tenim tots els elements de A.

(e) Certa. Podem usar (d).

(f) Certa. A l'esquerra tenim els elements de A que no pertanyen a B, i a la dreta els elements que no pertanyen a B i que pertanyen a A.

32. Descriviu el conjunt $(A \times A) \cap (B \times B)$ essent $A = \{a, b, c\}$ i $B = \{a, b, d\}$.
Descriviu el conjunt $A \times \emptyset$.

Solució: $(A \times A) \cap (B \times B) = \{(a, a), (a, b), (b, a), (b, b)\}$ *i* $A \times \emptyset = \emptyset$.

33. Donats X, Y dos conjunts, $A, B \subseteq X$ i $C, D \subseteq Y$, proveu les següents propietats del producte cartesià:

(a) Si $C \neq \emptyset$, $B \subseteq A$ si i només si $B \times C \subseteq A \times C$.

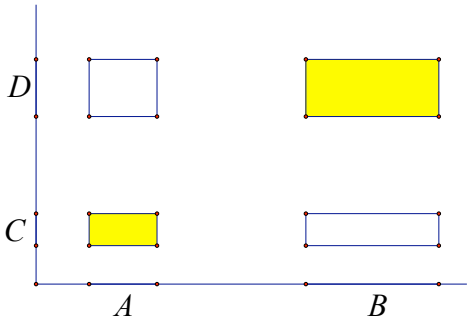
(b) $(A \times C) \cap (B \times D) = (A \cap B) \times (C \cap D)$.

(c) No és cert en general que $(A \times C) \cup (B \times D) = (A \cup B) \times (C \cup D)$.

Solució: *(a) Suposem $B \subseteq A$. Sigui $(b, c) \in B \times C$. Com $b \in A$, $(b, c) \in A \times C$ i per tant $B \times C \subseteq A \times C$.*
Suposem ara $B \times C \subseteq A \times C$, i sigui $b \in B$. Prenem $c \in C$ qualsevol (aquí usem la hipòtesi $C \neq \emptyset$). Llavors $(b, c) \in B \times C \subseteq A \times C$ i, per tant, $b \in A$. És a dir, $B \subseteq A$.

(b) Podem escriure la doble inclusió, com sempre. Però només cal observar que els elements de $(A \times C) \cap (B \times D)$ són exactament les parelles (x, y) amb x pertanyent a A i a B, i amb y pertanyent a C i a D. Però això descriu exactament els elements de $(A \cap B) \times (C \cap D)$.

(c) Just have a look at the picture.



34. Descriviu els elements de $\mathcal{P}(\mathcal{P}(\{a, b\}))$ i els de $\mathcal{P}(\mathcal{P}(\mathcal{P}(\mathcal{P}(\emptyset))))$.

Solució: *Observem primerament que*

$$\mathcal{P}(\{a, b\}) = \{\emptyset, \{a\}, \{b\}, \{a, b\}\}$$

És doncs un conjunt de 4 elements. Posem

$$\begin{aligned} \alpha &= \emptyset, \\ \beta &= \{a\}, \\ \gamma &= \{b\}, \\ \delta &= \{a, b\}. \end{aligned}$$

Així

$$\mathcal{P}(\{a,b\}) = \{\alpha,\beta,\gamma,\delta\}$$

Llavors

$$\begin{aligned}\mathcal{PP}(\{a,b\}) &= \{\emptyset,\{\alpha\},\{\beta\},\{\gamma\},\{\delta\},\{\alpha,\beta\},\{\alpha,\gamma\},\{\alpha,\delta\},\{\beta,\gamma\},\{\beta,\delta\},\{\gamma,\delta\},\\ &\quad \{\alpha,\beta,\gamma\},\{\alpha,\beta,\delta\},\{\alpha,\gamma,\delta\},\{\beta,\gamma,\delta\},\{\alpha,\beta,\gamma,\delta\}\}\end{aligned}$$

Ara substituïm $\alpha,\beta,\gamma,\delta$ pel seu valor i hem acabat (i tenim més claus que el Sereno!!).

35. Sigui $\mathbb{N} = \{0,1,2,\dots\}$ el conjunt dels nombres naturals.

1. Escriviu $\mathbb{N}$ com a unió disjunta de dos subconjunts infinits. És a dir, $\mathbb{N} = X_1 \cup X_2$ amb $X_1 \cap X_2 = \emptyset$ i $X_1, X_2 \subseteq \mathbb{N}$ conjunts infinits.
2. Feu el mateix per a 3 conjunts.
3. En general, donat $k \geq 1$, trobeu subconjunts disjunts $X_1,\dots,X_k \subseteq \mathbb{N}$ i amb infinits elements de manera que $\mathbb{N} = X_1 \cup X_2 \cup \cdots \cup X_k$.
4. Feu el mateix per a infinits conjunts disjunts i també infinits $\mathbb{N} = \bigcup_{i=1}^{\infty} X_i$.

Solució: *1) $\mathbb{N}$ és la unió disjunta dels parells amb els imparells. O bé, dels múltiples de 3 amb els múltiples de 3 més 1 o més 2. És a dir $X_1 = \{3n; n \in \mathbb{N}\}$ i $X_2 = \{3n+1, 3n+2; k \in \mathbb{N}\}$. Etc, etc.*

2) Múltiples de 3, múltiples de 3 més 1, i múltiples de 3 més 2. És a dir, $X_1 = \{3n; n \in \mathbb{N}\}$, $X_2 = \{3n+1; n \in \mathbb{N}\}$, $X_3 = \{3n+2; n \in \mathbb{N}\}$.

3) Múltiples de k, múltiples de k més 1, múltiples de k més 2, etc. És a dir,

$$X_j = \{kn + j; n \in \mathbb{N}\}, \qquad j \in \{0,1,\dots,k-1\}$$

4) Acceptem que tot nombre natural descompon de manera única com a producte de primers i que hi ha infinits primers.

$$\begin{aligned}X_1 &= \{2^\alpha; \alpha \in \mathbb{N}\} \cup \{1\},\\ X_2 &= \{3^\beta; \beta \in \mathbb{N}\},\\ X_3 &= \{2^\alpha 3^\beta; \alpha,\beta \in \mathbb{N}\},\\ X_4 &= \{5^\gamma; \gamma \in \mathbb{N}\},\\ X_5 &= \{2^\alpha 3^\gamma; \alpha,\gamma \in \mathbb{N}\},\\ X_6 &= \{2^\alpha 5^\gamma; \alpha,\gamma \in \mathbb{N}\},\\ X_7 &= \{3^\beta 5^\gamma; \beta,\gamma \in \mathbb{N}\},\\ X_8 &= \{2^\alpha 3^\beta 5^\gamma; \alpha,\beta,\gamma \in \mathbb{N}\},\\ X_9 &= \{7^\alpha; \alpha \in \mathbb{N}\},\\ &\vdots \quad = \quad \vdots\end{aligned}$$

Suposem $\alpha, \beta, \gamma, \ldots$ diferents de zero.
De fet, ho podem simplificar una mica considerant només els subconjunts de $\mathbb{N}$ que són, cadascun d'ells, potències d'un primer, i agafar després un subconjunt més que sigui el complementari a $\mathbb{N}$ de la unió de tots els anteriors.
Segona solució.[1] *Escrivim els enters en base 2 i considerem els subconjunts següents:*

$A_1 = \{n \in \mathbb{N}; \text{la seva expressió binària acaba en } 1\}$

$A_2 = \{n \in \mathbb{N}; \text{la seva expressió binària acaba en } 10\}$

$A_3 = \{n \in \mathbb{N}; \text{la seva expressió binària acaba en } 100\}$

$A_4 = \{n \in \mathbb{N}; \text{la seva expressió binària acaba en } 1000\}$

etc.

És clar que són infinits conjunts disjunts i que la seva unió és $\mathbb{N}$. Els podem descriure dient que A_1 són els imparells, A_2 els imparells multiplicats per 2, A_3 els imparells multiplicats per 4, A_4 els imparells multiplicats per 8, etc

36. Proveu que per a qualsevol conjunt X,

$$\bigcap_{Y \in \mathcal{P}(X)} Y = \emptyset; \qquad \bigcup_{Y \in \mathcal{P}(X)} Y = X.$$

Solució: *Com $\emptyset \in \mathcal{P}(X)$, i la intersecció de qualsevol conjunt amb el conjunt buit és el conjunt buit, la primera igualtat és clara. Com $X \in \mathcal{P}(X)$, i la unió de qualsevol subconjunt de X és X, la segona igualtat també és clara.*

37. Digueu si són certes o falses les afirmacions següents

(a)	$\emptyset \subseteq \{\emptyset\}$	(b)	$\emptyset \in \{\emptyset\}$	(c)	$\{\emptyset\} \subseteq \emptyset$
(d)	$\{\emptyset\} \in \{\emptyset\}$	(e)	$\{a, b\} \in \{a, \{a, b\}\}$	(f)	$\{a, b\} \subseteq \{a, \{a, b\}\}$
(g)	$\{a, b\} \subseteq \{a, b, \{a, b\}\}$	(h)	$\{a, b\} \in \{a, b, \{a, b\}\}$		

Solució:

(a) Certa (el buit és subconjunt de qualssevol conjunt).

(b) Certa (la notació $\{\emptyset\}$ fa referència a un conjunt que té un element: el conjunt buit).

(c) Falsa ($\emptyset \subseteq \emptyset$ seria certa, però en posar les claus al conjunt de l'esquerra l'afirmació és falsa, pel mateix motiu esmentat a l'apartat (b)).

(d) Falsa (el signe $\in$ representa que un cert element pertany a un conjunt, així $a \in A$ vol dir que l'element a és un dels elements de A. La notació de (d) diu $A \in A$, i un conjunt no és element de si mateix. Fora correcte escriure $A \subseteq A$).

[1] Proposada per Jaume de Dios.

(e) *Certa.*

(f) *Falsa. La notació correcte fora la utilitzada a l'apartat (e) o bé* $\{\{a,b\}\} \subseteq \{a,\{a,b\}\}$

(g) *Certa.* a *i* b *són dos elements del conjunt de la dreta, per tant* $\{a,b\}$ *n'és un subconjunt.*

(h) *Certa.*

38. Donat un conjunt X i un subconjunt $A \subseteq X$, és cert que $\mathcal{P}(A) \cap \mathcal{P}(A^c) = \emptyset$?

Solució: *Sí, ja que* $\emptyset$ *és l'únic conjunt que és a la vegada subconjunt de* A *i de* A^c.

39. Siguin A, B, C conjunts arbitraris. Proveu que

1. $A \setminus (B \cup C) = (A \setminus B) \cap (A \setminus C)$
2. $A \setminus (B \cap C) = (A \setminus B) \cup (A \setminus C)$

Solució: *(1) Sigui* $x \in A \setminus (B \cup C)$. *Això vol dir que* $x \in A$ *i que* $x \notin B \cup C$. *Però* $x \notin B \cup C$ *vol dir que* $x \notin B$ *i que* $x \notin C$. *Per tant,* $x \in A \setminus B$ *i* $x \in A \setminus C$.
Anàlogament, si $x \in (A \setminus B) \cap (A \setminus C)$ *llavors* $x \in A \setminus B$ *i* $x \in A \setminus C$. *Així* $x \in A$ *i* $x \notin B$ *i* $x \notin C$. *És a dir,* $x \in A$ *i* $x \notin B \cup C$. *Això vol dir que* $x \in A \setminus B \cup C$.

(2) Argument similar.

40. Lleis de de Morgan. Proveu que el complementari de la unió és la intersecció dels complementaris, i que el complementari de la intersecció és la unió dels complementaris. Concretament, si A, B són subconjunts d'un cert conjunt X, llavors

1. $(A \cup B)^c = A^c \cap B^c$.
2. $(A \cap B)^c = A^c \cup B^c$.

Aquestes lleis també són certes per a unions i interseccions arbitràries, es a dir, no necessàriament finites. Si I és un conjunt d'indexs, tenim

1. $(\bigcup_{i\in I} A_i)^c = \bigcap_{i\in I} A_i^c$.
2. $(\bigcap_{i\in I} A_i)^c = \bigcup_{i\in I} A_i^c$.

Solució: *(1) Veiem la inclusió "*$\subset$*". Si* x *pertany al complementari de la unió dels* A_i *és que* x *no pertany a cap dels* A_i. *Per tant* $x \in A_i^c$ *per tot* i.
Veiem la inclusió "$\supset$*". Si* x *pertany a tots els complementaris* A_i^c *és que* x *no pertany a cap dels* A_i. *Per tant* $x \notin \bigcup_{i\in I} A_i^c$.

(2) Argument similar.

41. Comproveu que $(A \setminus B) \setminus C \subset A \setminus (B \cap C)$, però que la inclusió recíproca no és certa en general.

Solució: *Sigui $x \in (A \setminus B) \setminus C$. Això vol dir $x \in (A \setminus B)$ i que $x \notin C$. És a dir, $x \in A$, $x \notin B$, i $x \notin C$. Això implica (no és equivalent) que $x \in A$ i $x \notin B \cap C$, i.e. $x \in A \setminus (B \cap C)$.*
Per veure que aquesta inclusió no és en general una igualtat podem agafar per exemple $C = \emptyset$. Llavors el terme de l'esquerra és $A \setminus B$ i el de la dreta és A. Si B és qualsevol conjunt que tingui intersecció amb A tenim que $A \setminus B \neq A$. Per exemple $A = \{1, 2\}$, $B = \{1\}$, $C = \emptyset$.

42. Comproveu que si els conjunts A_i, $i \in \mathbb{N}$, són finits, no buits i $A_i \supset A_{i+1}$ per a tot i, llavors $\bigcap_{i=1}^{\infty} A_i$ no és buit. Doneu un exemple que mostri que si els A_i no són finits, la conclusió no és certa.

Solució: *Es veu de seguida que aquests A_i s'ha d'anar repetint, ja que tots són subconjunts de A_1 que té un número finit de subconjunts. Però amb aquesta observació el resultat encara no és clar.*
Sigui n_i el número d'elements de A_i. Tenim $n_1 \geq n_2 \geq n_3 \geq \ldots$. Sigui n_s el mínim d'aquesta col·lecció de $n_i's$ (tot subconjunt de $\mathbb{N}$ té un primer element[2]). És ara evident que no podem extreure cap subconjunt de A_s estrictament més petit que A_s. Per tant, aquest és el més petit de la cadena i $\bigcap_{i=1}^{\infty} A_i = A_s$.
Per a la segona part prenem

$$A_i = \{x \in \mathbb{R}; 0 < x < \frac{1}{i}\}.$$

Llavors és clar que $\bigcap_{i=1}^{\infty} A_i = \emptyset$ ja que si hi hagués un element a en aquesta intersecció, aquest element seria per un costat estrictament positiu ($a > 0$) i per altra més petit que qualsevol número (la successió $\frac{1}{i}$ tendeix a zero i $a < \frac{1}{i}$ per a tot i), i això és impossible.

[2]Resultat equivalent al principi d'inducció.

Llista 4

Aplicacions

43. Sigui $f : X \to Y$ una aplicació, A i B subconjunts de X, C i D subconjunts de Y. Demostreu o trobeu un contraexemple de cadascuna de les següents afirmacions:

(a) $A \subseteq B \Longrightarrow f(A) \subseteq f(B)$

(b) $C \subseteq D \Longrightarrow f^{-1}(C) \subseteq f^{-1}(D)$

(c) $f(A \cup B) = f(A) \cup f(B)$.

(d) $f(A \cap B) = f(A) \cap f(B)$.

(e) $f^{-1}(f(A)) = A$.

(f) $f^{-1}(C \cup D) = f^{-1}(C) \cup f^{-1}(D)$.

(g) $f^{-1}(C \cap D) = f^{-1}(C) \cap f^{-1}(D)$.

(h) $f(f^{-1}(C)) = C$.

Solució: *(a) Suposem $A \subseteq B$. Volem demostrar $f(A) \subseteq f(B)$. Prenem doncs un element de $f(A)$. Aquest element serà de la forma $f(a)$ per a algun $a \in A$. Però com $A \subseteq B$, també és cert $a \in B$, de manera que $f(a) \in f(B)$.*

(b) Suposem $C \subseteq D$. Volem demostrar que $f^{-1}(C) \subseteq f^{-1}(D)$. Prenem doncs un element $x \in f^{-1}(C)$. Això vol dir que $f(x) \in C$. Però com $C \subseteq D$, també és cert que $f(x) \in D$, de manera que $x \in f^{-1}(D)$.

(c) Veiem la inclusió '$\subseteq$'. Prenem un element de $f(A \cup B)$. Aquest element serà de la forma $f(x)$ amb $x \in A \cup B$. Si $x \in A$ llavors $f(x) \in f(A)$. Si $x \in B$, llavors $f(x) \in f(B)$. De manera que en tot cas es compleix que $f(x) \in f(A) \cup f(B)$.
Veiem la inclusió '$\supseteq$'. Prenem un element z de $f(A) \cup f(B))$. Aquest element serà de la forma $z = f(x)$ amb $x \in A$ o bé de la forma $z = f(y)$ amb $y \in B$. Com que tant x com y són elements de $A \cup B$, és clar que $z \in f(A \cup B)$.

(d) Veiem la inclusió '$\subseteq$'. Prenem un element de $f(A \cap B)$. Aquest element serà de la forma $f(x)$ amb $x \in A \cap B$. Com x pertany a A i a B, $f(x) \in f(A) \cap f(B)$.
Veiem la inclusió '$\supseteq$'. Prenem un element z de $f(A) \cap f(B))$. Aquest element serà de la forma $z = f(x)$ amb $x \in A$ i de la forma $z = f(y)$ amb $y \in B$. Com que no podem assegurar que $x \in B$ ni que $y \in A$ no podem concloure res. No obstant veiem que si f fos injectiva, *la igualtat $z = f(x) = f(y)$ implica $x = y$. En particular $x \in B$ i tenim $z = f(x)$ amb $x \in A \cap B$ i la inclussió '$\supseteq$' queda demostrada.*
Un contraexemple a la igualtat (d) s'ha de buscar entre les aplicacions no injectives. Prenem, per exemple, $A = \{1, 2\}$, $B = \{3\}$, i $f : \mathbb{N} \longrightarrow \mathbb{N}$ donada per $f(n) = 3$ per a tot $n \in \mathbb{N}$. En aquest cas $f(A \cap B) = \emptyset$ i $f(A) \cap f(B) = \{3\}$.

(e) Veiem la inclusió '$\subseteq$'. Sigui $x \in f^{-1}f(A)$. Això vol dir que $f(x) \in f(A)$. És a dir, existeix $a \in A$ tal que $f(x) = f(a)$. Com abans, si f no és injectiva no podem prosseguir. En canvi, si f és injectiva, *ha de ser $a = x$ i per tant $x \in A$.*
Un contraexemple a la igualtat (e) s'ha de buscar entre les aplicacions no injectives. Prenem, per exemple, $A = \{1, 2\}$, $B = \{3\}$, i $f : \mathbb{N} \longrightarrow \mathbb{N}$ donada per $f(n) = 3$ per a tot $n \in \mathbb{N}$. En aquest cas $f^{-1}f(A) = f^{-1}(\{3\}) = \mathbb{N} \neq A$.
També les projeccions són bons contaexemples a aquesta situació. Per exemple, $f : \mathbb{R}^2 \longrightarrow \mathbb{R}$ donada per $f(x, y) = x$. Prenem $A = \{(x, 1); x \in \mathbb{R}\}$. Llavors $f^{-1}(f(A)) = f^{-1}(\mathbb{R}) = \mathbb{R}^2 \neq A$.
Veiem la inclusió '$\supseteq$'. Tot element $a \in A$ pertany a $f^{-1}(f(A))$ ja que $f(a) \in f(A)$.

(f) Veiem la inclusió '$\subseteq$'. Sigui $x \in f^{-1}(C \cup D)$. Això vol dir $f(x) \in C \cup D$. Si $f(x) \in C$, $x \in f^{-1}(C)$. Si $f(x) \in D$, $x \in f^{-1}(D)$. Per tant, en tot cas, $x \in f^{-1}(C) \cup f^{-1}(D)$.
Veiem la inclusió '$\supseteq$'. Sigui $x \in f^{-1}(C) \cup f^{-1}(D)$. Això vol dir que o bé $f(x) \in C$ o bé $f(x) \in D$. Per tant, $f(x) \in C \cup D$, com volíem.

(g) Veiem la inclusió '$\subseteq$'. Sigui $x \in f^{-1}(C \cap D)$. Això vol dir $f(x) \in C \cap D$, i per tant $x \in f^{-1}(C) \cap f^{-1}(D)$.
Veiem la inclusió '$\supseteq$'. Sigui $x \in f^{-1}(C) \cap f^{-1}(D)$. Això vol dir $f(x) \in C \cap D$, i per tant $x \in f^{-1}(C \cap D)$.

(h) Veiem la inclusió '$\subseteq$'. Sigui $z \in f(f^{-1}(C))$. Això vol dir que $z = f(y)$ amb $y \in f^{-1}(C)$. Equivalentment, $z = f(y)$ amb $f(y) \in C$. Per tant $z \in C$.
Veiem la inclusió '$\supseteq$'. Aquesta inclusió no és certa en general. Pot ser, per exemple que $C \neq \emptyset$ i en canvi $f^{-1}(C) = \emptyset$ (per a una f non exhaustiva). Suposem doncs que f és exhaustiva. *Sigui $c \in C$. Posem $c = f(x)$ amb $x \in X$. Com $x \in f^{-1}(C)$ hem escrit c com f aplicada a un element de $f^{-1}(C)$, és a dir, $c \in f(f^{-1}(C))$. Un contraexemple a la igualtat podria ser, per exemple, $f : \mathbb{N} \longrightarrow \mathbb{N}$ donada per $f(n) = 1$ per a tot $n \in \mathbb{N}$, i $C = \{2\}$.*

44. Què podem dir de les afirmacions anteriors si f és injectiva? I si és exhaustiva?

Solució: *Veure solució problema 43.*

45. Siguin X i Y conjunts no buits i $f : X \to Y$ una aplicació. Demostreu que:

1. f injectiva $\Leftrightarrow \exists\ g : Y \to X$ tal que $g \circ f = Id_X$. Aquesta g és exhaustiva.
2. f exhaustiva $\Leftrightarrow \exists\ g : Y \to X$ tal que $f \circ g = Id_Y$. Aquesta g és injectiva.

És la g única? Estudieu el cas en què $X = Y = \mathbb{N}$ amb les aplicacions

$$f(n) = 2n \ \text{ i } \ g(n) = \begin{cases} n/2 & \text{si } n \text{ és parell} \\ 0 & \text{si } n \text{ és senar} \end{cases}$$

Solució: *(1) '$\Rightarrow$'. Fixem un element $x_0 \in X$ que existeix perquè X és no buit. Donat $y \in Y$ definim $g(y)$ de la manera següent:*

$$g(y) = \begin{cases} x & si\ y = f(x) \\ x_0 & si\ y = f(x) \end{cases}$$

Observem que per ser injectiva si $y = f(x)$ aquest x és únic.
Ara és fàcil comprovar que $g \circ f = Id_X$, ja que

$$(g \circ f)x = g(f(x)) = x, \qquad \forall x \in X.$$

'$\Leftarrow$'. Suposem $f(x) = f(y)$. Aplicant g als dos costats obtenim

$$g(f(x)) = g(f(y)).$$

Però com que $g \circ f$ és al identitat, aquesta igualtat implica $x = y$, i f és injectiva.

(2) '$\Rightarrow$'. Sigui $y \in Y$. Per ser f exhaustiva existeix almenys un $x \in X$ (probablement més d'un) tal que $y = f(x)$. De tots els x que compleixen aquesta condició ($f(x) = y$) en triem un, diguem-li x_y. Llavors definim

$$g(y) = x_y.$$

Clarament

$$(f \circ g)y = f(g(y)) = f(x_y) = y,$$

és a dir $f \circ g = Id_Y$.

'$\Leftarrow$'. Sigui $y \in Y$. Prenem $x = g(y) \in X$. Llavors, $f(x) = f(g(y)) = y$, i per tant f és exhaustiva.
Observis que tant en el cas (1) com en el cas (2) l'aplicació g que hem construït no és pas única. Hem tingut llibertat en elegir el x_0 en el cas (1) i el x_y en el cas (2).
Finalment observem que $f : \mathbb{N} \longrightarrow \mathbb{N}$ donada per $f(n) = 2n$ és injectiva i

$$g(f(n)) = g(2n) = n,$$

és a dir, $g \circ f = Id_{\mathbb{N}}$. En canvi

$$f(g(n)) = \begin{cases} f(n/2) = n & si\ n\ és\ parell \\ f(0) = 0 & si\ n\ és\ senar \end{cases}$$

És a dir, $f \circ g \neq Id_{\mathbb{N}}$ d'acord amb el fet que f no és exhaustiva.

46. Sigui $X = A_1 \cup A_2$. Si tenim aplicacions $f_1 : A_1 \to Y$ i $f_2 : A_2 \to Y$, en quines condicions podem construir una aplicació $f : X \to Y$ tal que $f\,|_{A_1} = f_1$ i $f\,|_{A_2} = f_2$?

Solució: *Ha de passar que $f_1 = f_2$ sobre $A_1 \cap A_2$. Això permet construir f dient:*

$$f(x) = \begin{cases} f_1(x) & si\ x \in A_1, \\ f_2(x) & si\ x \in A_2. \end{cases}$$

47. En[1] cadascun dels casos següents determineu si existeix (i trobeu-la) una funció $f : A \longrightarrow B$ que sigui (a) injectiva, (b) exhaustiva, (c) bijectiva.

(a) $A = \{1, 2, 3, 4\}$, $B = \mathcal{P}(\{1\})$

(b) $A = \{1, 2, 3, 4, 5\}$, $B = \{0\} \times \{1, 2, 3, 4, 5\}$

(c) $A = \{0, 1\} \times \{0, 1\} \times \{0, 1\}$, $B = \{0, 1, 2, 3, 4, 5, 6, 7\}$

Solució: *(a) No pot haver-hi cap aplicació injectiva (i per tant, tampoc cap de bijectiva) de A a B ja que B té menys elements que A. Aplicacions exhaustives sí que n'hi han, per exemple podem definir* $f : A \longrightarrow B$ *per* $f(1) = \emptyset$, *i* $f(2) = f(3) = f(4) = \{1\}$.
(b) En aquest cas tant A com $B = \{(0, 1), (0, 2), (0, 3), (0, 4), (0, 5)\}$ *tenen* 5 *elements. Tota aplicació injectiva serà automàticament exhaustiva i recíprocament. Per exemple, l'aplicació*

$$f(i) = (0, i), \qquad i = 1, 2, 3, 4, 5,$$

és bijectiva.
(c) En aquest cas tant $A = \{(0, 0, 0), (0, 0, 1), (0, 1, 0), (0, 1, 1), (1, 0, 0), (1, 0, 1), (1, 1, 0), (1, 1, 1)\}$ *com B tenen* 8 *elements. Tota aplicació injectiva serà automàticament exhaustiva i recíprocament. Per exemple, l'aplicació que porta els elements de A, en l'ordre que acabem de donar, respectivament sobre els elements* $0, 1, 2, 3, 4, 5, 6, 7$ *de B és una bijecció entre A i B.*

48. És injectiva la funció $f : \{0, 1, 2, \ldots, 10\} \longrightarrow \{0, 1, 2, \ldots, 10\}$ donada per

$$f(x) = \begin{cases} x + 3 & \text{si } 0 \leq x \leq 3 \\ 10 - x & \text{si } 4 \leq x \leq 10. \end{cases}$$

Solució: *Observem que* $f(3) = f(4)$ *i per tant, no és injectiva.*

49. Donades les funcions $f, g, h : \mathbb{N} \longrightarrow \mathbb{N}$

$$\begin{aligned} f(n) &= n^3 \\ g(n) &= 2n + 4 \\ h(n) &= n^2 + 2 \end{aligned}$$

trobeu les 9 funcions que s'obtenen composant-les dos a dos: $f \circ f; f \circ g$, etc.

Solució: *Només farem* $f \circ g$ *i* $g \circ f$.

$$\begin{aligned} f(g(n)) &= f(2n + 4) = (2n + 4)^3. \\ g(f(n)) &= g(n^3) = 2n^3 + 4 \end{aligned}$$

[1] La resta d'exercicis d'aquesta secció són del llibre *Los números reales y el infinito*, Carlos Uzcàtegui, Universidad de los Andes.

50. Sigui $f : \mathbb{N} \longrightarrow \mathbb{N}$ donada per

$$f(x) = \begin{cases} x+1 & \text{si } x \text{ és parell} \\ x-1 & \text{si } x \text{ és imparell} \end{cases}$$

Demostreu que és bijectiva i trobeu la seva inversa.

Solució: *Suposem $f(x) = f(y)$. Si x i y són parells, llavors tenim $x+1 = y+1$ i, per tant, $x = y$. Si x és parell i y imparell, llavors tenim $x+1 = y-1$. És a dir, $x = y-2$. Però si a un número imparell (y) li restem 2 obtenim un número imparell, de manera que aquesta igualtat no es pot donar. És a dir, no podem tenir $f(x) = f(y)$ amb x és parell i y imparell. Anàlogament es veu que no podem tenir $f(x) = f(y)$ amb x imparell i y parell.*
Finalment, si x i y són imparells tenim $x-1 = y-1$, i per tant, $x = y$.
Observem que $f(f(x)) = x$ de manera que $f^{-1} = f$.

51. Trobeu la funció inversa del cosinus hiperbòlic. Recordeu que $\cosh x = \dfrac{e^x + e^{-x}}{2}$.

Solució: *Per trobar la funció inversa de $y = f(x)$ hem d'aïllar x en funció de y i canviar x per y i y per x a l'expressió trobada.*
En el nostre cas posem

$$y = \frac{e^x + e^{-x}}{2} = \frac{e^{2x}+1}{2e^x}$$

Dient $z = e^x$ tenim l'equació de segon grau

$$z^2 - 2yz + 1 = 0.$$

Per tant

$$z = \frac{2y \pm \sqrt{4y^2-4}}{2} = y \pm \sqrt{y^2-1}.$$

Així,

$$x = \ln(y \pm \sqrt{y^2-1}).$$

Canviant x per y i y per x tenim que la funció inversa demanda és

$$y = \ln(x \pm \sqrt{x^2-1}).$$

52. Trobeu la funció inversa de $f : \mathbb{R} \setminus \{2\} \longrightarrow \mathbb{R} \setminus \{3\}$ donada per $f(x) = \dfrac{3x}{x-2}$.

Solució: *Posem*

$$y = \frac{3x}{x-2}.$$

Aïllem x i trobem

$$x = \frac{2y}{y-3}.$$

Substituïm x per y i y per x i obtenim la funció inversa demanada:

$$y = \frac{2x}{x-3}.$$

Comprovació:

$$x \mapsto \frac{2x}{x-3} \mapsto \frac{3(\frac{2x}{x-3})}{\frac{2x}{x-3}-2} = x.$$

També

$$x \mapsto \frac{3x}{x-2} \mapsto \frac{2(\frac{3x}{x-2})}{\frac{3x}{x-2}-3} = x.$$

53. Sigui $f : \mathbb{N} \longrightarrow \mathbb{N}$ donada per $f(n) = 3n + 1$. Definim $g : \mathcal{P}(\mathbb{N}) \longrightarrow \mathcal{P}(\mathbb{N})$ per

$$g(A) = f[A], \qquad \text{on } \ f[A] = \{f(n); n \in A\}.$$

(a) Trobeu $g(\{1, 3, 5\})$.

(b) Trobeu $g(P)$ on P és el subconjunt dels nombres parells.

(c) Proveu que g és injectiva.

Solució: *(a)*

$$g(\{1, 3, 5\}) = f[\{1, 3, 5\}] = \{f(1), f(2), f(3)\} = \{4, 7, 10\}.$$

(b)

$$g(P) = f[P] = \{f(n); n \in P\} = \{f(2k); k \in \mathbb{N}\} = \{6k + 1; k \in \mathbb{N}\}$$

(c) Suposem $g(A) = g(B)$ amb A i B subconjunts de $\mathbb{N}$. Això vol dir $f[A] = f[B]$, és a dir,

$$\{f(a); a \in A \subseteq \mathbb{N}\} = \{f(b); b \in B \subseteq \mathbb{N}\}.$$

Equivalentment

$$\{3a + 1; a \in A \subseteq \mathbb{N}\} = \{3b + 1; b \in B \subseteq \mathbb{N}\}.$$

Això vol dir que tot element $n \in \mathbb{N}$ que es pot escriure com $n = 3a + 1$ amb $a \in A$ també es pot escriure com $3b + 1$ amb $b \in B$. Però això implica $a = b$, i tot element de A és de B (i recíprocament). Per tant, $A = B$ i g és injectiva.

Llista 5

Permutacions

54. Calculeu el signe de la permutació $\sigma = (1,3,2,5)(4,6)$.

Solució: *Sabem que* $(1,3,2,5) = (1,3)(3,2)(2,5)$*, de manera que* σ *és producte de* 4 *transposicions. Com* 4 *és parell,* σ *té signe* 1.

55. Calculeu el signe d'un cicle de longitud r.

Solució: *Com que* $(a_1,\ldots,a_r) = (a_1,a_2)\ldots(a_{r-1},a_r)$*, i aquí hi ha* $r-1$ *transposicions, el signe d'un cicle d'ordre* r *és* $(-1)^{r-1}$.

56. Donada una permutació $\sigma \in S_n$ diem que té **ordre** m si m és el mínim enter més gran que 0 tal que σ^m =Id.

(a) Demostreu que si σ és una permutació i si per a uns $s,t \geq 1$ amb $s > t$ es compleix $\sigma^s = \sigma^t$ aleshores $\sigma^{s-t} = \mathrm{Id}$. Justifiqueu que per a tota permutació té sentit parlar del seu ordre.

(b) Calculeu l'ordre de les permutacions $\sigma_1 = (1,2,3)(7,5)$ i $\sigma_2 = (1,2)(2,5,4)$.

(c) Demostreu que si una permutació σ té ordre m aleshores $\sigma^{mk} = \mathrm{Id}$, per a tot $k \geq 1$. Calculeu

$$\sigma_2^{1475} \quad \text{i} \quad (\ (2,5)\circ\sigma_1\ )^{123}.$$

Solució: *(a) Aplicant* σ^{-t} *als dos costats de la igualtat* $\sigma^s = \sigma^t$ *obtenim* $\sigma^{s-t} = Id$.
Per veure que sempre té sentit parlar de l'ordre d'una permutació considerem la successió infinita $\sigma, \sigma^2, \sigma^3, \ldots$. *Com que* S_n *és un conjunt finit, hi haurà un moment en que una d'aquestes potències de* $v\sigma$ *coincidirà amb alguna potència anterior. Estarem llavors en la situació que acabem d'estudiar.*
(b) Com que σ_1 *està donada com producte de cicles disjunts, el seu ordre és el mínim comú múltiple del ordres (vegeu problema 58). I l'ordre d'un cicle és la seva longitud. Per tant, l'ordre de* σ_1 *és* $3 \times 2 = 6$.

Com que σ_2 no està donada com producte de cicles disjunts, primer l'escrivim així:

$$\sigma_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 5 & 3 & 1 & 4 \end{pmatrix} = (1,2,5,4).$$

Per tant σ_2 té ordre 4, ja que és un cicle de longitud 4.
(c) Fent la divisió euclidiana de 1475 entre 4 (perquè 4 és l'ordre de σ_2) tenim $1475 = 368 \times 4 + 3$. Per tant

$$\sigma_2^{1475} = (\sigma_2^4)^{368}\sigma_2^3 = \sigma_2^3 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 1 & 3 & 5 & 2 \end{pmatrix} = (1,4,5,2)$$

Finalment observem que $(2,5) \circ \sigma_1$ té ordre 5. En efecte,

$$(2,5) \circ \sigma_1 = (2,5)(1,2,3)(7,5) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 5 & 3 & 1 & 4 & 7 & 6 & 2 \end{pmatrix} = (1,5,7,2,3).$$

Així

$$\begin{aligned} ((2,5) \circ \sigma_1)^{123} &= ((2,5) \circ \sigma_1)^{5\times 24+3} = ((2,5) \circ \sigma_1)^3 = (1,5,7,2,3)^3 \\ &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 5 & 7 & 4 & 3 & 6 & 1 \end{pmatrix} = (1,2,5,3,7). \end{aligned}$$

57. Demostreu que per a tota parella $\sigma, \tau \in S_n$ les permutacions σ i $\tau^{-1}\sigma\tau$ tenen el mateix signe i el mateix ordre.

Solució: *Si τ descompon com a producte de k transposicions, τ^{-1} també descompon com a producte de k transposicions (les mateixes en ordre invers), de manera que $\tau^{-1}\sigma\tau$ descompon com a producte de tantes transposicions com tingui sigma, més $2k$. Com $2k$ és parell, hem acabat. Observem que*

$$(\tau^{-1}\sigma\tau)^k = (\tau^{-1}\sigma\tau)(\tau^{-1}\sigma\tau)\ldots(\tau^{-1}\sigma\tau) = \tau^{-1}\sigma^k\tau$$

de manera que és clar que σ i $\tau^{-1}\sigma\tau$ tenen el mateix ordre.

58. Demostreu que si $\sigma_1, \sigma_2, \ldots, \sigma_s$ són cicles disjunts de S_n i

$$\sigma = \sigma_1 \circ \sigma_2 \circ \cdots \circ \sigma_r$$

aleshores l'ordre de σ és el mínim comú múltiple de les longituds dels cicles $\sigma_1, \ldots, \sigma_r$.

Solució: *Per ser disjunts commuten, de manera que*

$$\sigma^k = \sigma_1^k \circ \cdots \circ \sigma_r^k.$$

Per tenir $\sigma^k = Id$, i novament per ser disjunts, ha de ser $\sigma_i^k = Id$, per a tot i. Així k és múltiple de tots els ordres i com ha de ser el mínim amb aquesta propietat és el mínim comú múltiple.

59. Podem tenir a S_9 un element d'ordre 21? Quins són els ordres dels elements de S_7? Quin és l'ordre màxim d'un element de S_8?

Solució: *Com a* S_9 *no hi ha cicles més llargs de* 9*, és clar que no podem tenir cap cicle d'ordre* 21*. Si l'element de* S_9 *és producte de dos cicles disjunts, sabem que el seu ordre és el mínim comú múltiple de l'ordre (longitud) d'aquests cicles. Com* 21 *només descompon com a producte de* 3×7*, aquests dos cicles disjunts haurien de tenir longitud* 3 *i* 7*, i en ser disjunts, necessitaríem* $3 + 7 = 10$ *lletres per a escriure'ls, i només en tenim* 9 *ja que estem a* S_9*. Per tant a* S_9 *no hi ha cap element d'ordre* 21*.*

Estudiem S_7*.*
Elements amb 7 *punts fixos: la identitat. Ordre* 1*.*
Elements amb 6 *punts fixos: el setè element ha de ser també fix i estem en el cas anterior.*
Elements amb 5 *punts fixos: són les transposicions dels dos elements restants, que tenen ordre* 2*.*
Elements amb 4 *punts fixos: són els cicles formats pels tres elements restants, que tenen ordre* 3*. Cap d'aquests tres punts pot ser fix, ja que llavors estaríem en el cas anterior.*
Elements amb 3 *punts fixos: són els cicles formats pels quatre elements restants, que tenen ordre* 4*, o el producte de dues transposicions que es formen agafant aquests elements dos a dos. Aquests productes tenen ordre* 2*.*
Elements amb 2 *punts fixos: són els cicles formats pels cinc elements restants, que tenen ordre* 5*, o el producte d'un cicle d'ordre* 3 *per un d'ordre* 2*, que té doncs ordre* 6*.*
Elements amb 1 *punt fix: són els cicles formats pels sis elements restants, que tenen ordre* 6*, o el producte d'un cicle d'ordre* 4 *per un d'ordre* 2*, que té doncs ordre* 4*, o el producte d'un cicle d'ordre* 3 *per un d'ordre* 3*, que té doncs ordre* 3*,o el producte de tres cicle d'ordre* 2*, que té doncs ordre* 2*.*
Elements amb 0 *punts fixos: cicles d'ordre* 7*, o el producte d'un cicle d'ordre* 5 *per un d'ordre* 2*, que té doncs ordre* 10*, o el producte d'un cicle d'ordre* 4 *per un d'ordre* 3*, que té doncs ordre* 12*,o el producte de tres cicle d'ordres* 3*,* 2 *i* 2*, que té doncs ordre* 6*.*
Han aparegut doncs, els ordres $1, 2, 3, 4, 5, 6, 7, 10, 12$*.*

Estudiem S_8*. Podem repetir l'estudi anterior, o mirar simplement els possible mínims comuns múltiples formats entre nombres que sumin menys de* 8*. Es veu fàcilment que el nombre més gran que es pot obtenir així és* $5 \times 3 = 15$*.*

60. Considerem S_n amb $n \geq 2$.

(a) Trobeu totes les permutacions parells i totes les senars de S_3.

(b) Compteu quantes permutacions parells i quantes senars hi ha a S_4.

(c) Considerem una llista

$$\sigma_1, \sigma_2, \ldots, \sigma_t$$

de permutacions de S_n diferents i amb el mateix signe.

Prenem una transposició τ i formem la llista

$$\tau\sigma_1, \tau\sigma_2, \ldots, \tau\sigma_t.$$

Vegeu que a aquesta darrera llista totes les permutacions són diferents i tenen signe contrari a les de la llista anterior.

(d) Proveu que a S_n hi ha tantes permutacions parells com senars.

Solució: *(a) S_3 té 6 elements: $Id, (1,2), (1,3), (2,3), (1,2,3), (1,3,2)$. Les tres transposicions són imparells (el signe d'una permutació és igual a (-1) elevat al número de transposicions en les que descompon.) Les altres tres $(Id, (1,2,3), (1,3,2))$ són parells.*
Observem, doncs, que hi ha el mateix nombre (3) de permutacions parells que d'imparells.

(b) Els elements de S_4 són:

Id	*(1,2)*	*(1,2,3)*	*(1,2,3,4)*	*(1,2)(3,4)*
	(1,3)	*(1,2,4)*	*(1,2,4,3)*	*(1,3)(2,4)*
	(1,4)	*(1,3,2)*	*(1,3,2,4)*	*(1,4)(2,3)*
	(2,3)	*(1,3,4)*	*(1,3,4,2)*	
	(2,4)	*(1,4,2)*	*(1,4,2,3)*	
	(3,4)	*(1,4,3)*	*(1,4,3,2)*	
		(2,3,4)		
		(2,4,3)		

Imparells: 6 transposicions+ 6 cicles d'ordre 4 (recordem que $(1,2,3,4) = (1,2)(2,3)(3,4)$).
Parells: Id+8 cicles d'ordre 3 + 3 productes de dues transposicions.
Observem, doncs, que hi ha el mateix nombre (12) de permutacions parells que d'imparells.

(c) Per ser τ una transposició, és clar que $\tau\sigma$ té signe oposat a σ (descompon en una transposició més). També és clar, aplicant τ^{-1}, que la igualtat $\tau\sigma_i = \tau\sigma_j$ implica $\sigma_i = \sigma_j$.

(d) Conseqüència directa de l'apartat (c) aplicat a la llista formada per totes les permutacions parells. Observem que tota permutació imparell és de la forma $\tau\sigma$ amb σ parell (per exemple, si ϵ és imparell, podem escriure $\epsilon = \tau(\tau^{-1}\epsilon)$).

61. Considereu les dues permutacions de S_{10} següents:

$$\sigma_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 5 & 1 & 8 & 2 & 7 & 9 & 10 & 6 & 3 & 4 \end{pmatrix}, \qquad \sigma_2 = (8,1,7,2) \circ (5,2)$$

(a) Calculeu σ_1^2, $\sigma_1 \circ \sigma_2$ i σ_2^{-1}

(b) Descomponeu-les en producte de cicles disjunts.

(c) Descomponeu-les en producte de transposicions.

(d) Calculeu el signe de cadascuna d'elles.

(e) Calculeu $((3,4) \circ \sigma_2)^{41}$

Solució: *(a) Per escriure σ_1^2 només hem d'observar els següent:*
El 1 *va al* 5 *(en aplicar σ_1) i el* 5 *va al* 7 *(en tornar a aplicar σ_1). Per tant, l'*1 *va al* 7 *(en aplicar dos cops σ_1).*
Anàlogament, el 2 *va al* 1 *i el* 1 *va al* 5*. Per tant, el* 2 *va al* 5*. El* 3 *va al* 8 *i el* 8 *va al* 6*. Per tant, el* 3 *va al* 6*. El* 4 *va al* 2 *i el* 2 *va al* 1*. Per tant, el* 4 *va al* 1*. El* 5 *va al* 7 *i el* 7 *va al* 10*. Per tant, el* 5 *va al* 10*. El* 6 *va al* 9 *i el* 9 *va al* 3*. Per tant, el* 6 *va al* 3*. El* 7 *va al* 10 *i el* 10 *va al* 4*. Per tant, el* 7 *va al* 4*. El* 8 *va al* 6 *i el* 6 *va al* 9*. Per tant, el* 8 *va al* 9*. El* 9 *va al* 3 *i el* 3 *va al* 8*. Per tant, el* 9 *va al* 8*. El* 10 *va al* 4 *i el* 4 *va al* 2*. Per tant, el* 10 *va al* 2*. Equivalentment*

$$\sigma_1^2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 7 & 5 & 6 & 1 & 10 & 3 & 4 & 9 & 8 & 2 \end{pmatrix} = (1,7,4)(2,5,10)(3,6)(8,9).$$

Per entendre millor σ_2 l'escrivim en forma de matriu: la composició $(8,1,7,2)\circ(5,2)$ s'ha de llegir per la dreta: En aplicar la transposició $(5,2)$, l'$1,3,4,6,7,8$ *es queden fixos i* 5 *i el* 2 *es permuten. Un cop fet això, el* 8 *va a l'*1*, l'*1 *al* 7*, el* 7 *al* 2 *i el* 2 *al* 8 *i els demés $(3,4,5,6,9,10)$ es queden fixos. En total tenim doncs,*

$$\sigma_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 7 & 5 & 3 & 4 & 8 & 6 & 2 & 1 & 9 & 10 \end{pmatrix} = (1,7,2,5,8).$$

Per escriure σ_2^{-1} només cal permutar les dues files de la matriu de σ i reordenar:

$$\sigma_2^{-1} = \begin{pmatrix} 7 & 5 & 3 & 4 & 8 & 6 & 2 & 1 & 9 & 10 \\ 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 8 & 7 & 3 & 4 & 2 & 6 & 1 & 5 & 9 & 10 \end{pmatrix}.$$

Observem que $\sigma_2^{-1} = (1,8,5,2,7)$, que no és més que $\sigma_2 = (1,7,2,5,8)$ recorregut al revés.

$$\begin{aligned} \sigma_2^{-1} &= 1 \to 8 \to 5 \to 2 \to 7 \to 1 \\ \sigma_2 &= 1 \leftarrow 8 \leftarrow 5 \leftarrow 2 \leftarrow 7 \leftarrow 1 \end{aligned}$$

De manera anàloga a com hem calculat σ_1^2 calculem $\sigma_1 \circ \sigma_2$. Obtenim

$$\sigma_1 \circ \sigma_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 10 & 7 & 8 & 2 & 6 & 9 & 1 & 5 & 3 & 4 \end{pmatrix} = (1,4,2,7)(3,8,5,6,9).$$

(b) Ja fet a l'apartat anterior.
(c) Fàcil a partir de (b).
(d) Fàcil a partir de (c).
(e) Observem que $(3,4)\circ\sigma_2 = (3,4)(1,7,2,5,8)$. Producte de cicles disjunts. En particular, aquesta permutació té ordre $m.c.m.(2,5) = 10$. Així

$$[(3,4)\circ\sigma_2]^{41} = [[(3,4)\circ\sigma_2]^{10}]^4 \circ [(3,4)\circ\sigma_2] = (3,4)\circ(1,7,2,5,8).$$

62. Resoleu les equacions de S_5 següents (o digueu que no tenen solució):

(a) $(1,4,2)\circ\sigma\circ(1,4,2)^{-1}=(1,3)$.

(b) $\sigma\circ(2,1,4)^{34}=(2,3)\circ(3,1,4,5)$.

(c) $\sigma\circ(3,4,1)\circ\sigma^{-1}=(3,4)$.

Solució: *(a)* $\sigma=(1,4,2)^{-1}(1,3)(1,4,2)=(1,2,4)(1,3)(1,4,2)=(2,3)$.
(b) Com $34=3\times 11+1$ *tenim*

$$\sigma\circ(2,1,4)^{34}=\sigma\circ(2,1,4).$$

Així

$$\sigma=(2,3)(3,1,4,5)(2,1,4)^{-1}=(2,3)(3,1,4,5)(1,2,4)=(1,3)(2,5).$$

(c) No té solució, ja que a l'esquerra hi ha una permutació d'ordre 3 *i a la dreta una d'ordre* 2.

Llista 6

Conjunt quocient

63. Considereu les relacions següents als conjunt indicats:

(a) $X = \{1, 2, 3, 4\}$ amb les relacions, $1 \sim 1, 2 \sim 2, 3 \sim 3, 4 \sim 4, 1 \sim 4, 4 \sim 1, 2 \sim 4, 4 \sim 2$.

(b) $Y = \{a, b, c\}$ amb les relacions, $a \sim a, b \sim b, a \sim b, b \sim a, c \sim b, b \sim c$.

(c) $\mathbb{Z}$ amb la relació $n \sim m$ si $n - m$ és múltiple de 5.

(d) Al pla $\mathbb{R}^2 \setminus \{(0, 0)\}$, $(x, y) \sim (x', y')$ si (x', y') és a la recta que uneix (x, y) amb l'origen.

(e) Al conjunt $\mathcal{P}(\mathbb{N})$, $A \sim B$ si $A \subseteq B$.

Descriviu les propietats de cadascuna d'elles (si és reflexiva, simètrica, antisimètrica, transitiva, d'equivalència, d'ordre...). Si són d'equivalència estudieu el conjunt quocient.

Solució: *(a) És reflexiva i simètrica però no transitiva, ja que l'*1 *està relacionat amb el* 4*, el* 4 *està relacionat amb el* 2*, però en canvi, l'*1 *no està relacionat amb el* 2*. No és antisimètrica (i per tant no és d'ordre).*

(b) No és reflexiva ja que c no està relacionat amb c. És simètrica i no transitiva.

(c) És relació d'equivalència. No antisimètrica (i per tant no és d'ordre). El conjunt quocient és $\mathbb{Z}/(5)$*.*

(d) És relació d'equivalència. No antisimètrica (i per tant no és d'ordre). El conjunt quocient és l'espai projectiu de dimensió 1*, és a dir,* S^1 *amb els antipodals identificats. Estudieu la mateixa relació d'equivalència a l'espai.*

(e) És reflexiva, antisimètrica i transitiva (és a dir, és una relació d'ordre). No és simètrica, ja que $A \subset B$ *no implica* $B \subset A$*. No és d'ordre, ja que donats* $A, B \subset \mathcal{P}(\mathbb{N})$ *podem no tenir ni* $A \subset B$ *ni* $B \subset A$*.*

64. Denotem per $\mathbb{R}[x]$ el conjunt dels polinomis amb coeficients reals. Demostreu que la relació

$$f(x) \sim g(x) \text{ si } f(x) - g(x) \text{ és múltiple de } x^2 + 1$$

és una relació d'equivalència. Quina és la classe del x^4-3? I la classe de x^2? Qui és el conjunt quocient?

Solució: *És evident que és una relació d'equivalència. La pregunta "Quina és la classe del x^4-3" no és massa precisa, però com que dins de cada classe hi ha un polinomi especialment fàcil (el de grau més petit) que la caracteritza, entenem que es demana de trobar aquest polinomi.*
Observem que si fem la divisió euclidiana de qualsevol polinomi $D(x)$ entre x^2+1 obtenim

$$D(x) = (x^2+1)q(x) + r(x), \quad \text{grau } r(x) < 2.$$

En particular, el dividend $D(x)$ i el reste $r(x)$ estan relacionats per l'anterior relació d'equivalència: la seva diferència és múltiple de x^2+1.
En particular

$$x^4 - 3 = (x^2+1)(x^2-1) - 2,$$

és a dir, x^4-3 és equivalent a -2. La classe de x^4-3 és la classe de -2.
Anàlogament, la classe de x^2 és la classe de -1 (al dividir x^2 entre x^2+1 dóna quocient 1 i reste -1). En aquest nou espai tenim doncs un element que elevat al quadrat dóna -1. Això ens fa pensar en els complexos. De fet, el conjunt quocient s'identifica amb els complexos associant al complex $a+bi$ la classe del polinomi $a+bx$. En particular, la relació $\bar{x}^2 = -1$ es tradueix en $i^2 = -1$.

65. A S_n definim la relació

$$\sigma \sim \alpha \quad \text{si i només si} \quad \sigma = \gamma^{-1}\alpha\gamma \quad \text{per a algun } \gamma \in S_n.$$

En aquest cas es diu que σ i α són conjugades.

(a) Demostreu que $\sim$ és una relació d'equivalència.

(b) Compteu quantes classes diferents hi ha a S_4. Descriviu com és cada classe.

(c) Donada $\sigma \in S_n$, definim $d(\sigma)$ com el nombre de cicles disjunts en què descompon σ. Recordem que aquesta descomposició és única llevat de l'ordre.

Demostreu que l'aplicació

$$\begin{array}{rccc} f\colon & S_n/\sim & \longrightarrow & \{1,2,\ldots,n\} \\ & \overline{\sigma} & \longmapsto & d(\sigma) \end{array}$$

està ben definida. És injectiva? És exhaustiva?

(d) Compteu quants elements hi ha a $S_7/\sim$.

Solució: *(a) Reflexiva. Si prenem $\gamma = id$ a l'anterior definició tenim*

$$\sigma \sim \sigma \quad \textit{ja que } \sigma = \gamma^{-1}\sigma\gamma$$

Simètrica. Si $\sigma \sim \alpha$ conjugant amb γ, llavors $\alpha \sim \sigma$ conjugant amb γ^{-1}. Concretament $\sigma = \gamma^{-1}\sigma\gamma$, llavors $\alpha = \gamma\sigma\gamma^{-1}$. És a dir, $\sigma \sim \alpha$ implica $\alpha \sim \sigma$.
Transitiva. Suposem $\sigma \sim \alpha$ amb $\sigma = \gamma^{-1}\alpha\gamma$, i $\alpha \sim \tau$ amb $\alpha = \delta^{-1}\tau\delta$, per a certes $\gamma, \delta \in S_n$.
Llavors $\sigma \sim \tau$ ja que

$$\sigma = \gamma^{-1}(\delta^{-1}\tau\delta)\gamma = (\delta\tau)^{-1}\tau(\delta\tau), \qquad amb \quad \delta\tau \in S_n.$$

(b) Utilitzarem el resultat següent.

Lema. *Sigui $(a_1, \ldots, a_r)$ un cicle d'ordre r de S_n, i sigui $\tau \in S_n$. Llavors*

$$\tau(a_1, \ldots, a_r)\tau^{-1} = (\tau a_1, \ldots, \tau a_r).$$

Demostració. *Si un element és de la forma τa_i, amb $i = 1, \ldots, r$, el cicle de la dreta el porta a τa_{i+1} (o a τa_1 si $i = r$). Per altra banda, si li apliquem primer τ^{-1}, a continuació el cicle $(a_1, \ldots, a_r)$ i a continuació τ obtenim també τa_{i+1} (o τa_1 si $i = r$). Així docs $\tau(a_1, \ldots, a_r)\tau^{-1}$ i $(\tau a_1, \ldots, \tau a_r)$ coincideixen sobre elements de la forma τa_i, amb $i = 1, \ldots, r$.*
També coincideixen sobre els elements de la forma τa_i, amb $i = r+1, \ldots, n$, ja que aquests són fixos en els dos casos. □

Aquest lema ens diu que el conjugat d'un cicle d'ordre r és un cicle d'ordre r. En particular, el conjugat d'una composició de cicles és una composició de cicles de la mateixa longitud.
A més, dos cicles qualssevol de la mateixa longitud són conjugats, ja que només cal escollir γ adequadament. Per exemple, donats els cicles $(a_1, \ldots, a_r)$ i $(b_1, \ldots, b_r)$ elegim γ com qualsevol permutació tal que $\gamma(a_i) = b_i$.
Vist tot això i l'estructura de S_4 donada a la taula de la pàgina 44, veiem que a S_4 hi ha 5 classes d'equivalència per conjugació: les corresponents a les 5 columnes de la taula.

(c) Hem de demostrar que $d(\sigma) = d(\gamma\sigma\gamma^{-1})$. Però si descomponem σ com producte de cicles disjunts, per exemple dos,

$$\sigma = (a_1, \ldots, a_k)(b_1, \ldots, b_s),$$

llavors

$$\gamma\sigma\gamma^{-1} = \gamma(a_1, \ldots, a_k)\gamma^{-1}\gamma(b_1, \ldots, b_s)\gamma^{-1} = (\gamma a_1, \ldots, \gamma a_k)(\gamma b_1, \ldots, \gamma b_s),$$

és a dir, $\gamma\sigma\gamma^{-1}$ també descompon com a producte de dos cicles, que és fàcil veure, que també són disjunts.
Si en lloc de dos cicles n'hi ha més, l'argument és el mateix.
L'aplicació f no és ni injectiva ni exhaustiva. Només cal observar com funciona f en el cas $n = 4$ ja estudiat. Tenim concretament que $f : S_4/\sim \longrightarrow \{1, 2, 3, 4\}$ compleix

$$\begin{aligned} f(\bar{Id}) &= 4, \\ f(\overline{(1,2)}) &= 1, \\ f(\overline{(1,2,3)}) &= 1, \\ f(\overline{(1,2,3,4)}) &= 1, \\ f(\overline{(1,2)(3,4)}) &= 2, \end{aligned}$$

(d) Podríem repetir l'apartat (b) canviant S_4 per S_7. Però no cal escriure tots els elements de S_7, ja que només necessitem saber quants cicles i productes de cicles poden aparèixer a S_7. Equivalentment, hem de respondre la pregunta següent: de quantes maneres podem combinar números inferiors a 7 de manera que sumin 7?

$$\begin{aligned}
7 &= 1+1+1+1+1+1+1 \longrightarrow Id \\
7 &= 2+1+1+1+1+1 \longrightarrow (a_1,a_2) \\
7 &= 2+2+1+1+1 \longrightarrow (a_1,a_2)(b_1,b_2) \\
7 &= 2+2+2+1 \longrightarrow (a_1,a_2)(b_1,b_2)(c_1,c_2) \\
7 &= 3+1+1+1+1 \longrightarrow (a_1,a_2,a_3) \\
7 &= 3+2+1+1 \longrightarrow (a_1,a_2,a_3)(b_1,b_2) \\
7 &= 3+2+2 \longrightarrow (a_1,a_2,a_3)(b_1,b_2)(c_1,c_2) \\
7 &= 3+3+1 \longrightarrow (a_1,a_2,a_3)(b_1,b_2,b_3) \\
7 &= 4+1+1+1 \longrightarrow (a_1,a_2,a_3,a_4) \\
7 &= 4+2+1 \longrightarrow (a_1,a_2,a_3,a_4)(b_1,b_2) \\
7 &= 4+3 \longrightarrow (a_1,a_2,a_3,a_4)(b_1,b_2,b_3) \\
7 &= 5+1+1 \longrightarrow (a_1,a_2,a_3,a_4,a_5) \\
7 &= 5+2 \longrightarrow (a_1,a_2,a_3,a_4,a_5)(b_1,b_2) \\
7 &= 6+1 \longrightarrow (a_1,a_2,a_3,a_4,a_5,a_6) \\
7 &= 7 \longrightarrow (a_1,a_2,a_3,a_4,a_5,a_6,a_7)
\end{aligned}$$

66. Sigui A un conjunt finit d'n elements. Definim a $\mathcal{P}(A)$, el conjunt de les parts de A, la relació

$$X \sim Y \text{ si } \mid X \mid = \mid Y \mid .$$

Vegeu que és d'equivalència, descriviu el conjunt quocient i proveu que $\sum_{i=0}^{n} \binom{n}{i} = 2^n$.

Solució: *És clarament d'equivalència. El conjunt quocient està en bijecció amb $\{0,1,2,\ldots,n\}$ ja que dos conjunts són equivalents si i només si tenen el mateix nombre d'elements. I per a cada $0 \leq k \leq n$ hi ha un subconjunt de k elements.*
El número d'elements de $\mathcal{P}(A)$, que sabem que és 2^n, el podem trobar comptant quants elements té cada classe d'equivalència i sumant després totes aquestes quantitats (això és així ja que les classes d'equivalència formen una partició del conjunt).
Classe del 0. Un element: el conjunt buit.
Classe de l'1. n elements: els n subconjunts de 1 element.
Classe del 2. $\binom{n}{2}$: els $\binom{n}{2}$ subconjunts de 2 elements.
etc.

67. Considerem al pla $\mathbb{R}^2$ la relació $(x,y) \sim (x',y')$ si $(x-x', y-y') \in \mathbb{Z}^2$.

1. Proveu que és una relació d'equivalència i trobeu els elements de la classe de $(0,0)$. Feu el mateix per a la classe de $(\frac{5}{2},\frac{3}{2})$.
2. Proveu que cada classe d'equivalència té un representant al conjunt $[0,1]\times[0,1]$.
3. Descriviu el conjunt quocient $\mathbb{R}^2/\sim$. (*Indicació*: Observeu quins elements de $[0,1]\times[0,1]$ estan relacionats entre ells.)

Solució: *(1) És clarament d'equivalència. La classe del* $(0,0)$ *està formada per totes les parelles* (m,n) *amb* $m,n\in\mathbb{Z}$. *La classe del* $(\frac{5}{2},\frac{3}{2})$ *està formada per totes les parelles* $(m+\frac{5}{2},n+\frac{3}{2})$ *amb* $m,n\in\mathbb{Z}$.

(2) Observem que $(x,y)\sim(x-E(x),y-E(y))$, *on* $E(x)$ *denota la part entera del nombre real* x. *Observem que la classe del* $(0,0)$ *té* 4 *representants a* $[0,1]\times[0,1]$ *(*$(0,0),(0,1),(1,0),(1,1)$*).*

(3) El tor.

Llista 7

Conjunts infinits

68. Siguin A i B dos conjunts no buits. Demostreu que les afirmacions següents són equivalents

(i) Existeix una aplicació injectiva $f : A \longrightarrow B$.

(ii) Existeix una aplicació exhaustiva $g : B \longrightarrow A$.

Solució: *Vegeu problema 45.*

69. Demostreu les afirmacions següents.

(a) Si per a un conjunt infinit X existeix una aplicació injectiva $f\colon X \to \mathbb{N}$, aleshores X és numerable. En particular, tot subconjunt infinit d'un conjunt numerable és numerable.

(b) $\mathbb{Q}$ és numerable (utilitzant l'apartat anterior).

(c) Si A i B són numerables, aleshores $A \cup B$ és numerable. Per tant, la unió finita de conjunts numerables és numerable.

(d) Si A i B són numerables, aleshores $A \times B$ és numerable. Per tant, el producte cartesià d'un nombre finit de conjunts numerables és numerable. Per exemple, per tot $k \geq 1$, el conjunt $\mathbb{N}^k$ és numerable.

(e) La unió d'una família numerable de conjunts numerables és numerable.

(f) $\mathbb{Q}[x]$ és numerable.

Solució: *(a) Sigui $A = f(X)$. Observem que f com aplicació de X a A és bijectiva i que $A \subseteq \mathbb{N}$. Construirem una bijecció $\Phi : \mathbb{N} \longrightarrow A$ (i per tant, tindrem una bijecció entre $\mathbb{N}$ i X).*
Definim Φ sobre els nombres naturals així:

$$\begin{aligned}
\Phi(1) &= \textit{primer element de } A, \quad (\Phi(1) \leq a, \quad \forall a \in A).\\
\Phi(2) &= \textit{primer element de } A \setminus \Phi(1), \quad (\Phi(1) < \Phi(2) \leq a, \quad \forall a \in A).\\
\Phi(3) &= \textit{primer element de } A \setminus \Phi(1) \setminus \Phi(2), \quad (\Phi(1) < \Phi(2) < \Phi(3) \leq a, \quad \forall a \in A).\\
&\vdots
\end{aligned}$$

Aquest procés el podem fer per a tot $n \in \mathbb{N}$ ja que A és infinit. És a dir, sabem calcular $\Phi(n)$ per a tot $n \in \mathbb{N}$.
Aquesta Φ és clarament injectiva. Per veure que és exhaustiva observem primerament que per a tot $n \in \mathbb{N}$ es compleix que $n \leq \Phi(n)$. Prenem ara $a \in A$. Com que $a \leq \Phi(a)$ i entre $\Phi(1)$ i $\Phi(a)$ $(\Phi(1) < \Phi(2) < \cdots < \Phi(a))$ no hi ha altres elements de A que els $\Phi(i)$, resulta que ha de ser $a = \Phi(i)$, per a algun i amb $0 \leq i \leq a$. Però això diu que a pertany a la imatge de Φ i per tant Φ és exhaustiva.

(b) Considerem l'aplicació

$$\begin{array}{rccc} f: & \mathbb{Q} & \longrightarrow & \mathbb{N} \\ & (-1)^a \frac{p}{q} & \mapsto & 2^a 3^p 5^q \end{array}$$

que és clarament injectiva (més endavant veurem que la descomposició d'un nombre enter en producte de primers és única).
La típica demostració de que $\mathbb{Q}$ és numerable és l'anomenat lema de la serp, que consisteix en seguir la fletxa del diagrama següent, saltant les parelles equivalents (per exemple, quan s'arriba al $(2,4)$, com ja s'ha passat abans pel $(1,2)$, el $(2,4)$ ja no es considera). Aquest diagrama també demostra que $\mathbb{N} \times \mathbb{N}$ és numerable (cosa que també es pot demostrar considerant l'aplicació injectiva $f : \mathbb{N} \times \mathbb{N} \longrightarrow \mathbb{N}$ donada per $f(m,n) = 2^m 3^n$).

$$\begin{pmatrix} (1,1) & \to & (1,2) & & (1,3) & \to \\ & \swarrow & & \nearrow & & \\ (2,1) & & (2,2) & & (2,3) & \dots \\ \downarrow & \nearrow & & & & \\ (3,1) & & & & & \\ \vdots & & & & & \end{pmatrix}$$

Si volem agafar a la vegada els positius i negatius podem seguir les fletxes del diagrama següent començant en $(0,1)$.

$$\begin{pmatrix} (-2,1) & \leftarrow & (-1,1) & & (0,1) & \to & (1,1) & & (2,1) \\ & \searrow & & \nwarrow & & \swarrow & & \nearrow & \\ (-2,2 & & (-1,2) & & (0,2) & & (1,2) & & (2,2) \\ & & & \searrow & & \nearrow & & & \\ & & & & (0,3) & & & & \end{pmatrix}$$

(c) Primera demostració. *Podem escriure $A = \{a_1, a_2, \dots\}$, $B = \{b_1, b_2, \dots\}$ i aplicar el lema de la serp*

$$\begin{pmatrix} a_1 & \to & a_2 & & a_3 & \to & a_4 \\ & \swarrow & & \nearrow & & \swarrow & \\ b_1 & \to & b_2 & & b_3 & \to & b_4 \end{pmatrix}$$

Segona demostració. *Siguin $f : A \longrightarrow \mathbb{N}$ i $g : B \longrightarrow \mathbb{N}$ bijeccions. Definim $F : A \cup B \longrightarrow \mathbb{N}$ per*

$$\begin{aligned} F(a) &= 3f(a), \quad si \quad a \in A \setminus A \cap B \\ F(a) &= 3g(a) + 1, \quad si \quad a \in B \setminus A \cap B \\ F(a) &= 3f(a) + 2, \quad si \quad a \in A \cap B \end{aligned}$$

Aquesta F és injectiva.
Tercera demostració. *Amb la mateixa notació que a la segona demostració, definim $G : \mathbb{N} \times \{1,2\} \longrightarrow A \cup B$ per*

$$\begin{aligned} G(n,1) &= f^{-1}(n) \\ G(n,2) &= g^{-1}(n) \end{aligned}$$

És clarament exhaustiva. Pel problema 68 hi ha una aplicació injectiva $h : A \cup B \longrightarrow \mathbb{N} \times \{1,2\}$. Com $\mathbb{N} \times \{1,2\}$ és numerable, podem composar h amb una bijecció entre $\mathbb{N} \times \{1,2\}$ i $\mathbb{N}$ i ja tindrem una injecció entre $A \cup B$ i $\mathbb{N}$.
Una possible bijecció entre $\mathbb{N} \times \{1,2\}$ i $\mathbb{N}$ seria per exemple $q : \mathbb{N} \times \{1,2\} \longrightarrow \mathbb{N}$ donada per $q(n,1) = 2n+1$ i $q(n,2) = 2n$.

(d) Primera demostració. *Podem veure pel Lema de la serp que $\mathbb{N} \times \mathbb{N}$ és numerable i construir llavors*

$$\begin{array}{ccc} A \times B & \longrightarrow & \mathbb{N} \times \mathbb{N} \\ (a,b) & \mapsto & (f(a), g(b)) \end{array}$$

Segona demostració.

$$\begin{array}{ccc} A \times B & \longrightarrow & \mathbb{N} \\ (a,b) & \mapsto & 2^{f(a)}3^{g(b)} \end{array}$$

(e) Primera demostració. *Lema de la serp.*
Segona demostració. *Sigui A_m, $m \in \mathbb{N}$, la família numerable de conjunts numerables.*
Això vol dir que tenim aplicacions bijectives $f_m : \mathbb{N} \longrightarrow A_m$, per a cada $m \in \mathbb{N}$.
Definim

$$\begin{array}{ccc} \mathbb{N} \times \mathbb{N} & \longrightarrow & \cup_{\alpha \in \mathbb{N}} A_\alpha \\ (m,n) & \mapsto & f_m(n) \end{array}$$

Aquesta aplicació és exhaustiva, i per tant, pel problema 68 tenim una aplicació injectiva de la unió dels A_α a $\mathbb{N} \times \mathbb{N}$, i com que aquest és numerable, hem acabat.

(f) $\mathbb{Q}[x]$ és unió (numerable) dels polinomis de grau zero, amb els polinomis de grau 1, amb els polinomis de grau 2, etc. Els polinomis d'un grau fixat, per exemple n, estan en bijecció amb $\mathbb{Q}^{n+1}$ ja que queden determinats pels seus $n+1$ coeficients. Així el conjunt de polinomis de grau n és numerable i $\mathbb{Q}[x]$ també per ser unió numerable de numerables.

70. Demostreu que els intervals de nombres reals $[a,b]$ i $[0,1]$ són equipotents.

Solució: *És suficient considerar la bijecció*

$$\begin{array}{ccc} [0,1] & \longrightarrow & [a,b] \\ x & \mapsto & (b-a)x + a. \end{array}$$

71. Demostreu que X no és equipotent a $\mathcal{P}(X)$. En particular $\mathcal{P}(\mathbb{N})$ no és numerable.

Solució: *Suposem que existeix $f : X \longrightarrow \mathcal{P}(X)$ bijectiva. Sigui*

$$B = \{x \in X; x \notin f(x)\}.$$

Observem que $f(x)$ és un subconjunt de x al qual x pot pertànyer o no. Sigui $b \in X$ tal que $f(b) = B$.
Llavors $b \in B$ si i només si $b \notin B$, la qual cosa és una contradicció, i per tant no pot haver-hi cap bijecció entre X i $\mathcal{P}(X)$.

72. Demostreu que $\mathcal{P}(\mathbb{N})$ és equipotent al conjunt de successions de zeros i uns.

Solució: *Sigui S el conjunt de successions de zeros i uns. Definim una aplicació $f : \mathcal{P}(\mathbb{N}) \longrightarrow S$ per $f(A) = (a_1, a_2, a_3, \dots)$ on*

$$a_i = \begin{cases} 1 & \text{si } i \in A \\ 0 & \text{si } i \notin A \end{cases}$$

Es fàcil veure que f és bijectiva.
En particular hem vist que S no és numerable, cosa que també podem veure directament usant el mètode de la diagonal (el mateix que s'utilitza per provar que $\mathbb{R}$ no és numerable).

73. Digueu si els conjunts següents són finits, numerables o infinits no numerables.

$$\mathbb{N}, \quad \{e, \pi, \sqrt{2}, \ln(5)\}, \quad [-\pi, \pi] \cap \mathbb{Q}, \qquad \mathbb{Q}^4, \quad \mathcal{P}(\mathbb{N}), \quad (-1, 1).$$

Solució: *Per ordre: Numerable, finit, numerable, numerable, no numerable, no numerable.*

74. Demostreu que l'aplicació $f : \mathbb{N} \times \mathbb{N} \longrightarrow \mathbb{N}$ donada per

$$f(m, n) = 2^m(2n + 1) - 1$$

és una bijecció. Tenim doncs una altra manera de veure que $\mathbb{N} \times \mathbb{N}$ és numerable.

Solució: *La injectivitat la deixem com exercici. Per veure que és exhaustiva prenem $a \in \mathbb{N}$ i busquem $(m, n) \in \mathbb{N} \times \mathbb{N}$ tal que*

$$f(m, n) = 2^m(2n + 1) - 1 = a.$$

Per a això només hem de descompondre $a + 1$ en factors primers.

75. Demostreu que l'aplicació $h : [0, 1] \longrightarrow [0, 1)$ donada per

$$h(x) = \begin{cases} x & \text{si } x \neq \dfrac{1}{2^i}, \quad \forall i, \\ \dfrac{1}{2^{i+1}} & \text{si } x = \dfrac{1}{2^i} \text{ per a algun } i. \end{cases}$$

és bijectiva. Per tant, $[0,1]$ i $[0,1)$ són equipotents.

Solució: *Injectiva. Si suposem $h(x) = h(y)$ veiem de seguida que això només es pot donar si x i y són, a la vegada, potències o no de $\frac{1}{2}$. Si les dues són potències de $\frac{1}{2}$ i $h(x) = h(y)$ aquesta potència ha de ser la mateixa, i per tant $x = y$. Si cap de les dues és potència de $\frac{1}{2}$, llavors tenim $x = h(x)$ i $h(y) = y$, de manera que $h(x) = h(y)$ implica $x = y$, i hem acabat.*
Exhaustiva. Donat $x \in [0,1)$, si $x \neq \dfrac{1}{2^i}$ per a tot $i \in \mathbb{N}$, és clar que $h(x) = x$. Si $x = \dfrac{1}{2^i}$ per a algun $i \in \mathbb{N}$, prenem $y = 2x$ i tenim $h(y) = x$. Observem que $y \in [0,1]$ perquè $x \neq 1$. Per tant, tot element de $x \in [0,1)$ té antiimatge.

76. Demostreu que $\mathbb{R}$ i $(0,\infty)$ són equipotents. Demostreu que $(0,1)$ i $(0,\infty)$ són equipotents.

Solució: *La funció logaritme ens dóna una bijecció entre $(0,\infty)$ i $\mathbb{R}$. N'hi ha infinites més, per exemple*

$$f(x) = \begin{cases} 1/x & \text{si } 0 < x \leq 1 \\ -x+2 & \text{si } x \geq 1 \end{cases}$$

La mateixa aplicació considerada al problema 70 ens diu que (a,b) és equipotent a $(0,1)$, per a tota parella $a, b \in \mathbb{R}$ amb $a < b$. En particular $(0,1)$ és equipotent a l'interval $(-\frac{\pi}{2}, \frac{\pi}{2})$, el qual és equipotent amb $\mathbb{R}$ via la tangent.

77. El Teorema de Schroeder Bernstein diu: *Si per a dos conjunts X i Y existeixen dues aplicacions injectives $f : X \to Y$ i $g : Y \to X$, aleshores X i Y tenen el mateix cardinal (és a dir, existeix una aplicació bijectiva $h : X \to Y$).*
Usant aquest resultat, demostreu que

(a) $\mathbb{R}$ i $[0,1]$ són equipotents.

(b) $[0,1) \times [0,1)$ i $[0,1)$ són equipotents.

(c) $\mathbb{R}^2$ i $\mathbb{R}$ són equipotents.

Solució: *(a) Com que tenim una bijecció entre $\mathbb{R}$ i $(0,1)$, i aquest s'injecta canònicament a $[0,1]$, tenim, simplement composant aplicacions, una injecció de $\mathbb{R}$ a $[0,1]$. Per altra banda, com $[0,1] \subset \mathbb{R}$, tenim una inclusió (la inclusió canònica) de $[0,1]$ a $\mathbb{R}$. Pel teorema de Schroeder Bernstein tenim el resultat.*

(b) Tenim una injecció de $[0,1)$ a $[0,1) \times [0,1)$ evident, per exemple $x \mapsto (x,0)$. Per construir una injecció en sentit contrari, i poder aplicar així el teorema de Schroeder Bernstein, podem fer el següent:
Pensem els elements de $[0,1)$ com expressions decimals amb número finit de zeros (en lloc d'escriure, per exemple 0.5 escrivim $0,4999\ldots$). D'aquesta manera l'expressió decimal dels elements de $[0,1)$ és única. Llavors definim

$$\phi : [0,1) \times [0,1) \longrightarrow [0,1)$$

per

$$\phi(0.a_1a_2a_3\ldots, 0.b_1b_2b_3\ldots) = 0.a_1b_1a_2b_2a_3b_3\ldots$$

Per la unicitat de l'expressió decimal que hem comentat abans, aquesta aplicació es injectiva.

(c) Ajuntant el problema 75 amb el problema 77(a), veiem que $\mathbb{R}$ *és equipotent a* $[0, 1)$*. Ara el resultat és conseqüència de 77(b).*

Llista 8

Problemes de comptar

78. Proveu que si n és un enter senar i σ es una permutació de S_n, aleshores el producte $(1-\sigma(1))(2-\sigma(2))\dots(n-\sigma(n))$ és parell.

Solució: *Posem $n = 2k+1$. Entre els números $\sigma(1),\dots,\sigma(n)$ n'hi ha $k+1$ imparells i k parells, ja que són només una reordenació de $1,2,\dots,2k+1$. Per tant, no totes les parelles $(j-\sigma(j))$ poden estar formades per un parell i un imparell. Per tant, n'hi ha almenys una formada per dos parells o dos imparells. En ambdós casos el producte de totes elles és parell.*

79. Considereu una taulell d'escacs en què hem tret dues caselles, diagonalment oposades, de les cantonades. Creieu que és possible recobrir el taulell amb peces de dominó de la mida de dues caselles?

Solució: *Només cal observar que les dues caselles que traiem són les dues blanques, i que cada peça que posem tapa una casella blanca i una negra.*

80. Amb quants zeros acaba 1027! ?

Solució: *Comptem quants $5's$ apareixen a* $1027!$.
Només hem de mirar els múltiples de 5 *que van apareixen a la llista* $1,2,3,4,5,6,7,8,9,10,\dots,1027$.
Aquests són els números de la forma $5n$, amb $n = 1,2,\dots,205$, ja que $5\times 206 > 1027$. Així doncs, en multiplicar entre sí tots aquests números obtindrem

$$5\times(5\cdot 2)\times(5\cdot 3)\times\cdots\times(5\cdot 205) = 5^{205}\cdot 205!$$

I ara repetim el procés canviant 1027 *per* 205.
Comptem quants $5's$ apareixen a $205!$.
Només hem de mirar els múltiples de 5. *Aquests són els números de la forma $5n$, amb $n = 1,2,\dots,41$, ja que $5\times 42 > 205$. Així doncs, en multiplicar entre sí tots aquests números obtindrem*

$$5\times(5\cdot 2)\times(5\cdot 3)\times\cdots\times(5\cdot 41) = 5^{41}\cdot 41!$$

I ara repetim el procés canviant 205 *per* 41.

Comptem quants $5's$ *apareixen a* $41!$.
Només hem de mirar els múltiples de 5. *Aquests són els números de la forma* $5n$, *amb* $n = 1, 2, \ldots, 8$, *ja que* $5 \times 9 > 41$. *Així doncs, en multiplicar entre sí tots aquests números obtindrem*

$$5 \times (5 \cdot 2) \times (5 \cdot 3) \times \cdots \times (5 \cdot 8) = 5^8 \cdot 8!$$

$8!$ *només té un cinc.*
Resumint, a la descomposició en factors primers de $1027!$ *apareixen*

$$5^{205} \cdot 5^{41} \cdot 5^8 \cdot 5 = 5^{255}.$$

Com que és clar que a la descomposició en factors primers de $1027!$ *apareixen més dosos que cincs, podem formar tants deus com cincs tenim, de manera que* $1027!$ *és múltiple de* 10^{255}, *i acaba doncs en* 255 *zeros.*

81. Quants números entre 1000 i 1100 hi ha no divisibles per 5 ni per 7?

Solució: *Definim*

$$\begin{aligned} A_5 &= \{n \in \mathbb{N}; 1000 \leq n \leq 1100,\ i\ n = \dot{5}\} \\ A_7 &= \{n \in \mathbb{N}; 1000 \leq n \leq 1100,\ i\ n = \dot{7}\} \end{aligned}$$

El què es demana és justament el cardinal de $A_5^c \cap A_7^c$, *que denotarem per* $|A_5^c \cap A_7^c|$. *Pel principi d'inclusió exclusió tenim*

$$\begin{aligned} |A_5^c \cap A_7^c| &= 101 - |(A_5^c \cap A_7^c)^c| = 101 - |A_5 \cup A_7| \\ &= 101 - |A_5| - |A_7| + |A_5 \cap A_7|. \end{aligned}$$

Ara és fàcil veure que $|A_5| = 21$, *ja que* $1000 = 5 \cdot 200$ *i* $1100 = 5 \cdot 220$. *Anàlogament,* $|A_7| = 15$, *ja que* $1001 = 7 \cdot 143$ *i* $1099 = 7 \cdot 157$. *També,* $|A_5 \cap A_7| = 3$, *ja que* $1015 = 35 \cdot 29$ *i* $1085 = 35 \cdot 31$.
Hem utilitzat que els múltiples de 5 *i de* 7 *són els múltiples de* 35.
Per tant

$$|A_5^c \cap A_7^c| = 101 - 21 - 15 + 3 = 68.$$

82. Quants números entre 1 i 200 són senars i no quadrats.

Solució: *Definim*

$$\begin{aligned} A_1 &= \{\textit{senars entre } 1 \textit{ i } 200\} \\ A_2 &= \{\textit{quadrats entre } 1 \textit{ i } 200\} \end{aligned}$$

Ens demanen el cardinal de $A_1 \cap A_2^c$. *Pel principi d'inclusió exclusió tenim*

$$\begin{aligned} |A_1 \cap A_2^c| &= 200 - |(A_1 \cap A_2^c)^c| \\ &= 200 - |A_1^c \cup A_2| \\ &= 200 - |A_1^c| - |A_2| + |A_1^c \cap A_2| \\ &= 200 - 100 - 14 + 7 \\ &= 93. \end{aligned}$$

83. Quants nombres de l'1 al 90 no són divisibles ni per 2 ni per 3 ni per 5?

Solució: *Definim*

$$A_k = \{n \in \mathbb{N}; 1 \leq n \leq 90,\ i\ n = \dot{k}\}$$

El què es demana és justament el cardinal del complementari de $A_2 \cup A_3 \cup A_5$. *Pel principi d'inclusió exclusió tenim*

$$\begin{aligned} |A_2 \cup A_3 \cup A_5| &= |A_2| + |A_3| + |A_5| - |A_2 \cap A_3| - |A_2 \cap A_5| - |A_3 \cap A_5| + |A_2 \cap A_3 \cap A_5| \\ &= |A_2| + |A_3| + |A_5| - |A_6| - |A_{10}| - |A_{15}| + |A_{30}| \\ &= \frac{90}{2} + \frac{90}{3} + \frac{90}{5} - \frac{90}{6} - \frac{90}{10} - \frac{90}{15} + \frac{90}{30} = 66. \end{aligned}$$

Per tant $|(A_2 \cap A_3 \cup A_5)^c| = 24$.

84. Quants nombres de tres xifres hi ha que no siguin divisibles ni per 2 ni per 5?

Solució: *Definim*

$$\begin{aligned} A_2 &= \{n \in \mathbb{N}; 100 \leq n \leq 999,\ i\ n = \dot{2}\} \\ A_5 &= \{n \in \mathbb{N}; 100 \leq n \leq 999,\ i\ n = \dot{5}\} \end{aligned}$$

El què es demana és justament el cardinal de $A_2^c \cap A_5^c$. *Pel principi d'inclusió exclusió tenim*

$$\begin{aligned} |A_2^c \cap A_5^c| &= 900 - |(A_2^c \cap A_5^c)^c| = 900 - |A_2 \cup A_5| \\ &= 900 - |A_2| - |A_5| + |A_2 \cap A_5|. \end{aligned}$$

Ara és fàcil veure que $|A_2| = 450$, $|A_5| = 180$, *i* $|A_2 \cap A_5| = 90$.
Per tant

$$|A_5^c \cap A_7^c| = 900 - 450 - 180 + 90 = 360.$$

85. Donat un número natural, n, definim la seva Φ d'Euler com el número natural

$$\Phi(n) := \text{nombre de números naturals } x \text{ comprimers amb } n \text{ i tals que } 1 \leq x \leq n$$

Per exemple

$$\Phi(3) = 2\,,\ \Phi(4) = 2\,,\ \Phi(6) = 2\,,\ \Phi(8) = 4.$$

1. Calculeu $\Phi(7)\,,\ \Phi(11)\,,\ \Phi(12)\,,\ \Phi(30)\,,\ \Phi(9)\,,\ \Phi(27)$.
2. Demostreu que $\Phi(p) = p - 1$ si p és primer.
3. Demostreu que $\Phi(p^k) = p^k - p^{k-1}$ per a tot $k \geq 1$ i p primer.
4. Demostreu que si la descomposició d'un número natural n en producte de primers diferents és

   $$n = p_1^{k_1} p_2^{k_2} \dots p_m^{k_m}$$

   i $x \in \mathbb{Z}$, aleshores

   $$x \text{ és coprimer amb } n \iff x \text{ no és múltiple de } p_i, \text{ per a tot } i$$

5. Amb la notació de l'apartat anterior, siguin

   $$A_i := \{x \in \mathbb{N} \mid 1 \leq x \leq n,\ x \text{ és múltiple de } p_i\}.$$

   Calculeu $|A_i|\ ,\ |A_i \cap A_j|\ ,\ |A_i \cap A_j \cap A_t|\ ,\ \dots$
6. Useu els apartats anteriors i el principi de inclusió-exclusió per deduir la fórmula de càlcul de $\Phi(n) = |(A_1 \cup \dots \cup A_m)^c|$:

   $$\Phi(n) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\dots\left(1 - \frac{1}{p_m}\right)$$

Solució: *Veure ACM, pàgina* 135.

86. Proveu que existeix un enter n tal que 7^n acaba amb 001.

Solució: Primer mètode. *Considero tots els restos que obtenim en dividir* 7^n *entre* 1000, *en variar* $n \in \mathbb{N}$. *Quan hem fet aquesta operació per a més de 1000* $n's$ *diferents, algun reste s'ha de repetir.*
De manera que tindrem, per a dos $p, q \in \mathbb{N}$ *diferents (suposem* $p < q$*),* $7^p = 1\dot{0}00 + r$ *i* $7^q = 1\dot{0}00 + r$. *Restant obtenim*

$$7^p(7^{q-p} - 1) = 1\dot{0}00.$$

Com 7 *no divideix* 1000, *ha de ser* $7^{q-p} - 1 = 1\dot{0}00$, *i hem acabat.*

Segon mètode. *Com* 7 *i* 1000 *són coprimers, la congruència d'Euler* $a^{\Phi(m)} \equiv 1 \ (mod\ m)$, *(ACM*[1], *p. 183) ens diu que*

$$7^{\Phi(1000)} \equiv 1_{(1000)}$$

on Φ *és la funció d'Euler. Per tant, el número* n *buscat és* $n = \Phi(1000)$.
Si el volem calcular explícitament, apliquem el problema anterior i tenim $\Phi(1000) = 1000(1 - \frac{1}{2})(1 - \frac{1}{5}) = 400$. *Així, aquest segon mètode dóna més informació que el primer.*

[1] *Introducció a l'àlgebra abstracta*, R. Antoine, R. Camps, J. Moncasi, Manuals UAB, **46**, 2006.

Llista 9

Combinatòria

87. Quants cicles de longitud 6 hi ha a S_{10}?

Solució: *Els cicles de longitud* 6 *de* S_{10} *s'escriuen elegint, en un ordre determinat,* 6 *elements del conjunt* $\{1,2,3,4,5,6,7,8,9,10\}$. *Això correspon exactament a la definició de* variacions de 10 elements elegits de 6 en 6. *Però com els cicles són cíclics hem de tenir en compte que*

$$(a_1,a_2,a_3,a_4,a_5,a_6)=(a_2,a_3,a_4,a_5,a_6,a_1)=(a_3,a_4,a_5,a_6,a_1,a_2)=\dots$$

i, per tant, el número de variacions s'ha de dividir per 6. *Per tant*

$$\textit{Cicles de longitud } 6 = V_{10}^6/6 = (10\cdot 9\cdot 8\cdot 7\cdot 6\cdot 5)/6 = 10\cdot 9\cdot 8\cdot 7\cdot 5.$$

88. De quantes maneres podem ordenar les 26 lletres de l'alfabet de manera que:

(a) Les lletres M,A,T,E,S surtin totes 5 juntes i en aquest ordre.

(b) Igual que a l'apartat anterior però no necessàriament en aquest ordre.

(c) Les lletres M,A,T,E,S no surtin totes 5 juntes.

Solució: *(a) La M només pot ocupar les* 22 *primeres posicions. Un cop fixada M queden fixades la A,T,E,S, i queden 21 espais lliures. Per tant la resposta és*

$$22\cdot 21! = 22!$$

(b) Permutem MATES a l'apartat anterior i tenim

$$22!\cdot 5!$$

(c) El complementari de (b). Per tant

$$26! - 22!\cdot 5!$$

89. Una butlleta de la Lotto 6/49 consta de 49 caselles numerades de l'1 al 49. Una aposta consisteix en marcar 6 d'aquests 49 números. Suposem que una persona addicte al joc vol encertar amb tota seguretat.

(a) Calculeu quantes butlletes ha d'emplenar.

(b) Quantes d'aquestes encertaran només 5 números?

(c) Quantes butlletes obtindran premi? (Obtenim premi si encertem 3 o més números)

Solució: *(a)*

$$\binom{49}{6} = 13983816.$$

(b) Suposem que la combinació guanyadora ha estat $\{1,2,3,4,5,6\}$*. Hi ha* $\binom{6}{5}$ *maneres d'elegir* 5 *números d'entre aquests* 6*. Suposem que elegim* $\{1,2,3,4,5\}$*. Quantes butlletes hi ha amb aquests* 5 *números i amb el sisè diferent de* 6*? Doncs, clarament,* 43*. Total*

$$43 \cdot 6 = \binom{43}{1}\binom{6}{5} = 258.$$

(c) Mirem primer, comparant amb l'apartat (b), quantes butlletes hi ha amb exactament 4 *resultats encertats. El mateix argument ens diu que la resposta és*

$$\binom{6}{4}\binom{43}{2}$$

Per exemple, si hem encertat només els números $1,2,3,4$*, els altres dos números poden ser qualsevols dels 43 restants, però no importa l'ordre, i.e. per exemple les ordenacions* $\{1,2,3,4,7,8\}$ *i* $\{1,2,3,4,8,7\}$ *donen lloc a la mateixa butlleta.*
Anàlogament trobem que hi ha

$$\binom{6}{3}\binom{43}{3}$$

butlletes amb exactament 3 *resultats encertats.*
Finalment, doncs, hi ha

$$1 + \binom{43}{1}\binom{6}{5} + \binom{43}{2}\binom{6}{4} + \binom{43}{3}\binom{6}{3} = 569149.$$

butlletes premiades.

90. Quantes solucions enteres té l'equació $x_1 + x_2 + x_3 + x_4 + x_5 = 128$ amb $x_i \geq 0$? I amb $x_i \geq 1$?

Solució: *No s'està preguntant de quantes maneres diferents podem sumar* 5 *números perquè doni* 128. *En aquesta pregunta no importaria l'ordre (per exemple 124 més quatre* $1's$*) i en canvi les solucions de l'equació donada depenen de l'ordre (les solucions* $x_1 = 124$, $x_2 = x_3 = x_4 = x_5 = 1$ *i* $x_2 = 124$, $x_1 = x_3 = x_4 = x_5 = 1$ *són diferents).*
La manera estàndard de pensar aquest tipus de problemes és imaginar una fila amb 132 *espais, i ocupar aquests espais amb* 128 $1's$*, i* 4 *pals verticals. Si dos pals apareixen consecutivament assignem el valor zero a la variable corresponent.*
Per exemple

$$1 \quad 1 \quad | \quad | \quad 1 \quad 1 \quad \dots \quad 1 \quad | \quad | \quad 1 \quad 1$$

correspondria a $x_1 = 2, x_2 = 0, x_3 = 124, x_4 = 0, x_5 = 2$.
I

$$| \quad 1 \quad 1 \quad | \quad 1 \quad 1 \quad \dots \quad 1 \quad | \quad 1 \quad 1 \quad |$$

correspondria a $x_1 = 0, x_2 = 2, x_3 = 124, x_4 = 2, x_5 = 0$.
Així, doncs, la pregunta que es fa és equivalent a saber de quantes maneres podem posar 4 *pals en* 132 *espais. Resposta, en el cas* $x_1 \geq 0$,

$$\binom{132}{4}.$$

Estudiem ara el cas $x_i \geq 1$. *Fem el canvi de variable* $y_i = x_i - 1$. *Així, si les* x_i *són solució del problema donat, tenim*

$$y_1 + y_2 + y_3 + y_4 + y_5 = 123.$$

I recíprocament, qualsevol solució d'aquí amb $y_i \geq 0$, *ens dóna lloc a unes* x_i *que sumen* 128.
Com que aquestes y_i *compleixen que* $y_i \geq 0$, *estem en el cas anterior i la resposta és*

$$\binom{127}{4}.$$

91. Quin és el coeficient de $x^5y^8z^6$ en el desenvolupament de l'expressió $(xy + yz + z^{3/2})^{10}$?

Solució: *Utilitzarem el teorema multinomial (ACM, p.130).*

$$(a + b + c)^n = \sum_{i+j+k=n} \binom{n}{ijk} a^i b^j c^k.$$

Apliquem aquesta fórmula amb $n = 10$, $a = xy$, $b = yz$, $c = z^{3/2}$. *Tenim*

$$(xy + yz + z^{3/2})^{10} = \sum_{i+j+k=10} \binom{10}{ijk} x^i y^i y^j z^j (z^{3/2})^k.$$

El terme que ens interessa és $i = 5$, $i + j = 8$, $k = 2$. Observem que en aquest cas l'exponent de z és 6. Per tant

$$\binom{10}{5\ 3\ 2} = \frac{10!}{5! \cdot 3! \cdot 2!}.$$

92. (a) Quantes transposicions hi ha a S_{10} ? (b) I quantes permutacions d'ordre 30? (c) I quantes permutacions d'ordre 15?

Solució: *(a) Tantes com parelles no ordenades.*

$$\binom{10}{2} = 45.$$

(b) Per tenir ordre 30 hem de tenir (pensem que cada permutació descompon en producte de cicles disjunts i que el seu ordre és el m.c.m. dels ordres)

$$30 = 30 \cdot 1 = 15 \cdot 2 = 10 \cdot 3 = 6 \cdot 5 = 2 \cdot 3 \cdot 5.$$

Com estem a S_{10} només és possible la darrera solució, ja que la suma dels elements dels cicles involucrats no pot superar 10.
Número de cicles d'ordre 2: tants com parelles no ordenades es poden formar amb 10 elements:

$$\binom{10}{2}.$$

Un cop fixat un cicle d'ordre 2 ens queden 8 elements.
Número de cicles d'ordre 3: tants com ternes ordenades es poden formar amb $10 - 2$ elements, dividit per tres, perquè els cicles són cíclics ($(a_1, a_2, a_3) = (a_2, a_3, a_1) = (a_3, a_1, a_2)$):

$$V_8^3/3 = 8 \cdot 7 \cdot 6/3 = 112.$$

També podem pensar que hi ha tants cicles d'ordre 3 com ternes no ordenades ($\binom{8}{3}$) multiplicat per 3! per ordenar-les, dividit per 3, pel mateix argument d'abans de que els cicles són cíclics: total

$$\binom{8}{3} \cdot 3!/3 = \binom{8}{3} \cdot 2 = 112.$$

Finalment, un cop fixat un cicle d'ordre 2 i un d'ordre 3 ens queden 5 elements. Tenim 5! maneres d'ordenar-los, i per ser cicles d'ordre 5 (les ordenacions cícliques són iguals) hem de dividir per 5. Total

$$\binom{10}{2} \cdot \binom{8}{3} \cdot 2 \cdot 4! = 120960.$$

(c) En aquest cas la permutació és producte d'un cicle d'ordre 3 per un d'ordre 5 (mateix argument que l'apartat anterior).

Número de cicles d'ordre 3. *També com en l'apartat anterior, sabem que n'hi ha*

$$\binom{10}{3} \cdot 2 = 240.$$

Número de cicles d'ordre 5 *que podem formar amb els* $10-3$ *elements restants. N'hi ha*

$$\binom{7}{5} \cdot 4! = 504$$

Total

$$\binom{10}{3} \cdot 2 \cdot \binom{7}{5} \cdot 4! = 120960.$$

93. Una banda de quinze delinqüents decideix atracar cinc bancs diferents simultàniament i han de decidir qui va a cadascun dels bancs.

(a) De quantes maneres es poden distribuir tenint en compte que tots han d'anar a algun banc i que a cada banc hi ha d'anar com a mínim un delinqüent?

(b) Si decideixen fer grups de tres, de quantes maneres es podran distribuir?

(c) Si, a més, han decidit repartir-se les tasques dins de cada grup (un vigila la porta, l'altre amenaça el personal i el tercer recull els diners), de quantes maneres es podran repartir la feina?

Solució: *(a)*[1] *Imaginem els lladres ordenats en una fila. A cadascun d'ells se li assigna un dels* 5 *bancs* B_1, B_2, B_3, B_4, B_5. *D'aquesta manera tenim una paraula de* 15 *lletres formada per les* 5 *lletres* B_1, B_2, B_3, B_4, B_5. *I sabem que totes les lletres hi han de sortir almenys un cop. Denotem*

$$P_i = \{\textit{paraules que contenen almenys un cop la lletra } B_i\}.$$

Volem calcular el cardinal de $P_1 \cap P_2 \cap P_3 \cap P_4 \cap P_5$. *Pel principi d'inclusió exclusió tenim*

$$\begin{aligned} |P_1 \cap P_2 \cap P_3 \cap P_4 \cap P_5| &= 5^{15} - |(P_1 \cap P_2 \cap P_3 \cap P_4 \cap P_5)^c| \\ &= 5^{15} - |P_1^c \cup P_2^c \cup P_3^c \cup P_4^c \cup P_5^c| \\ &= 5^{15} - \sum_i |P_i^c| + \sum_{i,j} |P_i^c \cap P_j^c| - \sum_{i,j,k} |P_i^c \cap P_j^c \cap P_k^c| + \dots \end{aligned}$$

Ara bé, observem que les paraules de 15 *lletres que no contenen la* B_1 *són les paraules de* 15 *lletres que es poden formar amb* B_2, B_3, B_4, B_5. *De les quals n'hi ha carament* 4^{15}.
Anàlogament, les paraules de 15 *lletres que no contenen la* B_1 *ni la* B_2 *són les paraules de* 15 *lletres que es poden formar amb* B_3, B_4, B_5. *De les quals n'hi ha carament* 3^{15}.

[1] Solució donada per Fernando Etayo.

Resumint

$$|P_i^c| = 4^{15}; \quad |P_i^c \cap P_j^c| = 3^{15}; \quad |P_i^c \cap P_j^c \cap P_k^c| = 2^{15}; \quad |P_i^c \cap P_j^c \cap P_k^c \cap P_l^c| = 1.$$

Així doncs,

$$|P_1 \cap P_2 \cap P_3 \cap P_4 \cap P_5| = 5^{15} - 5 \cdot 4^{15} + \binom{5}{2}3^{15} - \binom{5}{3}2^{15} + \binom{5}{4} = 25292030400.$$

(b) Imaginem els bancs ja ordenats, B_1, B_2, B_3, B_4, B_5*. Comptem ara els grups de* 3 *que podem formar amb els* 15 *lladres. Cada solució que obtinguem la imaginarem donada en cinc grups ordenats* G_1, G_2, G_3, G_4, G_5*. A partir d'aquí el grup* G_i *anirà al banc* B_i*.*
Comencem a fer els grups. Hi ha $\binom{15}{3}$ *maneres d'elegir* 3 *lladres d'entre els* 15 *inicials. És a dir,* $\binom{15}{3}$ *maneres de formar el grup* G_1*. Suposem doncs que n'elegim ja* 3 *i tenim format ja el grup* G_1*. Queden encara* 12 *lladres que hem de continuar distribuint en grups de* 3*. N'elegim* 3 *d'aquests, cosa que podem fer de* $\binom{12}{3}$ *maneres diferents. Un cop tenim dos grups de* 3 *lladres, en queden encara* 9 *que hem de distribuir en grups de* 3*. N'elegim* 3 *d'aquests, cosa que podem fer de* $\binom{9}{3}$ *maneres diferents. Un cop tenim tres grups de* 3 *en queden encara* 6 *que hem de distribuir en grups de* 3*. N'elegim* 3 *d'aquests, cosa que podem fer de* $\binom{6}{3}$ *maneres diferents. Un cop tenim quatre grups de* 3 *en queden només* 3 *i ja tenim els* 5 *grups de* 3*.*
Resumint

$$\binom{15}{3} \cdot \binom{12}{3} \cdot \binom{9}{3} \cdot \binom{6}{3} \cdot \binom{3}{3} = \frac{15!}{6^5} = 168168000.$$

Observem que tal com hem fet els càlculs hem comptat com diferents les solucions

$$G_{\sigma(1)}, G_{\sigma(2)}, G_{\sigma(3)}, G_{\sigma(4)}, G_{\sigma(5)}; \qquad \sigma \in S_5.$$

(c) El resultat anterior multiplicat per $(3!)^5$ *és a dir* $15!$*. El motiu de multiplicar per* $(3!)^5$ *és que permutem independentment cadascuna de les bandes. Observeu que el resultat és coherent amb la idea de posar-los a tots en una fila i anar assignant tascas: vigilant al banc A, amenaçador al banc A, recaptador al banc A, vigilant al banc B, ...*

Llista 10

Nombres Enters

94. Quin és el quocient i la resta quan dividim els enters
(a) 19 entre 7 (b) -111 entre 11 (c) 0 entre 19
(d) -1 entre 3 (e) -107 entre 101 (f) -23 entre -17.

Solució: *(b) Com que* $111 = 11 \cdot 10 + 1$ *tenim*

$$-111 = -11 \cdot 10 - 1 = 11 \cdot (-10) - 1 = 11 \cdot (-10) - 11 + 11 - 1 = 11 \cdot (-10 - 1) + 10 = 11 \cdot (-11) + 10.$$

(d) Com que $1 = 3 \cdot 0 + 1$ *tenim*

$$-1 = -3 \cdot 0 - 1 = -3 \cdot 0 - 3 + 3 - 1 = 3(-1) + 2$$

(f) Com que $23 = 17 \cdot 1 + 6$ *tenim*

$$-23 = -17 \cdot 1 - 6 = (-17) \cdot 1 - 6 = (-17) \cdot 1 - 17 + 17 - 6 = (-17) \cdot (1 + 1) + 10 = (-17) \cdot 2 + 11.$$

95. Proveu que si a, b són enters no nuls i $c \in \mathbb{N}$, aleshores $\text{mcd}(ca, cb) = c \cdot \text{mcd}(a, b)$.

Solució: Primera solució. *Recordem que* $d = mcd(a, b)$ *vol dir que l'ideal generat per* d *és l'ideal format per les combinacions lineals enteres de* a *i* b*:*

$$(d) = \{\lambda a + \mu b; \lambda, \mu \in \mathbb{Z}\}.$$

Denotem $\bar{d} = mcd(ca, cb)$*. Això vol dir*

$$(\bar{d}) = \{\lambda ca + \mu cb; \lambda, \mu \in \mathbb{Z}\}.$$

En particular,

$$\bar{d} = \lambda_1(ca) + \mu_1(cb) = c(\lambda_1 a + \mu_1 b) = c\xi d, \quad amb \quad \xi \in \mathbb{Z}.$$

Com que $d, \bar{d}$ *i* c *són positius, també* ξ *és positiu.*

També

$$cd = c(\lambda_0 a + \mu_0 b) = \lambda_0 ca + \mu_0 cb = \delta\bar{d}, \quad \text{amb} \quad \delta \in \mathbb{Z}.$$

Com abans, ta,bé δ és positiu. Per tant, combinant aquestes dues últimes igualtats, tenim

$$\bar{d} = \xi\delta\bar{d}.$$

Per tant, $\xi = \delta = 1$, i $\bar{d} = cd$.
Segona solució. *Acceptem que sabem que $d = mcd(a, b)$ si i només si $a = da'$, $b = db'$, amb $mcd(a', b') = 1$.*
Llavors, simplement multiplicant per c, tenim $ac = da'c = (dc)a'$, $bc = db'c = (dc)b'$, amb $mcd(a', b') = 1$, i hem acabat.

96. Proveu que no existeixen parelles d'enters a,b tals que $\text{mcd}(a, b) = 7$ i $a + b = 100$. En canvi, hi ha infinites parelles de nombres que compleixen $\text{mcd}(a, b) = 5$ i $a + b = 100$. Què diferencia els dos casos?

Solució: *Si posem*

$$\begin{aligned} a &= 7a' \\ 100 - a &= 7b' \end{aligned}$$

amb $mcd(a', b')$=1, tenim

$$100 = a + 7b' = 7a' + 7b' = \dot{7},$$

cosa que no és certa.
Si canviem 7 per 5 no obtenim contradicció, ja que 100 és múltiple de 5.
Prenem p qualsevol enter primer amb 20. N'hi ha infinits. Prenem

$$\begin{aligned} a &= 5p \\ b &= 100 - 5p \end{aligned}$$

Està clar que sumen 100 i (pel problema 95)

$$mcd(a, b) = mcd(5p, 5(20 - p)) = 5 \cdot mcd(p, 20 - p) = 5.$$

97. Calculeu $\text{mcd}(28n + 5, 35n + 2)$ per a tot $n \geq 1$.

Solució: *Recordem que si fem la divisió euclidiana de $a \in \mathbb{Z}$ entre $b \in \mathbb{Z}$, i posem $a = bq + r$, $0 \leq r < |q|$, tenim*

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

En el nostre cas tenim

$$mcd(35n+2, 28n+5) = mcd(28n+5, 7n-3) = mcd(7n-3, 17).$$

Com que 17 *és primer, aquest màxim comú divisor serà sempre* 1*, excepte en els casos en què* $7n-3 = \dot{17}$*, en que valdrà* 17*.*
Ara només hem de resoldre l'equació $7n \equiv 3$ *a* $\mathbb{Z}/(17)$*. Anem provant els valors i veiem que ha de ser* $n \equiv 15$*. És a dir,* $n = 15 + \dot{17}$*.*
Resumint

$$mcd(35n+2, 28n+5) = \begin{cases} 1 & si\ n \not\equiv 15 \pmod{17} \\ 17 & si\ n \equiv 15 \pmod{17} \end{cases}$$

98. Demostreu que la fracció $\dfrac{4n+5}{2n+3}$ és irreductible $\forall n \in \mathbb{N}$.

Solució: *Calculem el mcd de numerador i denominador.*

$$mcd(4n+5, 2n+3) = mcd(2n+3, -1) = 1.$$

Per tant és irreductible.

99. Demostreu que si a, b, c són enters no nuls aleshores

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

Calculeu el màxim comú divisor de $11339, 1173, 425$.

Solució: *Sigui* $d = mcd(b, c)$*. Demostrarem que l'ideal generat per* a *i* d*, que denotarem* (a, d)*, coincideix amb l'ideal generat per* a, b *i* c*, que denotarem* (a, b, c)*.*
Demostrem primer la inclusió $(a, b, c) \subseteq (a, d)$ *Sigui* $\alpha a + \beta b + \gamma c \in (a, b, c)$*. Com que tota combinació lineal de* b *i* c *és un múltiple de* d*, tenim* $\alpha a + \nu d \in (a, d)$*.*
Recíprocament, sigui $\alpha a + \beta d \in (a, d)$*. Com* $d = \beta_0 b + \gamma_0 c$*, per a certs* $\beta_0, \gamma_0 \in \mathbb{Z}$*, tenim* $\alpha a + \beta d = \alpha a + \beta(\beta_0 b + \gamma_0 c) \in (a, b, c)$*. Hem demostrat, doncs, que*

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

Com que tots els ideals de $\mathbb{Z}$ *són principals, existeix* $\bar{d} \in \mathbb{Z}$ *tal que*

$$(a, b, c) = (a, d) = (\bar{d}).$$

En particular, $mcd(a, d) = mcd(a, mcd(b, c)) = \bar{d}$*.*
Si revisem la demostració veurem que hem demostrat que donats tres enters arbitraris a, b, c*, es compleix que*

$$mcd(a, mcd(b, c)) = \bar{d}, \quad on \quad (\bar{d}) = (a, b, c).$$

Aplicant aquest resultat a la terna c, a, b hem acabat.
Finalment, com $mcd(1173, 425) = 17$ i $mcd(11339, 17) = 17$, $mcd(11339, 1173, 445) = 17$.

100. Demostreu que

1. Si a i b són coprimers i $a, b \geq 0$, aleshores $\text{mcm}(a, b) = a \cdot b$
2. Si $c \in \mathbb{N}$ aleshores $\text{mcm}(ca, cb) = c \cdot \text{ mcm}(a, b)$

Solució: *(a) És ben sabut que*

$$mcd(a, b) \cdot mcm(a, b) = ab.$$

Si a i b són coprimers, $mcd(a, b) = 1$, i hem acabat.
(b) Sabem que

$$mcd(ca, cb) \cdot mcm(ca, cb) = cacb.$$

Pel problema 95 tenim

$$mcd(ca, cb) \cdot mcm(ca, cb) = c \cdot mcd(a, b) \cdot mcm(ca, cb) = cacb.$$

Simplificant c,

$$mcd(a, b) \cdot mcm(ca, cb) = acb = c(ab) = c \cdot mcd(a, b) \cdot mcm(a, b).$$

Simplificant $mcd(a, b)$ hem acabat.

101. Proveu que si a, b són enters no nuls i $\text{mcd}(a, b) = d$, aleshores $\text{mcd}(a^2, b^2) = d^2$.

Solució: *Suposem primerament que $mcd(a, b) = 1$. Sigui $d = mcd(a^2, b^2)$. Volem demostrar que $d = 1$.*
Posem $a^2 = dA$, $b^2 = dB$, amb A i B coprimers. En particular, $a^2B = dAB = b^2A$. Ara utilitzem el resultat que diu que si $a|bc$, i a i b són coprimers, llavors $a|c$.
Com $a(aB) = b(bA)$, tenim que $a|b(bA)$. Per tant, com a i b són coprimers, $a|bA$. Com a i b són coprimers, $a|A$. Anàlogament deduïm $b|B$.
Podem escriure doncs $A = a\lambda$, $B = b\mu$, amb $\lambda, \mu \in \mathbb{Z}$. Així $a^2 = dA = da\lambda$ i $b^2 = dB = db\mu$. Simplificant, $a = d\lambda$, $b = d\mu$. Això ens diu que d és divisor comú de a i b, per tant ha de ser $d = 1$, com volíem.

Suposem ara $mcd(a, b) = d$. Posem $a = da'$, $b = db'$ amb $mcd(a', b') = 1$. En particular sabem, pel que acabem de demsostrar, que $mcd(a'^2, b'^2) = 1$. Per tant

$$d^2 = d^2 \cdot mcd(a'^2, b'^2) = mcd(d^2a'^2, d^2b'^2) = mcd(a^2, b^2).$$

102. Trobeu el màxim comú divisor de les parelles següents i expresseu-lo com a combinació lineal entera d'ells (*identitat de Bézout*):

$$52 \quad \text{i} \quad 127; \qquad 1237 \quad \text{i} \quad 4711; \qquad 2^2 5 \quad \text{i} \quad 7^2 25.$$

Solució: *Una manera de procedir per trobar els coeficients de Bézout de dos nombres enters D i d és disposar els càlculs com s'indica a la taula següent.*

	q_1	q_2	q_3	q_4	
D	d	r_1	r_2	r_3	
1	*0*	α_1	α_2	α_3	
0	*1*	β_1	β_2	β_3	

Sempre es complirà que

$$r_i = \alpha_i d + \beta_i D$$

és a dir, la segona fila és igual a la tercera multiplicada per D, més la quarta multiplicada per d. *El procediment que ara explicarem per omplir aquesta taula l'hem d'anar fent fins arribar a tenir un* 0 *a la segona fila. És a dir, fins que arribem a $r_{k+1} = 0$. Llavors*

$$mcd(D, d) = r_k, \quad r_k = \alpha_k D + \beta_k d.$$

És a dir, α_k, β_k són els coeficients de Bézout de la parella D, d.
Per omplir la taula primer es comença dividint D entre d:

$$D = dq_1 + r_1,$$

i s'agafa $\alpha_1 = 1$, $\beta_1 = -q_1$.

	$\mathbf{q_1}$				
D	**d**	$\mathbf{r_1}$			
1	*0*	*1*			
0	*1*	$-q_1$			

A continuació dividim d entre r_1

$$d = r_1 q_2 + r_2$$

i posem

	q_1	$\mathbf{q_2}$			
D	**d**	$\mathbf{r_1}$	$\mathbf{r_2}$		
1	*0*	*1*			
0	*1*	$-q_1$			

Per trobar α_2 i β_2 usarem les fórmules recurrents següents:

$$\begin{aligned} \alpha_i &= \alpha_{i-2} - q_i\alpha_{i-1} \\ \beta_i &= \beta_{i-2} - q_i\beta_{i-1} \end{aligned}$$

Si $i = 2$,

$$\begin{aligned} \alpha_2 &= \alpha_0 - q_2\alpha_1 = 1 + q_1q_2 \\ \beta_2 &= \beta_0 - q_2\beta_1 = -q_2 \end{aligned}$$

Ara dividim r_1 entre r_2,

$$r_1 = r_2q_3 + r_3$$

i continuem el procés.

	q_1	q_2	q_3	q_4	
D	d	r_1	r_2	r_3	
1	*0*	α_1	$\alpha_2 = \alpha_0 - q_2\alpha_1$	$\alpha_3 = \alpha_1 - q_3\alpha_2$	
0	*1*	β_1	$\beta_2 = \beta_0 - q_2\beta_1$	$\beta_3 = \beta_1 - q_3\beta_2$	

Apliquem-ho ara al cas particular $D = 127$ i $d = 52$. Dividim 127 entre 52. Quocient 2, resta 23.

	2				
127	52	**23**			
1	*0*	*1*			
0	*1*	*-2*			

A continuació dividim 52 entre 23. Quocient 2, resta 6.

	2	**2**			
127	52	23	**6**		
1	*0*	*1*			
0	*1*	-2			

I calculem α_2 i β_2 per la fórmula de recurrència $\alpha_2 = \alpha_0 - q_2\alpha_1$, $\beta_2 = \beta_0 - q_2\beta_1$.

	2	2			
127	52	23	6		
1	*0*	*1*	$\mathbf{-2}$		
0	*1*	-2	$\mathbf{-5}$		

A continuació dividim 23 entre 6. Quocient 3, resta 5.

	2	2	**3**		
127	52	23	6	**5**	
1	*0*	*1*	-2		
0	*1*	*-2*	*5*		

I calculem α_3 i β_3 per la fórmula de recurrència $\alpha_3 = \alpha_1 - q_3\alpha_2$, $\beta_3 = \beta_1 - q_3\beta_2$.

	2	2	*3*		
127	52	23	6	*5*	
1	*0*	*1*	-2	**7**	
0	*1*	-2	*5*	**-17**	

A continuació dividim 6 entre 5. Quocient 1, resta 1.

	2	2	3	**1**	
127	52	23	6	5	**1**
1	*0*	*1*	-2	*7*	
0	*1*	*-2*	*5*	*-17*	

I calculem α_4 i β_4 per la fórmula de recurrència $\alpha_4 = \alpha_2 - q_4\alpha_3$, $\beta_4 = \beta_2 - q_4\beta_3$.

	2	2	*3*	*1*	
127	52	23	6	*5*	*1*
1	*0*	*1*	*-2*	*7*	**-9**
0	*1*	*-2*	*5*	*-17*	**22**

Conclusió: el $mcd(127, 52) = 1$, i $22 \cdot 52 + (-9) \cdot 127 = 1$.

103. Resoleu les equacions diofàntiques següents:

$$(a)\ 45x + 21y = 3, \qquad (b)\ 9x + 12y = 2, \qquad (c)\ 7x - 5y = 1, \qquad (d)\ -16x + 12y = 20.$$

Solució: *(a) Mirem primer si el màxim comú divisor dels coeficients divideix el terme independent. Com $mcd(45, 21) = 3$, l'equació té solució.*
Dividim per 3 i tenim

$$15x + 7y = 1.$$

Per tant, x, y són els coeficients de Bézout de 15 i 7, i que podem trobar pel procediment explicat al problema anterior. En aquest cas, com que $15 = 7 \cdot 2 + 1$, tenim directament que $15 \cdot (1) + 7 \cdot (-2) = 1$. Així, una solució particular de $15x + 7y = 1$ és $x = 1$, $y = -2$. La solució general s'obté sumant a la solució particular la solució general de la homogènia $15x + 7y = 0$.

$$\begin{aligned} x &= 1 + 7\lambda, \\ y &= -2 - 15\lambda, \qquad \text{per a tot } \lambda \in \mathbb{Z}. \end{aligned}$$

(b) No té solució, ja que $mcd(9, 12) = 3$ no divideix el terme independent.

104. Es disposa d'un euro per comprar 40 segells de $1,4$ i 12 cèntims. Quants segells de cada un d'aquests preus es pot comprar?

Solució: *Sigui x = número de segells d'*1 *euro que podem comprar, y = número de segells de* 4 *euros, i z = número de segells de* 12 *euros. Tenim*

$$\begin{aligned} x + 4y + 12z &= 100, \\ x + y + z &= 40. \end{aligned}$$

Aïllant x a la segona equació i substituint aquest valor a la primera equació tenim

$$3y + 11z = 60,$$

equació diofàntica que té solució, ja que $mcd(3, 11) = 1$.
Una solució particular la podem trobar simplement combinant uns quants múltiples de 3 *amb uns quants de* 11*, per veure si tenim sort. Aquí es veu de seguida que $y = -2$, $z = 6$, és una solució particular.*
El mètode general no és tant bo com la nostra vista. En efecte, si fem l'algorisme d'Euclides entre 3 *i* 1 *obtenim*

	3	*1*	*2*
11	*3*	*2*	*1*
1	*0*	*1*	*-1*
0	*1*	*-3*	*4*

De manera que tenim $3 \cdot (4) + 11 \cdot (-1) = 1$. Multiplicant per 60 *obtenim una solució particular, concretament $y = 240$, $z = -60$.*
La solució general és doncs,

$$\begin{aligned} y &= 240 + 11\lambda, \\ z &= -60 - 3\lambda, \qquad \text{per a tot } \lambda \in \mathbb{Z}. \end{aligned}$$

que també es pot escriure com

$$\begin{aligned} y &= -2 + 11\lambda, \\ z &= 6 - 3\lambda, \qquad \text{per a tot } \lambda \in \mathbb{Z}. \end{aligned}$$

Ara bé, com que ha de ser $0 \leq x, y, z \leq 40$ hem de tenir $1 \leq \lambda \leq 2$. Si $\lambda = 1$, $y = 9$, $z = 3$, i per tant $x = 28$. Si $\lambda = 2$, $y = 20$, $z = 0$, i per tant $x = 20$.

105. Resoleu les equacions diofàntiques $111x + 36y = 15$, $10x + 26y = 1224$.

Solució: *Estudiem la primera. Podem dividir-la per* 3*: $37x + 12y = 5$. Els coeficients de Bézout de* 37 *i* 12 *són* 1 *i* -3*, és a dir*

$$37 \cdot (1) + 12 \cdot (-3) = 1.$$

Per tant, una solució particular és $x = 5$, $y = -15$, i la solució general

$$\begin{aligned} x &= 5 + 12\lambda \\ y &= -15 - 37\lambda. \end{aligned}$$

106. Demaneu a una persona que multipliqui el dia del mes en que va néixer per 12, que multipliqui el número del mes per 31 i que us digui només el resultat de sumar aquestes dues xifres. Endevineu quan l'heu de felicitar pel seu aniversari.
(*) S'us acut un mètode similar per codificar també l'any de naixement?

Solució: *Sigui* $1 \leq x \leq 31$ *el dia del naixement, i sigui* $1 \leq y \leq 12$ *el mes de naixement. Sigui* r *el resultat de fer la operació que es demana, és a dir,*

$$12x + 31y = r.$$

Aquest valor r *és, doncs, conegut per nosaltres.*
Els coeficients de Bézout de 12 *i* 31 *(coprimers) són* 13 *i* -5*, és a dir,*

$$12 \cdot (13) + 31 \cdot (-5) = 1.$$

Per tant, la solució general de l'equació diofàntica anterior és

$$\begin{array}{rcll} x & = & 13r + 31\lambda, & \\ y & = & -5r - 12\lambda, & \text{per a tot } \lambda \in \mathbb{Z}. \end{array}$$

Només hi ha una λ *tal que*

$$\frac{1}{31} - \frac{13}{31}r \leq \lambda \leq 1 - \frac{13}{31}r,$$

ja que l'interval $[\frac{1}{31} - \frac{13}{31}r, 1 - \frac{13}{31}r]$ *té longitud menor que* 1*. Aquesta desigualtat prové d'imposar que* x *està entre* 1 *i* 31*.*
Aquest valor de λ *ens permet calcular* x *i* y*.*
Tenim

$$\lambda = \begin{cases} -E(\frac{13}{31}r - 1) - 1, & si \quad \frac{13r}{31} \notin \mathbb{Z} \\ \\ -\frac{13r}{31} + 1, & si \quad \frac{13r}{31} \in \mathbb{Z} \end{cases}$$

on $E(t)$ *vol dir part entera de* $t \in \mathbb{R}$*. El segon cas només es dóna si la persona ha nascut el dia* 31*.*
Nota: El valor de λ *es pot donar de manera més condensada dient que* $\lambda = E[1 - \frac{13r}{31}]$*, ja que, si* $x \geq 0$ *tenim* $E[x] = -E[-x] - 1$ *si* $x \notin \mathbb{N}$*, i* $E[x] = -E[-x]$ *si* $x \in \mathbb{N}$*. Per exemple* $E[-1] = -1$*, i* $E[-1.2] = -2$*. Observem que* $(1 - \frac{13r}{31}) < 0$*.*

Exemple 1. Suposem una persona nascuda el 31 *de gener. Calcula* r *i obté*

$$r = 12x + 31y = 12 \cdot 31 + 31 \cdot 1 = 403$$

En particular, $\frac{13r}{31} = 169 \in \mathbb{Z}$*, i per tant* $\lambda = -169+1 = -168$*. Així* $x = 13r+31\lambda = 5239-5208 = 31$*, i* $y = -5r - 12\lambda = -2015 + 2016 = 1$*.*
Exemple 2. Suposem una persona nascuda el 16 *d'agost. Calcula* r *i obté*

$$r = 12x + 31y = 12 \cdot 16 + 31 \cdot 8 = 440$$

En particular, $\frac{13r}{31} = 184,5161\ldots \notin \mathbb{Z}$*, i per tant* $\lambda = -E(183,5161\ldots) - 1 = -183 - 1 = -184$*. Així* $x = 13r + 31\lambda = 5720 - 5704 = 16$*, i* $y = -5r - 12\lambda = -2200 + 2208 = 8$*.*

L'any de naixement es pot codificar de diverses maneres.
Podem començar com abans i fer calcular a una persona el mateix r d'abans, és a dir $r = 12d+31m$ amb d= dia del mes, entre 1 i 31, i m = mes de l'any, entre 1 i 12. Aquest número ell el coneix però nosaltres no.
A continuació li fem calcular un segon valor s donat per

$$s = 121r + 744a,$$

on a = número de l'any que va néixer menys 1900. Acceptarem $0 \leq a \leq 120$, és a dir que parlem amb una persona nascuda entre 1900 i 2020. Molt important remarcar que $744 = 2 \cdot 12 \cdot 31$. El valor de s sí que ens l'ha de dir. Posem 121 perquè l'interval on varia a té longitud 120 i volem un número primer amb 744 per tal de que l'equació diofàntica tingui solució.
A continuació resolem l'equació diofàntica

$$121t + 744z = s.$$

La solució general és de la forma

$$\begin{aligned} t &= t_0 + 744\lambda, \\ z &= z_0 - 121\lambda, \qquad \text{per a tot } \lambda \in \mathbb{Z}. \end{aligned}$$

on (t_0, z_0) és una solució particular. En aquesta equació z representa l'any de naixement menys 1900.
Hi ha una sola λ per a la que la solució general compleix $1 \leq z \leq 120$.
Per a aquesta λ calculem z i hem acabat.
Exemple: Suposem una persona nascuda el 16 d'agost de 1952. Aprofitant els càlculs de l'exemple 2 anterior sabem que $r = 440$.
A continuació li fem calcular

$$s = 121 \cdot 440 + 744 \cdot 52 = 91928.$$

Aquest número ens l'ha de comunicar i codifica dia, mes i any.
Plantegem la diofàntica

$$121t + 744z = 91928.$$

Busquem els coeficients de Bëzout de 121 i 744.

	6	*6*	*1*	*2*	*1*	*1*	
744	*121*	*18*	*13*	*5*	*3*	*2*	*1*
1	*0*	*1*	*-6*	*7*	*-20*	*27*	*-47*
0	*1*	*-6*	*37*	*-43*	*123*	*-166*	*289*

És a dir,

$$121 \cdot (289) + 744 \cdot (-47) = 1.$$

Una solució particular és doncs $t = 289 \cdot 91928 = 26567192$, $z = -47 \cdot 91928 = -4320616$.
La solució general és de la forma

$$\begin{aligned} t &= 26567192 + 744\lambda, \\ z &= -4320616 - 121\lambda, \qquad \textit{per a tot } \lambda \in \mathbb{Z}. \end{aligned}$$

En imposar que $0 \leq z \leq 120$, *veiem que ha de ser* $\lambda = 35708$, *que substituint a la solució general ens dóna que l'any de naixement d'aquesta persona és*

$$\textit{any naixement} = 1900 + z = 1900 - 4320616 - 121 \cdot 35708 = 1952.$$

107. En una batalla en que van participar entre 10000 i 11000 soldats resultaren morts el $\frac{23}{165}$ del total i ferits el $\frac{35}{143}$ del total. Quants soldats van resultar il·lesos?

Solució: *Sigui* x *el nombre total de soldats, i sigui* i *el nombre de soldats il·lesos. Tenim*

$$\frac{23}{165}x + \frac{35}{143}x + i = x.$$

Deduïm

$$i = \frac{1321}{11 \cdot 13 \cdot 15}x.$$

Com que 1321 *no és divisible ni per* 11, *ni per* 13 *ni per* 15, *ha de ser*

$$x = 11 \cdot 13 \cdot 15 \cdot \lambda.$$

La unica λ *que dóna per a* x *un valor entre* 10000 *i* 11000 *és* $\lambda = 8$, *per tant la resposta és* $x = 10568$.

108. Proveu[1] que a la successió de Fibonacci $1, 1, 2, 3, 5, \ldots$ dos termes consecutius són sempre primers entre ells. Recordem que donats $a, b \in \mathbb{Z}$, tenim $mcd(a, b) = mcd(a + \lambda b, b)$, per a tot $\lambda \in \mathbb{Z}$.

Solució: *Suposem, per inducció forta, que* F_{n-2} *i* F_{n-1} *són coprimers. Anem a demostrar que* F_{n-1} *i* F_n *són coprimers.*

$$mcd(F_{n-1}, F_n) = mcd(F_{n-1}, F_{n-1} + F_{n-2}) = mcd(F_{n-1}, F_{n-2}) = 1.$$

109. Calculeu 2011^{2011} mòdul 17.

Solució: *Hem de calcular*[2]

$$\overline{2011} \cdot \cdots \cdot \overline{2011}$$

classes considerades a $\mathbb{Z}/(17)$. *Ara bé, com que* $\overline{2011} = \overline{5}$, *en realitat hem de calcular*

$$\overline{5} \cdot \cdots \cdot \overline{5} = \overline{5}^{2011}$$

[1] La resta d'exercicis d'aquesta llista són del llibre *Àlgebra Lineal i Geometria*, de M. Castellet, I. Llerena.
[2] La comanda de Maple seria Power(2011, 2011), mod 17.

Però com que $\overline{5}^{16} = \overline{1}$, *i* $2011 = 125 \cdot 16 + 11$, *tenim*

$$\overline{5}^{2011} = \overline{5}^{16 \cdot 125 + 11} = ((\overline{5})^{16})^{125} \cdot \overline{5}^{11} = \overline{5}^{11} = \overline{11}.$$

Nota: Per saber que $\overline{5}^{16} = \overline{1}$ *ho podem fer a base d'anar provant totes les potències de* $\overline{5}$ *a* $\mathbb{Z}/(17)$, *o bé usar el petit teorema de Fermat que diu que si* a *i* p *són enters coprimers llavors*

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

Aquest teorema es demostra observant que a $\mathbb{Z}/(p)$ *multiplicar per* a *és una permutació.*

110. Demostreu que si $x \in \mathbb{Z}/(n)$ és invertible existeix $k \geq 1$ el mínim natural tal que $x^k = \bar{1}$. En aquest cas, vegeu que per a tot $m \in \mathbb{Z}$ es compleix que $x^m = x^r$ per algun enter $1 \leq r < k$. Useu això per calcular les últimes dues xifres de 3007^{1345}. Calculeu també l'invers a $\mathbb{Z}/(100)$ de $\bar{7}$.

Solució: *Considerem la successió* $x, x^2, x^3, \cdots \in \mathbb{Z}/(n)$. *Per ser* $\mathbb{Z}/(n)$ *finit ha des ser* $x^j = x^s$, *per a alguns* $j, s \in \mathbb{N}$. *Si* $j > s$, *multiplicant per* x^{-1} s *vegades, tenim* $x^{j-s} = 1 \in \mathbb{Z}/(n)$. *Denotem* $k = j - s$ *i fem la divisió euclidiana de* m *entre* k. *Tindrem* $m = qk + r$ *amb* $0 \leq r < k$.
Llavors és clar que $x^m = x^{qk+r} = (x^k)^q x^r = x^r$.

Per calcular les dues últimes xifres de 3007^{1345} *només hem de mirar aquest número a* $\mathbb{Z}/(100)$.
Observem que $\overline{3007} = \overline{7} \in \mathbb{Z}/(100)$. *I que* $\overline{7}^4 = \overline{1} \in \mathbb{Z}/(100)$.
Per tant, a $\mathbb{Z}/(100)$,

$$\overline{3007}^{1345} = \overline{7}^{1345} = \overline{7}^{(4 \cdot 336 + 1)} = (\overline{7}^4)^{336} \cdot \overline{7} = \overline{7}.$$

Equivalentment, les dues últimes xifres de 3007^{1345} *són* 07.

Finalment, com que hem vist que $\overline{7}^4 = \overline{1}$, *aquesta mateixa equació ens diu que* $\overline{7}^3 = \overline{7}^{-1}$. *Clarament* $\overline{7}^3 = \overline{43}$, *així doncs l'invers de* $\overline{7}$ *a* $\mathbb{Z}/(100)$ *és* $\overline{43}$.

111. Demostreu els criteris de divisibilitat per $3, 4, 5, 7, 9, 11, 13, 17, 19$.

Solució: *Hi ha diversos criteris en cada cas. Aquí en donem alguns.*

Divisibilitat per 3. Un número escrit en base decimal és divisible per 3 si i només si la suma dels seus dígits és divisible per 3.
En efecte, només cal veure que $n = a_k \ldots a_1 a_0 = \sum_{i=0}^{k} a_i 10^i$, *pensat a* $\mathbb{Z}/3$ *és*

$$\overline{n} = \overline{a_k} + \cdots + \overline{a_0} = \overline{a_k + \cdots + a_0}.$$

Com que un número és divisible per 3 *si i només si la seva classe mòdul* 3 *és zero, hem acabat.*

Divisibilitat per 4. Un número escrit en base decimal és divisible per 4 si i només si el doble de les desenes més les unitats $(2a_1 + a_0)$ és divisible per 4.
En efecte, només cal veure que $n = a_k \ldots a_1 a_0 = \sum_{i=0}^{k} a_i 10^i$, *pensat a* $\mathbb{Z}/4$ *és*

$$\overline{n} = \overline{2a_1} + \overline{a_0} = \overline{2a_1 + a_0}.$$

Divisibilitat per 5. Un número escrit en base decimal és divisible per 5 si i només si caba en 0 o 5. *En efecte, només cal veure que* $n = a_k \dots a_1 a_0 = \sum_{i=0}^{k} a_i 10^i$, *pensat a* $\mathbb{Z}/5$ *és*

$$\overline{n} = \overline{a_0}.$$

Divisibilitat per 7. Un número escrit en base decimal és divisible per 7 si i només si les unitats per 2 ($2a_0$) restada de la xifra que s'obté en suprimir les unitats ($(n - a_0)/10$) és divisible per 7. *En efecte, observem primer que l'invers de* $\overline{10}$ *a* $\mathbb{Z}/(7)$ *és* $\overline{5}$, *ja que*

$$\overline{10} \cdot \overline{5} = \overline{50} = \overline{1}.$$

Així, doncs, a $\mathbb{Z}/(7)$ *tenim*

$$\overline{\frac{n - a_0}{10} - 2a_0} = \overline{10^{-1}} \cdot \overline{n - a_0} - \overline{2a_0} = \overline{5}(\overline{n} - \overline{a_0}) - \overline{2a_0} = \overline{5n}.$$

Però $\overline{5n} = \overline{0}$ *si i només si* $5n$ *és divisible per* 7. *Com* 5 *i* 7 *són coprimers, això passa si i només si* n *és divisible per* 7.
Exemple: Per mirar si 70357 *és divisible per* 7 *fem* $7035 - 14 = 7021$. *Ara repetim el procés: fem* $702 - 2 = 700$, *que ja veiem que és múltiple de* 7.

Divisibilitat per 9. Un número escrit en base decimal és divisible per 9 si i només si la suma dels seus dígits és divisible per 9. *Igual que la divisibilitat per* 3, *però ara raonant a* $\mathbb{Z}/(9)$.

Divisibilitat per 11. Un número escrit en base decimal és divisible per 11 si i només si la suma dels seus dígits agafats de dos en dos és divisible per 11.
En efecte, només cal veure que $n = a_k \dots a_1 a_0 = \sum_{i=0}^{k} a_i 10^i$, *pensat a* $\mathbb{Z}/11$ *és*

$$\overline{n} = \cdots + \overline{10a_3} + \overline{a_2} + \overline{10a_1} + \overline{a_0}.$$

Equivalentment, la suma alternada de les xifres és múltiple de 11.
Exemple: Per mirar si 2542903 *és divisible per* 11 *fem* $03 + 29 + 54 + 2 = 88$, *que és clarament divisible per* 11.

Divisibilitat per 13. Un número escrit en base decimal és divisible per 13 si i només si les unitats per 9 ($9a_0$) restada de la xifra restant ($(n - a_0)/10$) és divisible per 13.
En efecte, observem primer que l'invers de $\overline{10}$ *a* $\mathbb{Z}/(13)$ *és* $\overline{4}$, *ja que*

$$\overline{10} \cdot \overline{4} = \overline{40} = \overline{1}.$$

Així, doncs, a $\mathbb{Z}/(13)$ *tenim*

$$\overline{\frac{n - a_0}{10} - 9a_0} = \overline{10^{-1}} \cdot \overline{n - a_0} - \overline{9a_0} = \overline{4}(\overline{n} - \overline{a_0}) - \overline{9a_0} = \overline{4n}.$$

Però $\overline{4n} = \overline{0}$ *si i només si* $4n$ *és divisible per* 13. *Com* 4 *i* 13 *són coprimers, això passa si i només si* n *és divisible per* 13.
Exemple: Per mirar si 70357 *és divisible per* 13 *fem* $7035 - 63 = 6972$. *Ara repetim el procés: fem* $697 - 18 = 679$. *Tornant a repetir, tenim,* $67 - 81 = -14$ *que ja veiem que no és divisible per* 13.

En canvi, 69120727 *sí que és divisible per* 13 *ja que* $6912072-63 = 6912009$*;* $691200-81 = 691119$*;* $69111-81 = 69030$*;* $6903-0 = 6903$*;* $690-27 = 663$*;* $66-27 = 39$*, que ja veiem que és múltiple de* 13.

Divisibilitat per 17. Un número escrit en base decimal és divisible per 17 si i només si les unitats per 5 ($5a_0$) restada de la xifra restant ($(n-a_0)/10$) és divisible per 17. *En efecte, observem primer que l'invers de* $\overline{10}$ *a* $\mathbb{Z}/(17)$ *és* $\overline{12}$*, ja que*

$$\overline{10}\cdot\overline{12} = \overline{120} = \overline{1}.$$

Així, doncs, a $\mathbb{Z}/(17)$ *tenim*

$$\overline{\frac{n-a_0}{10} - 5a_0} = \overline{10^{-1}}\cdot\overline{n-a_0} - \overline{5a_0} = \overline{12}(\overline{n}-\overline{a_0}) - \overline{5a_0} = \overline{12n}.$$

Però $\overline{12n} = \overline{0}$ *si i només si* $12n$ *és divisible per* 17*. Això passa si i només si* n *és divisible per* 17*.*

Divisibilitat per 19. Un número escrit en base decimal és divisible per 19 si i només si les unitats per 2 ($2a_0$) restades a la xifra restant ($(n-a_0)/10$) és divisible per 19.
En efecte, observem primer que l'invers de $\overline{10}$ *a* $\mathbb{Z}/(19)$ *és* $\overline{2}$*, ja que*

$$\overline{10}\cdot\overline{2} = \overline{12} = \overline{1}.$$

Així, doncs, a $\mathbb{Z}/(19)$ *tenim*

$$\overline{\frac{n-a_0}{10} - 2a_0} = \overline{10^{-1}}\cdot\overline{n-a_0} - \overline{2a_0} = \overline{2}(\overline{n}-\overline{a_0}) - \overline{2a_0} = \overline{2n}.$$

Però $\overline{2n} = \overline{0}$ *si i només si* $2n$ *és divisible per* 19*. Això passa si i només si* n *és divisible per* 19*.*

112. En una illa deserta–només habitada per un mono i molts cocoters–arriben cinc nàufregs; recullen tants cocos com poden i es posen a descansar. A mitja nit, un mariner desconfiat, temerós que els altres es despertin i es mengin algun coco, es lleva, fa cinc parts iguals del total de cocos, separa la seva part i deixa la resta; però li ha sobrat un coco que dóna al mono. Al cap d'una hora un segon mariner té la mateixa pensada: fa cinc parts iguals del total de cocos (dels que queden, és clar!), se'n guarda una part, deixa la resta i dóna al mono un coco que ha sobrat. Al cap d'una altra hora,.... Cada un dels cinc mariners fa la mateixa operació.
L'endemà al matí en llevar-se decideixen repartir els cocos (els del piló final) entre els cinc (cada un d'ells rient per sota el nas). Sobra un coco que el donen al mono. Pregunta: quants cocos havien collit? (The Saturday Evening Post, $\simeq$ 1925).

Solució: *Veurem que podem saber exactament la resposta només si sabem dir a simple vista la resposta amb un error d'uns* 15000 *cocos.*
Sigui x *= número total de cocos. Sigui* y_i *el número de cocos que hi ha a cadascuna de les piles iguals que fa el mariner* i*.*

Tenim el sistema següent:

$$\begin{aligned} x &= 5y_1 + 1 && (10.1)\\ 4y_1 &= 5y_2 + 1 && (10.2)\\ 4y_2 &= 5y_3 + 1 && (10.3)\\ 4y_3 &= 5y_4 + 1 && (10.4)\\ 4y_4 &= 5y_5 + 1 && (10.5)\\ 4y_5 &= 5\lambda + 1 && (10.6) \end{aligned}$$

Comencem a resoldre des de sota: La solució general de $4y_5 - 5\lambda = 1$ *és*

$$\begin{aligned} y_5 &= -1 + 5\alpha \\ \lambda &= -1 + 4\alpha. \end{aligned}$$

Substituïm y_5 *a la penúltima equació:*

$$4y_4 - 5(-1 + 5\alpha) = 4y_4 - 25\alpha + 5 = 1.$$

Resolem $4y_4 - 25\alpha = -4$. *Obtenim*

$$\begin{aligned} y_4 &= 24 + 25\beta \\ \alpha &= 4 + 4\beta. \end{aligned}$$

Substituïm y_4 *a l'equació anterior.*

$$4y_3 - 5(24 + 25\beta) = 4y_3 - 125\beta - 120 = 1.$$

Resolem $4y_3 - 125\beta = 121$. *Obtenim*

$$\begin{aligned} y_3 &= -1 + 125\gamma \\ \beta &= -1 + 4\gamma. \end{aligned}$$

Substituïm y_3 *a l'equació anterior.*

$$4y_2 - 5(-1 + 125\gamma) = 4y_2 - 625\gamma + 5 = 1.$$

Resolem $4y_2 - 625\gamma = -4$. *Obtenim*

$$\begin{aligned} y_2 &= 624 + 625\delta \\ \gamma &= 4 + 4\delta. \end{aligned}$$

Substituïm y_2 *a l'equació anterior.*

$$4y_1 - 5(624 + 625\delta) = 4y_1 - 3125\delta - 3120 = 1.$$

Resolem $4y_1 - 3125\delta = 3121$. *Obtenim*

$$\begin{aligned} y_1 &= -1 + 3125\tau \\ \gamma &= -1 + 4\tau. \end{aligned}$$

Per tant, $x = 5y_1 + 1 = 15625\tau - 4$.
El número possible més petit de cocos és 15621.
Observem que, per exemple, que 31246 *també funciona: En efecte, el primer mariner fa cinc parts de 6249 cocos. Es queda una part i dóna un coco al mico. En queden 24996.*
El segon mariner fa cinc parts de 4999 cocos. Es queda una part i dóna un coco al mico. En queden 19996.
El tercer mariner fa cinc parts de 3999 cocos. Es queda una part i dóna un coco al mico. En queden 15996.
El quart mariner fa cinc parts de 3199 cocos. Es queda una part i dóna un coco al mico. En queden 12796.
El cinquè mariner fa cinc parts de 2559 cocos. Es queda una part i dóna un coco al mico. En queden 10236.
No hem hagut de partir cap coco.

Llista 11

Enters primers i congruències

113. Proveu que si p és primer, aleshores $\sqrt{p} \notin \mathbb{Q}$. En general, per a quins $n \in \mathbb{Z}$ tindrem que $\sqrt{n} \in \mathbb{Q}$?

Solució: *És fàcil veure, copiant l'argument estàndard que s'utilitza per demostrar que* $\sqrt{2} \notin \mathbb{Q}$, *que* $\sqrt{n} \in \mathbb{Q}$ *si i només si* n *és quadrat perfecte, i.e. existeix* $m \in \mathbb{Z}$ *tal que* $n = m^2$.
Sigui

$$n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$$

la descomposició en factors primers de n. *Demostrarem que si* $\sqrt{n} \in \mathbb{Q}$ *totes les* α_i *són parells (i per tant* n *quadrat perfecte).*
Suposem que una de les α_i, *diguem-li* α_r, *és imparell. Suposem*

$$n = \frac{a^2}{b^2}, \quad \text{amb} \quad mcd(a, b) = 1.$$

Tindríem $a^2 = nb^2$, *la qual cosa implica que* p_r *apareix a la descomposició en factors primers de* a. *Per tant, apareix a l'esquerra d'aquesta igualtat elevat a un exponent parell. Com* a *i* b *són coprimers,* p_r *no apareix a la descomposició en factors primers de* b. *Per tant* p_r *apareix a la dreta d'aquesta igualtat elevat a un exponent imparell. Contradicció.*

114. Compteu quants divisors té 40. Feu el mateix per a 11475.

Solució: *És fàcil veure que*

$$n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$$

implica

$$\text{Número de divisors positius de } n = \Pi_{i=1}^{k}(1 + \alpha_i).$$

Com $40 = 2^3 \cdot 5$,

$$\text{Número de divisors positius de } 40 = (1 + 3)(1 + 1) = 8.$$

Concretament són $1, 2, 4, 5, 8, 10, 20, 40$.

Anàlogament, com $11475 = 3^3 \cdot 5^2 \cdot 17$,

$$\textit{Número de divisors positius de } 11475 = (1+3)(1+2)(1+1) = 24.$$

Concretament són

1	*3*	*5*	3^2	$3 \cdot 5$	*17*
5^2	3^3	$3^2 \cdot 5$	$3 \cdot 17$	$3 \cdot 5^2$	$17 \cdot 5$
$3^3 \cdot 5$	$3^2 \cdot 17$	$3^2 \cdot 5^2$	$3 \cdot 5 \cdot 17$	$17 \cdot 5^2$	$3^3 \cdot 17$
$3^3 \cdot 5^2$	$3^2 \cdot 17 \cdot 5$	$3 \cdot 5^2 \cdot 17$	$3^3 \cdot 17 \cdot 5$	$3^2 \cdot 17 \cdot 5^2$	$3^3 \cdot 5^2 \cdot 17$

115. Siguin a, b i m enters, $m > 1$. Posem $d = \text{mcd}(a, m)$.

1. Demostreu que l'equació diofàntica $ax - my = b$ té solució si i només si $d|b$. Dieu com són les solucions.
2. Demostreu que la congruència $ax \equiv b \pmod{m}$ té solució si i només si $d|b$. Demostreu que, en cas que tingui solucions, n'hi ha exactament d entre 0 i $m-1$ inclosos.
3. A $\mathbb{Z}/(m)$ considerem l'equació $\bar{a}\bar{x} = \bar{b}$. Demostreu que té solució si i només si $d|b$. Demostreu que en cas que tingui solució en té exactament d.

Apliqueu això per estudiar, en funció de m, l'equació diofàntica $6x - my = 4$, la congruència $6x \equiv 4 \pmod{m}$ i l'equació a $\mathbb{Z}/(m)$ $\bar{6}z = \bar{4}$.

Solució: *1) Suposem primer que té solució. Llavors, d divideix el primer terme de l'equació i per tant també el segon.*
Recíprocament, si d|b, podem posar b = dB, i per Bézout

$$b = (\alpha a + \beta m)B = a(\alpha B) + m(\beta B),$$

per tant $x = \alpha B$ *i* $y = -\beta B$, *és una solució.*
Qualsevol altre solució s'obté sumant a aquesta la solució general de l'equació homogènia (un cop simplificada):

$$\begin{aligned} x &= \alpha B + m'\lambda \\ y &= -\beta B + a'\lambda, \qquad \textit{per a tot } \lambda \in \mathbb{Z}. \end{aligned}$$

on $m = dm'$, $a = da'$, *amb* $mcd(a', b') = 1$.

2) La congruència $ax \equiv b \pmod{m}$ *té solució si i només si existeix* $y \in \mathbb{Z}$ *tal que*

$$ax - b = my.$$

És a dir, si i només l'equació diofàntica

$$ax - my = b,$$

té solució. Per 1) sabem que aquesta equació té solució si i només si d|b.

També sabem que la solució general és de la forma $x = x_0 + m'\lambda$
Sigui $x_1 = x_0 + m'\lambda_1$ *la primera solució positiva o zero. En particular,* $x_1 - m' < 0$.
Les successives d *solucions són*

$$x_1, x_1 + m', x_1 + 2m', \ldots, x_1 + (d-1)m'$$

i aquesta última compleix

$$x_1 + dm' - m' = x_1 + m - m' = (x_1 - m') + m < m.$$

Tenim doncs d *solucions entre* 0 *i* $m - 1$,

$$0 \leq x_1 \leq x_1 + m' \leq x_1 + 2m' \leq \cdots \leq x_1 + (d-1)m' \leq m - 1.$$

3) L'equació $\overline{ax} = \overline{b}$ *té solució si i només si existeix* $y \in \mathbb{Z}$ *tal que* $ax - b = my$, *és a dir, si i només si l'equació diofàntica* $ax - my = b$ *té solució. Estem doncs en el cas anterior 1).*
Ja hem vist a 2) que aquesta equació té, per x, *exactament* d *solucions a l'interval* $[0, m-1]$. *La primera l'hem denotat* x_1 *i hem vist que la darrera era* $x_1 + (d-1)m'$. *Si considerem la solució que vindria a continuació :*

$$[x_1 + (d-1)m'] + m' = x_1 + dm' = x_1 + m$$

veiem que pertany a la mateixa classe d'equivalència mòdul m *que* x_1, *és a dir, a* $\mathbb{Z}/(m)$ *tenim*

$$\overline{x_1} = \overline{x_1 + m}.$$

El mateix passa amb totes les solucions, és a dir, les solucions $x_1 + jm'$ *i la que tenim* d *llocs més endavant,* $x_1 + jm' + dm'$, *donen lloc a la mateixa classe a* $\mathbb{Z}/(m)$.

1a) Estudiem l'equació $6x - my = 4$. *Sigui* $d = mcd(6, m)$. *Tenim quatre casos* $d = 1, 2, 3, 6$.
Primer cas $d = 1$. *Té solució ja que* $1|4$. *Per resoldre-la trobem els coeficients de Bézout de* 6 *i* m. *Suposem* $6\alpha + m\beta = 1$. *Llavors la solució general és*

$$\begin{aligned} x &= 4\alpha + m\lambda \\ y &= -4\beta + 6\lambda, \qquad \text{per a tot } \lambda \in \mathbb{Z}. \end{aligned}$$

Segon cas $d = 2$. *Té solució ja que* $2|4$. *Per resoldre-la primer dividim per* 2 *i tenim*

$$3x - m'y = 2$$

amb $m = 2m'$. *Trobem ara els coeficients de Bézout de* 3 *i* m'. *Suposem* $3\alpha + m'\beta = 1$. *Llavors la solució general és*

$$\begin{aligned} x &= 2\alpha + m'\lambda \\ y &= -2\beta + 3\lambda, \qquad \text{per a tot } \lambda \in \mathbb{Z}. \end{aligned}$$

Tercer cas $d = 3$. *No té solució ja que* $3 \not| 4$.
Quart cas $d = 6$. *No té solució ja que* $6 \not| 4$.

2a) Volem resoldre $6x \equiv 4 \pmod{m}$.

Només hem d'estudiar el casos $d = 1$ i $d = 2$.
$d = 1$. Sabem $x = 4\alpha + m\lambda$. Comprovem que hi ha una única solució (justament perquè $d = 1$) a l'interval $[0, m-1]$ Això és evident ja que la diferència entre dues solucions consecutives és m i aquest interval conté m enters.
$d = 2$. Sabem $x = 2\alpha + m'\lambda$ amb $m = 2m'$. Comprovem que hi ha dues solucions (justament perquè $d = 2$) a l'interval $[0, m-1]$ Això és evident ja que la diferència entre dues solucions consecutives és $m' = m/2$ i aquest interval conté m enters.

3a) Volem resoldre $\overline{6}z = \overline{4}$ a $\mathbb{Z}/(m)$.
Només hem d'estudiar el casos $d = 1$ i $d = 2$.

$d = 1$. Sabem $x = 4\alpha + m\lambda$ és solució de $6x - my = 4$. A $\mathbb{Z}/(m)$ ens dóna directament $\overline{6}\overline{x} = \overline{4}$. Per tant, $\overline{x} = \overline{4}\overline{\alpha}$ és la solució buscada. Però com que també teníem $6\alpha + m\beta = 1$, això vol dir que $\overline{\alpha} = \overline{6}^{-1}$. Si coneguéssim m podríem calcular explícitament aquest invers de $\overline{6}$.
Així doncs $z = \overline{4} \cdot \overline{6}^{-1}$.

$d = 2$. Sabem $x = 2\alpha + m'\lambda$ amb $m = 2m'$ és solució de $6x - my = 4$. Prenent classes a $Z/(m)$ a les dues equacions tenim que la incògnita z buscada és $z = \overline{x} = \overline{2}\overline{\alpha}$ si λ és parell, o bé $z = \overline{x} = \overline{2}\overline{\alpha} + m'$ si λ és senar.

116. Resoleu les següents congruències:

(a) $8x \equiv 5 \pmod{15}$ (b) $15x \equiv 9 \pmod{21}$ (c) $9x \equiv 7 \pmod{33}$

Solució: *(a) Resolem l'equació diofàntica $8x - 15y = 5$. Té solució, ja que $mcd(8, 15) = 1$. Els coeficients de Bézout de 8 i 15 són 2 i -1 ja que*

$$8 \cdot (2) + 15 \cdot (-1) = 1.$$

Per tant, la solució general és

$$\begin{aligned} x &= 2 \cdot 5 + 15\lambda \\ y &= 1 \cdot 5 + 8\lambda, \qquad \text{per a tot } \lambda \in \mathbb{Z}. \end{aligned}$$

De fet, només ens demanen el valor de $x = 10 + 15\lambda$. Equivalentment, la resposta és que x és qualsevol enter congruent amb 10, mòdul 15.
Podem també considerar la igualtat $\overline{8}\overline{x} = \overline{5}$ a $\mathbb{Z}/(15)$. Com que l'invers de $\overline{8}$ a $\mathbb{Z}/(15)$ és $\overline{2}$ tenim

$$\overline{x} = \overline{25} = \overline{10}.$$

És a dir, la classe de x és la classe del 10 a $\mathbb{Z}/(15)$, com ja sabíem.

117. Sigui K un cos i $f(x) = ax^2 + bx + c \in K[x]$, amb $a \neq 0$. Demostreu que α és arrel de $f(x)$, és a dir $f(\alpha) = 0$, si i només si

$$\alpha = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}.$$

Així doncs, quina condició han de complir a, b, c per tal de que $f(x)$ tingui alguna arrel? Trobeu les arrels de $x^2 + 4x + 1 \in \mathbb{Z}/(11)[x]$.

Solució: *Completació de quadrats:*

$$ax^2 + bx + c = a(x + \frac{b}{2a})^2 - \frac{b^2}{4a} + c = 0$$

Per tant

$$a(x + \frac{b}{2a})^2 = \frac{b^2 - 4ac}{4a},$$

$$x + \frac{b}{2a} = \frac{\sqrt{b^2 - 4ac}}{2a}.$$

$$x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$$

Vegeu el problema 118.
Per resoldre $x^2 + 4x + 1 = 0$ a $\mathbb{Z}/(11)[x]$, apliquem la fórmula

$$x = \frac{-4 \pm \sqrt{12}}{2} = \frac{7 \pm \sqrt{1}}{2}.$$

Com $\mathbb{Z}/(11)$ és un cos $\sqrt{1} = \pm 1$. Així doncs, com l'invers de 2 a $\mathbb{Z}/(11)$ és 6, tenim $x = \frac{7+1}{2} = 8 \cdot 6 = 4$; o bé $x = \frac{7-1}{2} = 6 \cdot 6 = 3$.

118. a) Trobeu[1] les solucions de l'equació $6x \equiv 14$ (16), i de l'equació de segon grau $x^2 - 3x - 3 \equiv 0$ (7).
b) Estudieu, en general, la resolució de $ax \equiv b$ (m), $ax^2 + bx + c \equiv 0$ (p) amb p primer.

Solució: *a) La primera congruència la deixem com exercici. Per resoldre la congruència relativa a l'equació de segon grau el que farem és resoldre la igualtat $x^2 - 3x - 3 = 0$ a $\mathbb{Z}/(7)$. Apliquem la fórmula general*

$$x = \frac{3 \pm \sqrt{9 + 12}}{2} = \frac{3 \pm \sqrt{21}}{2} = \frac{3}{2} = 2^{-1} \cdot 3 = 4 \cdot 3 = 12 = 5.$$

Resumint, tot x de la forma $x = 5 + 7\lambda$, per a alguna $\lambda \in \mathbb{Z}$, és solució de la congruència donada.

b) Per a la primera part vegeu el problema 115. En quant a l'equació de segon grau ja hem comentat que la fórmula

$$x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$$

és vàlida, ben entès que l'arrel quadrada i la divisió s'ha d'efectuar a $\mathbb{Z}/(p)$.
Suposarem $mcd(a, p) = 1$, ja que si a fos múltiple de p, aquesta equació no seria de segon grau a $\mathbb{Z}/(p)$.

[1] La resta d'exercicis d'aquest llista són del llibre *Àlgebra Lineal i Geometria*, de M. Castellet, I. Llerena.

Com p és primer $\mathbb{Z}/(p)$ és un cos, i per tant té sentit dividir per $2a$ (si $p \neq 2$). Si $p = 2$, veiem que $x = 0$ és solució si i només si $c = 0 \in \mathbb{Z}/(2)$, i que $x = 1$ és solució si i només si $a + b + c = 0 \in \mathbb{Z}/(2)$. Però no tots els elements de $\mathbb{Z}/(p)$ tenen arrel quadrada, de manera que pot ser que $b^2 - 4ac$ no tingui arrel quadrada i, per tant, l'equació no tingui solució.
Per exemple $x^2 = 3$ a $\mathbb{Z}/(5)$. Els elements de $\mathbb{Z}/(5)$ elevats al quadrat són $0^2 = 0, 1^2 = 1, 2^2 = 4, 3^2 = 4, 4^2 = 1$. Per tant, no hi cap element que elevat al quadrat doni 3. Equivalentment, no hi ha cap nombre enter que elevat al quadrat sigui congruent amb 3 mòdul 5.
Donar un criteri general en funció de a, b, c, p per saber si $b^2 - 4ac$ té arrel quadrada a $\mathbb{Z}/(p)$ sembla difícil[2].

119. Resoleu les següents equacions als anells indicats:

$$(a)\ x^2 - 3x - 3 = 0,\ \text{a } \mathbb{Z}/(7); \quad (b)\ x^2 - 1 = 0,\ \text{a } \mathbb{Z}/(35); \quad (c)\ x^6 + x^3 - x^2 + x + 1 = 0,\ \text{a } \mathbb{Z}/(3)\,.$$

Solució: *(a) Apliquem la fórmula de l'equació de segon grau posant cura al càlcul de l'arrel quadrada i la divisió en l'anell $\mathbb{Z}/(7)$.*

$$x = \frac{3 \pm \sqrt{3^2 + 4 \cdot 3}}{2} = \frac{3 \pm \sqrt{21}}{2} = \frac{3}{2}$$

ja que 21 és 0 a $\mathbb{Z}/(7)$. Observem que l'invers de 2 a $\mathbb{Z}/(7)$ és 4. Per tant

$$x = \frac{3}{2} = 3 \cdot 4 = 5.$$

(b) Utilitzarem que hi ha un isomorfisme entre $\mathbb{Z}/(35)$ i el producte cartesià $\mathbb{Z}/(5) \times \mathbb{Z}/(7)$. La gran diferència és que $\mathbb{Z}/(35)$ no és cos i en canvi $\mathbb{Z}/(5)$ i $\mathbb{Z}/(7)$ sí que ho són.
L'isomorfisme funciona així

$$\begin{array}{rccc} \Phi : \mathbb{Z}/(35) & \longrightarrow & \mathbb{Z}/(5) \times \mathbb{Z}/(7) \\ \overline{x} & \mapsto & (\overline{x} \quad , \quad \overline{x}) \end{array}$$

Ben definit. *Si canviem a l'esquerra x per $x + 35$, les dues classes de la dreta, denotades igual però computades primer a $\mathbb{Z}/(5)$ i després a $\mathbb{Z}/(7)$, no queden afectades ja que 35 és múltiple de 5 i de 7.*
Injectiu. *Suposem $\Phi(\overline{x}) = \Phi(\overline{y})$. Això vol dir $\overline{x} = \overline{y}$ a $\mathbb{Z}/(5)$ i $\overline{x} = \overline{y}$ a $\mathbb{Z}/(7)$. És a dir, existeixen λ i μ tals que*

$$\begin{aligned} x - y &= 5\lambda \\ x - y &= 7\mu \end{aligned}$$

Però la igualtat $5\lambda = 7\mu$ implica $\mu = 5 \cdot \mu'$. De manera que $x - y = 7\mu = 35\mu'$, i.e. $\overline{x} = \overline{y}$ a $\mathbb{Z}/(35)$.

[2] $x \in \mathbb{Z}/(p)$ té arrel quadrada si i només si $x^{(p-1)/2} = 1$ (comentari de Jaume de Dios).

Exhaustiu. *Donat* $\overline{a} \in \mathbb{Z}/(5)$ *i* $\overline{b} \in \mathbb{Z}/(7)$ *busquem* $\overline{x} \in \mathbb{Z}/(35)$ *tal que* $\overline{x} = \overline{a}$ *a* $\mathbb{Z}/(5)$ *i* $\overline{x} = \overline{b}$ *a* $\mathbb{Z}/(7)$.
Equivalentment, busquem $x \in \mathbb{Z}$ *tal que* $x - a = 5\lambda$, *per a una certa* $\lambda \in \mathbb{Z}$ *i, al mateix temps,* $x - b = 7\mu$, *per a una certa* $\mu \in \mathbb{Z}$. *Observem que si trobem una tal* x *llavors* $x + \dot{35}$ *també compleix aquestes equacions (per a altres valors de* λ *i* μ*), i recíprocament, si* $z \in \mathbb{Z}$ *compleix aquestes dues equacions llavors* $z - x = \dot{35}$.
Hem de trobar, doncs, λ *i* μ *tals que* $a + 5\lambda = b + 7\mu$. *Estudiem doncs l'equació diofàntica*

$$5\lambda - 7\mu = b - a.$$

Com $mcd(5, 7) = 1$ *aquesta equació té solució. Si* (λ_0, μ_0) *és una solució, llavors* $x = a + 5\lambda_0 = b + \mu_0$ *és el nombre enter buscat. Concretament, aquest* x *compleix* $\Phi(\overline{x}) = (\overline{a}, \overline{b})$.
Morfisme. *Es compleix* $\Phi(\overline{x} \cdot \overline{y}) = \Phi(\overline{x}) \cdot \Phi(\overline{y})$. *Ho deixem com exercici.*
Tornem al problema inicial: resoldre la congruència $x^2 \equiv 1 \pmod{35}$. *Equivalentment, resoldre l'equació* $\overline{x}^2 = \overline{1}$ *a* $\mathbb{Z}/(35)$. *Apliquem* Φ *als dos costats d'aquesta igualtat i, per ser* Φ *morfisme, tenim*

$$\Phi(\overline{x}^2) = (\Phi(\overline{x}))^2 = \Phi(\overline{1}).$$

Equivalentment, a $\mathbb{Z}/(5) \times \mathbb{Z}/(7)$,

$$(\overline{x}, \overline{x})^2 = (\overline{1}, \overline{1}).$$

Hem de resoldre doncs les dues equacions

$$\begin{aligned} \overline{x}^2 &= \overline{1}, \quad \text{a } \mathbb{Z}/(5) \\ \overline{x}^2 &= \overline{1}, \quad \text{a } \mathbb{Z}/(7) \end{aligned}$$

Com son cossos ha de ser $x = \pm 1$ *en ambdós casos. És a dir, el nombre* $x \in \mathbb{Z}$ *que estem buscant ha de ser tal que la seva classe a* $\mathbb{Z}/(5)$ *sigui* $\overline{1}$ *o* $\overline{4}$ *(recordem que* $4 = -1$ *a* $\mathbb{Z}/(5)$*), i que la seva classe a* $\mathbb{Z}/(7)$ *sigui* $\overline{1}$ *o* $\overline{6}$ *(recordem que* $6 = -1$ *a* $\mathbb{Z}/(7)$*).*
Les parelles $(1, 1), (4, 1), (1, 6), (4, 6) \in \mathbb{Z}/(5) \times \mathbb{Z}/(7)$ *compleixen que*

$$(1, 1)^2 = (4, 1)^2 = (1, 6)^2 = (4, 6)^2 = 1.$$

Si resolem les equacions

$$\begin{aligned} \Phi(\overline{x}) &= (1, 1) \\ \Phi(\overline{x}) &= (4, 1) \\ \Phi(\overline{x}) &= (1, 6) \\ \Phi(\overline{x}) &= (4, 6) \end{aligned}$$

tindrem quatre valors diferents de $\overline{x} \in \mathbb{Z}/(35)$ *que compliran* $\overline{x}^2 = \overline{1} \in \mathbb{Z}/(35)$.
Resoldrem les dues primeres equacions, que en realitat són dos sistemes de dues equacions amb dues incògnites, directament i les altres dues equacions usant el teorema dels restos xinesos (ACM, p.187); d'aquesta manera veurem dues maneres de procedir, la primera té l'avantatge de que no has de recordar cap fórmula, i la segona és més ràpida però has de saber la fórmula.

Primer sistema.

$$\begin{aligned} x &\equiv 1 \pmod 5 \\ x &\equiv 1 \pmod 7 \end{aligned}$$

Resolem l'equació diofàntica $x - 5y = 1$. *Solució general*

$$\begin{aligned} x &= 6 + 5\lambda \\ y &= 1 + \lambda, \qquad \textit{per a tot } \lambda \in \mathbb{Z}. \end{aligned}$$

Ara posem el valor de x *a la segona equació*

$$x - 7z = 6 + 5\lambda - 7z = 1$$

i resolem l'equació diofàntica

$$5\lambda - 7z = -5.$$

Solució general

$$\begin{aligned} \lambda &= 6 + 7\mu \\ z &= 5 + 5\mu, \qquad \textit{per a tot } \mu \in \mathbb{Z}. \end{aligned}$$

Per tant,

$$x = 6 + 5\lambda = 6 + 5(6 + 7\mu) = 36 + 35\mu,$$

és a dir $\overline{x} = \overline{1} \in \mathbb{Z}/(35)$.
Segon sistema.

$$\begin{aligned} x &\equiv 4 \pmod 5 \\ x &\equiv 1 \pmod 7 \end{aligned}$$

Resolem l'equació diofàntica $x - 5y = 4$. *Solució general*

$$\begin{aligned} x &= 9 + 5\lambda \\ y &= 1 + \lambda, \qquad \textit{per a tot } \lambda \in \mathbb{Z}. \end{aligned}$$

Ara posem el valor de x *a la segona equació*

$$x - 7z = 9 + 5\lambda - 7z = 1$$

i resolem l'equació diofàntica

$$5\lambda - 7z = -8.$$

Solució general

$$\begin{aligned} \lambda &= 4 + 7\mu \\ z &= 4 + 5\mu, \qquad \textit{per a tot } \mu \in \mathbb{Z}. \end{aligned}$$

Per tant,

$$x = 9 + 5\lambda = 9 + 5(4 + 7\mu) = 29 + 35\mu,$$

és a dir $\overline{x} = \overline{29} \in \mathbb{Z}/(35)$.
Tercer sistema.

$$\begin{aligned} x &\equiv 1 \pmod 5 \\ x &\equiv 6 \pmod 7 \end{aligned}$$

La tècnica xinesa per resoldre el sistema $x \equiv a_i \pmod{m_i}$, *amb els* m_i *coprimers, consisteix en resoldre les equacions independents*

$$M_i y_i \equiv a_i \pmod{m_i}, \qquad M_i = M/m_i, \quad \textit{on} \quad M = m_1 \cdot \cdots \cdot m_k.$$

Un cop trobats aquests y_i, *la solució general és*

$$x = \sum M_i y_i + M\lambda, \quad \textit{per a tot } \lambda \in \mathbb{Z}.$$

En el nostre cas doncs $M_1 = 7$, $M_2 = 5$, *i les equacions són*

$$\begin{aligned} 7y_1 &\equiv 1 \pmod 5 \\ 5y_2 &\equiv 6 \pmod 7 \end{aligned}$$

Obtenim $y_1 = -2 + 5\lambda$, *per tot* $\lambda \in \mathbb{Z}$, *i* $y_2 = 4 + 7\mu$, *per a tot* $\mu \in \mathbb{Z}$.
La solució buscada és doncs $M_1y_1 + M_2y_2 = 7(-2 + 5\lambda) + 5(4 + 7\mu) = 6 + \dot{35}$. *És a dir,* $\overline{x} = \overline{6} \in \mathbb{Z}/(35)$.
Quart sistema.

$$\begin{aligned} x &\equiv 4 \pmod 5 \\ x &\equiv 6 \pmod 7 \end{aligned}$$

En aquest cas també $M_1 = 7$, $M_2 = 5$, *i les equacions són*

$$\begin{aligned} 7y_1 &\equiv 4 \pmod 5 \\ 5y_2 &\equiv 6 \pmod 7 \end{aligned}$$

Obtenim $y_1 = 2 + 5\lambda$, *per tot* $\lambda \in \mathbb{Z}$, *i* $y_2 = 4 + 7\mu$, *per a tot* $\mu \in \mathbb{Z}$.
La solució buscada és doncs $M_1y_1 + M_2y_2 = 7(2 + 5\lambda) + 5(4 + 7\mu) = 34 + \dot{35}$. *És a dir,* $\overline{x} = \overline{34} \in \mathbb{Z}/(35)$.
Resumint, a $\mathbb{Z}/(35)$, *els quatre elements* $\overline{1}, \overline{6}, \overline{29}, \overline{34}$ *són solucions de l'equació* $x^2 = 1$.

(c) Com que $\mathbb{Z}/(3)$ *només té tres elements és més còmode procedir directament a comprovar un per un si compleixen l'equació.*

$$x^6 + x^3 - x^2 + x + 1 = \begin{cases} 0^6 + 0^3 - 0^2 + 0 + 1 &= 1, \\ 1^6 + 1^3 - 1^2 + 1 + 1 &= 0, \\ 2^6 + 2^3 - 2^2 + 2 + 1 &= 2. \end{cases}$$

Així la solució (única) és $x = 1$.

120. Resoleu el sistema de congruències:

$$\left.\begin{array}{rl} x \equiv 11 & (\mathrm{mod}\ 12) \\ x \equiv 1 & (\mathrm{mod}\ 10) \\ x \equiv 2 & (\mathrm{mod}\ 7) \end{array}\right\}$$

Solució: *Usarem el resultat següent, de demostració immediata, i que és un cas particular del teorema dels restos xinesos.*

Lema. *Siguin* m_1 *i* m_2 *coprimers. Llavors*

$$x \equiv a \pmod{m_1 \cdot m_2} \Longleftrightarrow \left\{\begin{array}{ll} x \equiv a & (\mathrm{mod}\ m_1), \\ x \equiv a & (\mathrm{mod}\ m_2). \end{array}\right.$$

Aplicant aquest lema a $x \equiv 11 \pmod{12}$, *i a* $x \equiv 1 \pmod{10}$, *el sistema que hem de resoldre és*

$$\left.\begin{array}{rl} x \equiv 11 & (mod\ 3) \\ x \equiv 11 & (mod\ 4) \\ x \equiv 1 & (mod\ 2) \\ x \equiv 1 & (mod\ 5) \\ x \equiv 2 & (mod\ 7) \end{array}\right\}$$

Ara bé, l'equació $x \equiv 1 \pmod{2}$, *es pot treure ja que tota solució de* $x \equiv 11 \pmod{4}$ *és imparell i, per tant, compleix* $x \equiv 1 \pmod{2}$.
Ara el nostre sistema s'ha reduït a

$$\left.\begin{array}{rl} x \equiv 11 & (mod\ 3) \\ x \equiv 11 & (mod\ 4) \\ x \equiv 1 & (mod\ 5) \\ x \equiv 2 & (mod\ 7) \end{array}\right\}$$

i a aquest sistema ja se li pot aplicar el mètode xinès dels restes, ja que $3, 4, 5, 7$ *són coprimers. Preparem els càlculs:*

$$\begin{aligned} M_1 &= 4 \cdot 5 \cdot 7 = 140 \\ M_2 &= 3 \cdot 5 \cdot 7 = 105 \\ M_3 &= 3 \cdot 4 \cdot 7 = 84 \\ M_4 &= 3 \cdot 4 \cdot 5 = 60 \end{aligned}$$

Les equacions independents que hem de resoldre són

$$\left.\begin{array}{rl} 140y_1 \equiv 11 & (mod\ 3) \\ 105y_2 \equiv 11 & (mod\ 4) \\ 84y_3 \equiv 1 & (mod\ 5) \\ 60y_4 \equiv 2 & (mod\ 7) \end{array}\right\}$$

Prenent classes tenim

$$\left.\begin{array}{ll} \mathbb{Z}/(3); & \overline{2y_1} = \overline{2} \\ \mathbb{Z}/(4); & \overline{y_2} = 3 \\ \mathbb{Z}/(5); & \overline{4y_3} = \overline{1} \\ \mathbb{Z}/(7); & \overline{4y_4} = \overline{2} \end{array}\right\}$$

Obtenim directament

$$\left.\begin{array}{ll} \mathbb{Z}/(3); & \overline{y_1} = \overline{1} \\ \mathbb{Z}/(4); & \overline{y_2} = \overline{3} \\ \mathbb{Z}/(5); & \overline{y_3} = \overline{4} \\ \mathbb{Z}/(7); & \overline{y_4} = \overline{4} \end{array}\right\}$$

La solució és doncs

$$\sum M_i y_i + 420\lambda = 140 \cdot 1 + 105 \cdot 3 + 84 \cdot 4 + 60 \cdot 4 + 420\lambda = 1031 + 420\lambda.$$

Observeu que no depèn de quin representant de les classes $\overline{y_i}$ s'elegeix.
Si no coneixem el xinès.
Podem resoldre aquest problema simplement anant resolent les congruències ordenadament.
Resolem primer $x \equiv 11 \pmod{12}$. *Equival a resoldre l'equació diofàntica* $x - 12y = 11$. *Dóna* $x = 11 + 12\eta$.
Resolem ara $x \equiv 1 \pmod{10}$. *Equival a resoldre l'equació diofàntica* $x - 10z = 1$. *Dóna* $x = 11 + 10\mu$.
Per tant, ha de ser $11 + 12\eta = 11 + 10\mu$. *Resolem l'equació diofàntica* $6\eta - 5\mu = 0$. *Dóna* $\eta = 5\alpha$. *Així*

$$x = 11 + 12\eta = 11 + 12(5\alpha) = 11 + 60\alpha$$

La tercera equació diu que $x - 2$ *és múltiple de* 7, *és a dir, hem de resoldre l'equació diofàntica* $11 + 60\alpha - 7t = 2$, *equivalentment*

$$60\alpha - 7t = -9.$$

Obtenim $\alpha = -18 + 7\nu$.
Així

$$x = 11 + 60(-18 + 7\nu) = -1069 + 420\nu$$

que coincideix amb la solució obtinguda prèviament, ja que si posem $\nu = \lambda + 5$ *tenim*

$$x = -1069 + 420\nu = 1031 + 420\lambda.$$

121. Considereu $x = 2010^{2010}$. Sigui a la suma de les xifres de x i b la suma de les xifres de a. Podeu dir quant és exactament la suma de les xifres de b?

Solució: *Recordem que la classe a* $\mathbb{Z}/(9)$ *d'un nombre enter és igual a la classe de la suma dels seus dígits.*
Considerem la classe de $x = 2010^{2010}$ *a* $\mathbb{Z}/(9)$. *Com* $\overline{2010} = \overline{3}$ *i* $\overline{3}^2 = \overline{0}$, *tenim que*

$$\overline{x} = \overline{3}^{2010} = \overline{0}.$$

Equivalentment, la suma de les xifres de x, que hem denotat a, és múltiple de 9. Com $\overline{a} = \overline{0} \in \mathbb{Z}/(9)$, la suma de les xifres de a, que hem denotat b, és múltiple de 9.
Ara bé, $2010^{2010} < (10000)^{10000} = 10^{40000}$. Això ens diu que $a < 9 \cdot 40000 = 360000$ ja que x té, en base decimal, menys de 40000 dígits que poden ser cadascun d'ells coma molt 9. I això vol dir que $b < 6 \cdot 9 = 54$. Això vol dir que els possibles valors de b són $9, 18, 27, 36, 45$. En particular, la suma de les seves xifres és 9.

122. (Teorema xinés de la resta) Demostreu que si $(m, n) = 1$ les equacions $x \equiv a$ (m) i $x \equiv b$ (n) tenen una única solució mòdul mn.

Solució: *Vegeu problema 119, apartat b). L'existència de solució és la exhaustivitat de Φ i la unicitat la injectivitat.*

123. Determineu els $a \in \mathbb{Z}/(8)$ tals que el sistema $7x + 5y = 2$, $5x + ay = 16$ té solució a $Z/(8)$.

Solució: *De la primera equació deduïm $x = 6 - 3y$ (recordem que l'invers de 7 a $\mathbb{Z}/(8)$ és 7). Substituint a la segona obtenim $5(6 - 3y) + ay = 16$, és a dir, $(a - 15)y = -24$, que com que estem a $\mathbb{Z}/(8)$ s'escriu com $(a - 7)y = 2$. Si $(a - 7)$ és invertible, tenim solució única donada per $y = 2 \cdot (a - 7)^{-1}$. Hem de mirar doncs si $a - 7$ és invertible o no a $\mathbb{Z}/(8)$.*

$$
\begin{array}{lll}
a = 0; & \text{l'invers de } 0 - 7 = 1 \text{ és } 1; & y = 2, x = 0 \\
a = 1; & 1 - 7 = -6 = 2 \text{ no és invertible.} & \\
a = 2; & \text{l'invers de } 2 - 7 = -5 = 3 \text{ és } 3; & y = 6, x = 4 \\
a = 3; & 3 - 7 = -4 = 4 \text{ no és invertible.} & \\
a = 4; & \text{l'invers de } 4 - 7 = -3 = 5 \text{ és } 5; & y = 2, x = 0 \\
a = 5; & 5 - 7 = -2 = 6 \text{ no és invertible.} & \\
a = 6; & \text{l'invers de } 6 - 7 = -1 = 7 \text{ és } 7; & y = 6, x = 4 \\
a = 7; & 7 - 7 = 0 \text{ no és invertible.} &
\end{array}
$$

Resumint, si a és imparell, $a - 7$ és parell, que no és invertible a $\mathbb{Z}/(8)$. Si a és parell, $a - 7$ és imparell i tots els imparells són invertibles i coincideixen amb els seus inversos: $1 \cdot 1 = 3 \cdot 3 = 5 \cdot 5 = 7 \cdot 7 = 1$ a $\mathbb{Z}/(8)$. Així, per a $a = 0, 2, 4, 6$, el sistema donat té solució única.
Però l'equació $(a - 7)y = 2$ pot tenir solució encara que $(a - 7)$ no sigui invertible. Els casos que ens queden pendents són els següents.

a=1. *L'equació és $2y = 2$ admet la solució $y = 1$ (en aquest cas $x = 3$) i la solució $y = 5$ (en aquest cas $x = 7$). Per veure això es poden donar tots els valors possibles a $y \in \mathbb{Z}/(8)$ o es pot resoldre la diofàntica corresponent.*

a=3. *L'equació és $4y = 2$ no té solució.*

a=5. *L'equació és $6y = 2$ admet la solució $y = 3$ (en aquest cas $x = 5$) i la solució $y = 6$ (en aquest cas $x = 4$).*

a=7. *L'equació és $0y = 2$ que no té solució.*

Notem que si haguéssim aplicat la regla de Cramer, només haguéssim obtingut que per a $a = 7$ el sistema és incompatible, ja que el determinant del sistema val $7a - 1$, i el rang de la matriu ampliada val 2.

124. a) Demostreu que si $(a, n) = 1$ o $(b, n) = 1$ l'equació $ax + by = c$ té exactament n solucions a $\mathbb{Z}/(n) \times \mathbb{Z}/(n)$.
b) Trobeu les solucions de $3x + 4y = 1$, a $\mathbb{Z}/(7)$, i de $3x + 7y = 2$, a $\mathbb{Z}/(8)$.

Solució: *a) A $\mathbb{Z}/(n)$, a o b són invertibles. Si a és invertible*

$$x = a^{-1}(c - by).$$

Per a cada $y \in \mathbb{Z}/(n)$, simplement substituint el seu valor a l'anterior equació, tenim una solució $(x, y) \in \mathbb{Z}/(n) \times \mathbb{Z}/(n)$.
Si l'invertible és b, tenim

$$y = b^{-1}(c - ax)$$

i, com abans, per a cada valor de x tenim el coresponent valor de y.

b) Primera equació. *Com $(3, 7) = (4, 7) = 1$, estem en les hipòtesis de l'apartat a) i per tant la solucions són*

$$x = 3^{-1}(1 - 4y) = 5(1 - 4y) = 5 - 6y.$$

Donem a y els valors $0, 1, \ldots, 6$ i obtenim els corresponents 7 valors de x. Les parelles (x, y) són: $(5, 0), (6, 1), (0, 2), (1, 3), (2, 4), (3, 5), (4, 6)$.

Segona equació. *Com $(3, 8) = (7, 8) = 1$, estem en les hipòtesis de l'apartat a) i per tant la solucions són*

$$x = 3^{-1}(2 - 7y) = 3(2 - 7y) = 6 - 5y.$$

Donem a y els valors $0, 1, \ldots, 7$ i obtenim els corresponents 7 valors de x. Les parelles (x, y) són: $(6, 0), (1, 1), (4, 2), (7, 3), (2, 4), (5, 5), (0, 6), (3, 7)$

Llista 12

Polinomis

125. Trobeu tots els divisors de $3x^2+3$ a $\mathbb{C}[x]$, $\mathbb{R}[x]$ i $\mathbb{Z}/(5)[x]$.

Solució: *Tot està en trobar les arrels de* $x^2+1=0$ *en els tres cossos* $\mathbb{C},\mathbb{R},\mathbb{Z}/(5)$. *Sobre* $\mathbb{C}[x]$ *tenim* $3x^2+3=3(x+i)(x-i)$. *Sobre* $\mathbb{R}[x]$, *tenim* $3x^2+3=3(x^2+1)$. *Sobre* $\mathbb{Z}/(5)$ *tenim* $3x^2+3=3(x-2)(x-3)$, *ja que les arrels de* x^2+1 *són* 2 *i* 3. *Observem que* $3(x-2)(x-3)=3(x^2-5x+6)=3(x^2+1)$ *ja que* $-5x=0$ *i* $6=1$ *a* $\mathbb{Z}/(5)$. *També les podem trobar posant* $x=\sqrt{-1}=\sqrt{4}=\pm 2=2,-3$.

126. Trobeu per a quins primers positius p el polinomi $x^2+\overline{3}x+\overline{1}$ divideix a $x^5+\overline{4}x^4-x+\overline{5}$ a l'anell $\mathbb{Z}/(p)[x]$.

Solució:

$$\begin{array}{l|l} x^5+4x^4-x+5 & |x^2+3x+1 \\ \hline -x^5-3x^4-x^3 & x^3+x^2-4x+11 \\ \hline x^4-x^3-x+5 & \\ -x^4-3x^3-x^2 & \\ \hline -4x^3-x^2-x+5 & \\ 4x^3+12x^2+4x & \\ \hline 11x^2+3x+5 & \\ -11x^2-33x-11 & \\ \hline -30x-6 & \end{array}$$

Per tant, per que x^2+3x+1 *divideixi a* x^5+4x^4-x+5 *ha de ser* $30=0$ *i* $6=0$ *a* $\mathbb{Z}/(p)$. *Això només passa a la vegada si* $p=2$, *o* $p=3$, *ja que* 2 *i* 3 *són els únics divisors comuns a* 30 *i* 6.

127. Trobeu el màxim comú divisor i una identitat de Bézout pels següents parells de polinomis

$$\begin{array}{lllll} a) & P(x) = x^4+2x+3, & Q(x)=3x^2+x, & \text{a } \mathbb{Z}/(7)[x]. \\ b) & P(x) = x^4-i, & Q(x)=x^3-i, & \text{a } \mathbb{C}[x]. \\ c) & P(x) = x^3+2x+1, & Q(x)=x^2+1, & \text{a } \mathbb{Z}/(5)[x]. \end{array}$$

Solució: *a) Fem la divisió euclidiana a* $\mathbb{Z}/(7)[x]$ *de* x^4+2x+3 *entre* $3x^2+x$.

$$\begin{array}{r|l} x^4+2x+3 & 3x^2+x \\ \cline{2-2} -x^4-5x^3 & 5x^2+3x+6 \\ \cline{1-1} 2x^3+2x+3 & \\ -2x^3-3x^2 & \\ \cline{1-1} 4x^2+2x+3 & \\ -4x^2-6x & \\ \cline{1-1} -4x+3 & \end{array}$$

I organitzem els càlculs com sempre

	$5x^2+3x+6$	$x+4$	
x^4+2x+3	$3x^2+x$	$3x+3$	*2*
1	*0*	*1*	$6x+3$
0	*1*	$-(5x^2+3x+6)$	$5x^3+2x^2+4x+4$

Això vol dir que els polinomis són coprimers (el seu màxim comú divisor és una constant), i

$$(3x^2+x)\cdot(5x^3+2x^2+4x+4)+(x^4+2x+3)(6x+3)=2.$$

És a dir, els coeficients de Bézout, determinats llevat d'escalars, són $5x^3+2x^2+4x+4$ *i* $6x+3$.

b) En quest cas tenim

	x	$-ix^2-xi-i$	
x^4-i	x^3-i	$xi-i$	$1-i$
1	*0*	*1*	ix^2+ix+i
0	*1*	$-x$	$-ix^3-ix^2-ix+1$

Així doncs, $mcd(x^4-i, 3x^2+x)=1-i$ *(en particulart, els polinomis donats són coprimers), i les coeficients de Bézout són* $-ix^3-ix^2-ix+1$ *i* ix^2+ix+i. *Comprovem-ho:*

$$(x^4-i)(ix^2+ix+i)+(x^3-i)(-ix^3-ix^2-ix+1)=1-i.$$

128. Trobeu tots els polinomis $f(x)$ i $g(x)$ de $\mathbb{Z}/(5)[x]$ tals que

$$x=(x^2+2)f(x)+(3x+1)g(x) \text{ a } \mathbb{Z}/(5)[x].$$

Solució: *Fem la divisió euclidiana a* $\mathbb{Z}/(5)$ *i obtenim*

$$\begin{array}{r|l} x^2+2 & 3x+1 \\ \cline{2-2} -x^2+2x & 2x+1 \\ \cline{1-1} -2x+2 & \\ -3x-1 & \\ \cline{1-1} 1 & \end{array}$$

Per tant,

$$x^2 + 2 = (3x + 1)(2x + 1) + 1.$$

Equivalentment

$$x^2 + 2 - (3x + 1)(2x + 1) = 1.$$

Multiplicant per x,

$$(x^2 + 2)x - (3x + 1)(2x^2 + x) = x.$$

Per tant ja tenim una resposta: $f(x) = x$, $g(x) = -2x^2 - x = 3x^2 + 4x$.
Tota altra solució ha de ser de la forma

$$\begin{aligned} \bar{f}(x) &= f(x) + (3x + 1)q(x) \\ \bar{g}(x) &= g(x) - (x^2 + 2)q(x) \end{aligned}$$

per a algun $q(x) \in \mathbb{Z}/(5)[x]$.
En efecte, si posem

$$(x^2 + 2)f(x) + (3x + 1)g(x) = (x^2 + 2)\bar{f}(x) + (3x + 1)\bar{g}(x)$$

obtenim

$$(f(x) - \bar{f}(x))(x^2 + 2) = -(g(x) - \bar{g}(x))(3x + 1),$$

però com $x^2 + 2$ i $3x + 1$ són coprimers, $x^2 + 2$ ha de dividir $g(x) - \bar{g}(x)$. És a dir, $g(x) = \bar{g}(x) + q(x)(x^2 + 2)$, per a algun $q(x) \in \mathbb{Z}/(5)[x]$. Substituint i simplificant, tenim

$$(f(x) - \bar{f}(x))(x^2 + 2) = -(q(x)(x^2 + 2))(3x + 1),$$

és a dir

$$f(x) - \bar{f}(x) = -q(x)(3x + 1).$$

129. Sigui K un cos, $p(x) \in K[x]$ un polinomi i $\alpha \in K$. Proveu que $p(x) = (x - \alpha)q(x) + p(\alpha)$ per a algun $q(x) \in K[x]$ i que per tant, si $p(\alpha) = 0$ aleshores $(x - \alpha) \mid p(x)$.
Useu aquest resultat per interpretar el mètode de Ruffini com una divisió de polinomis.

Solució: *Com que el grau del polinomi reste que s'obté en dividir dos polinomis és menor que el grau del divisor, si dividim per $(x - \alpha)$, que és de grau 1, el reste és una constant k. Tindrem $p(x) = (x - \alpha)q(x) + k$, i per tant, $p(\alpha) = k$. Així doncs, tenim el típic enunciat de Ruffini:* un polinomi és divisible per $(x - \alpha)$ si i només si al substituir x per α dóna 0.

130. Trobeu les arrels dels polinomis següents als cossos indicats i factoritzeu-los.

(a) $p(x) = x^6 - 7x^3 - 8$ a $\mathbb{Q}$.

(b) $p(x) = x^3 - 3x^2 + x + 2$ a $\mathbb{R}$.

(c) $p(x) = x^4 + 3x^3 + 2x + 1$ a $\mathbb{Z}/(5)$.

(d) ($\star$) $p(x) = x^4 + x^3 + x^2 + x + 1$ a $\mathbb{C}$.

(e) $p(x) = x^{2^n} - 1$ a $\mathbb{Z}/(2)$.

(f) $p(x) = y^{-2} + xy + x^2$ a $\mathbb{R}(y)$.

Solució: a) *Posem $t = x^3$. Resolem $t^2 - 7t - 8 = 0$. Obtenim $t = 8$, o $t = -1$. Per tant, $x = 2$, 0 $x = -1$. Per tant,*

$$x^6 - 7x^3 - 8 = (x^3 - 8)(x^3 + 1).$$

I ara trobem les arrels d'aquest dos polinomis sobre $\mathbb{Q}$. El primer només té l'arrel 2, i el segon -1. Per tant, la factorització sobre $\mathbb{Q}$ és

$$x^6 - 7x^3 - 8 = (x - 2)(x^2 + 2x + 4)(x + 1)(x^2 - x + 1).$$

b) Com 2 és arrel tenim

$$x^3 - 3x^2 + x + 2 = (x - 2)(x^2 - x - 1).$$

c) Com $\mathbb{Z}/(5)$ té pocs elements els provem un per un a $x^4 + 3x^3 + 2x + 1$ i veiem que l'únic que dóna zero és $x = 2$: $2^4 + 3 \cdot 2^3 + 2 \cdot 2 + 1 = 45 = 0$.
Dividim per $x - 2$ i obtenim

$$x^4 + 3x^3 + 2x + 1 = (x^3 + 2)(x - 2) = (x^3 + 2)(x + 3).$$

Recordem que per dividir per $x-2$ podem utilitzar el mètode de Ruffini, que consisteix en escriure només els coeficients segons la taula adjunta.

	1	*3*	*0*	*2*	*1*
2		*2*	*0*	*0*	*4*
	1	*0*	*0*	*2*	*0*

Novament $x = 2$ és arrel de $x^3 + 2$ ja que $2^3 + 2 = 10 = 0$. Per tant,

$$x^4 + 3x^3 + 2x + 1 = (x^3 + 2)(x + 3) = (x^2 + 2x + 4)(x + 3)^2.$$

El discriminant de $x^2 + 2x + 4$ és -12, és a dir 3 a $\mathbb{Z}/(5)$, i 3 no té arrel quadrada a $\mathbb{Z}/(5)$, vegeu el problema 118. Per tant, $x^2 + 2x + 4$ és irreductible a $\mathbb{Z}/(5)$ i ja tenim la factorització buscada.

d) Primera solució. *Aquest problema pot sorprendre a algú que no hagi dibuixat mai un pentàgon. Però els que sí que hi han pensat saben que*

$$\frac{x^5 - 1}{x - 1} = x^4 + x^3 + x^2 + x + 1,$$

de manera que només hem de trobar les arrels cinquenes de 1 a $\mathbb{C}$. Tenim doncs

$$x^4 + x^3 + x^2 + x + 1 = \prod_{k=1}^{4} (x - e^{2\pi ik/5})$$

Segona solució. *També es pot arribar aquí per la força bruta, és a dir, descomposant primer sobre* $\mathbb{R}$ *a base d'escriure*

$$x^4 + x^3 + x^2 + x + 1 = (x^2 + Ax + 1)(x^2 + Bx + 1)$$

i trobant A *i* B *igualant coeficients. Obtenim* $A = \frac{1+\sqrt{5}}{2}$ *i* $B = \frac{1-\sqrt{5}}{2}$. *La raó d'or i l'oposat del seu invers, com era d'esperar, tractant-se del pentàgon.*
Ara cadascun d'aquests dos polinomis de segon grau es pot descompondre sobre $\mathbb{C}$.
Tercera solució.[1] *Escrivim*

$$x^4 + x^3 + x^2 + x + 1 = x^2(x^2 + x + 1 + \frac{1}{x} + \frac{1}{x^2}) = x^2\left((x + \frac{1}{x})^2 + (x + \frac{1}{x}) - 1\right),$$

i ara resolem l'equació de segon grau $z^2 + z - 1 = 0$, *i trobem* x *resolent* $z = x + \frac{1}{x}$.

e) A $\mathbb{Z}/(2)$ *es compleix que*

$$x^{2^n} - 1 = (x - 1)^{2^n}.$$

Només hi ha l'arrel 1 *amb multiplicitat* 2^n.
Això es pot provar, per exemple, per inducció. En efecte, simplement elevant al quadrat la igualtat certa per hipòtesis d'inducció

$$x^{2^{n-1}} - 1 = (x - 1)^{2^{n-1}},$$

obtenim el resultat.
També podem escriure el desenvolupament del binomi de Newton de $(x - 1)^{2^n}$ *i veure que tots els termes intermedis són* 0 *a* $\mathbb{Z}/(2)$ *ja que*

$$\binom{2^n}{j}, \quad j = 1, 2, \ldots, 2^n - 1,$$

és parell.
Això és fàcil de veure si acceptem que els números combinatoris són enters. Llavors escrivim

$$\binom{2^n}{j} = \frac{2^n \cdot 2^n - 1 \cdot 2^2 - 2 \ldots 2^n - j + 1}{j!}$$

Si j *és parell comparem* $2^n/j$, $(2^n - 2)/(j - 2)$, *etc. i veiem que tenim més dosos al numerador que al denominador (en descompondre en factors primers). Si* j *és imparell comparem* $2^n/(j-1)$, $(2^n - 2)/(j - 3)$, *etc. i fem el mateix argument.*

f) Recordem que $\mathbb{R}(y)$ *és l'anell de fraccions de la forma* $\frac{p(y)}{q(y)}$, *on* $p(y)$ *i* $q(y)$ *són polinomis en* y.
Aplicant la fórmula general per a la solució de les equacions de segon grau tenim

$$x = \frac{-y \pm \frac{1}{y}\sqrt{y^4 - 4}}{2}$$

[1] Proposada per Abel Rodríguez.

Mirem si y^4-4 té arrel quadrada. És a dir, mirem si hi ha polinomis $a(y), b(y)$ tals que

$$\left(\frac{a(y)}{b(y)}\right)^2 = y^4 - 4.$$

Podem suposar $a(y)$ i $b(y)$ coprimers.
Com

$$y^4 - 4 = (y^2+2)(y+\sqrt{2})(y-\sqrt{2})$$

observem que, per exemple $y-\sqrt{2}$ és un polinomi irreductible de grau 1 que divideix y^4-4.
Com

$$a(y)^2 = b(y)^2(y^2+2)(y+\sqrt{2})(y-\sqrt{2})$$

el polinomi $y-\sqrt{2}$ apareix elevat a una potència parell a l'esquerra i imparell a la dreta. Contradicció. Per tant, el polinomi donat és irreductible a $R(y)$.

131. a) Quants polinomis irreductibles de grau menor o igual a tres hi ha a $\mathbb{Z}/(5)[x]$?
b) Quants polinomis irreductibles de grau menor o igual a tres hi ha a $\mathbb{Z}/(p)[x]$ (p primer) ?

Solució: *Comencem mirant quants polinomis de grau 1 hi ha a $\mathbb{Z}/(p)$. Aquests s'escriuen com a_0+a_1x, amb $a_0, a_1 \in \mathbb{Z}/(p)$, amb $a_1 \neq 0$. Per tant, hi ha $p(p-1)$ polinomis de grau 1 a $\mathbb{Z}/(p)$.*
Si volem contar els mònics de grau 1 posem $a_1=1$ i per tant de mònics de grau 1 n'hi ha p.
El mateix argument demostra que hi ha $p^2(p-1)$ polinomis de grau 2 a $\mathbb{Z}/(p)$ (p^2 mònics). I $p^3(p-1)$ polinomis de grau 3 a $\mathbb{Z}/(p)$ (p^3 mònics).
Mirem ara quants n'hi ha de irreductibles.
És més còmode pensar primer només en els mònics i després multiplicar per $p-1$.
Així doncs, mònics irreductibles de grau 1: tots els de grau 1 són irreductibles, per definició, de manera que n'hi ha p. Escriurem $I_1^m = p$.
Mònics irreductibles de grau 2: N'hi tants com mònics de grau 2 (p^2) menys mònics de grau 2 reductibles. *Aquests seran els que provindran de multiplicar dos qualssevol dels polinomis mònics de grau 1, amb repeticions. Combinacions de p elements agafats de k en k amb repetició*

$$C_{p,k}^r = \binom{p+k-1}{k}$$

Així, doncs, quan $k=2$, tenim

$$\binom{p+1}{2} = \frac{p(p+1)}{2}$$

polinomis mònics de grau 2 reductibles.
Els irreductibles mònics de grau 2 són, doncs,

$$I_2^m = p^2 - \frac{p(p+1)}{2} = \frac{p(p-1)}{2}.$$

I els irreductibles de grau 2, mònics o no,

$$I_2 = \frac{p(p-1)^2}{2}$$

Mònics irreductibles de grau 3: N'hi tants com mònics de grau 3 (p^3) menys mònics de grau 3 reductibles. *Aquests seran els que provindran de multiplicar tres qualssevol dels polinomis mònics de grau 1, amb repeticions, més els que provinguin de multiplicar un irreductible mònic de grau 2 per mònics de grau 1.*
Els productes de tres de grau 1 són combinacions amb repetició de p elements agafats de tres en tres, de manera que tenim

$$\binom{p+2}{3} = \frac{p(p+1)(p+2)}{6}.$$

I dels que provenen de multiplicar un irreductible de grau dos per un de grau 1 n'hi ha

$$I_2^m \cdot p = \frac{p^2(p-1)}{2}$$

En total, doncs, hi ha

$$\frac{p^2(p-1)}{2} + \frac{p(p+1)(p+2)}{6} = \frac{p(2p^2+1)}{3}$$

polinomis mònics reductibles de grau 3.
I per tant hi ha

$$I_3^m = p^3 - \frac{p(2p^2+1)}{3} = \frac{p(p^2-1)}{3}.$$

polinomis mònics irreductibles de grau 3.
Si traiem la condició de mònic, tenim

$$I_3 = \frac{p(p^2-1)(p-1)}{3}$$

polinomis irreductibles de grau 3.
Finalment, de polinomis irreductibles de grau menor o igual a tres n'hi ha

$$I = I_1 + I_2 + I_3 = p(p-1) + \frac{p(p-1)^2}{2} + \frac{p(p^2-1)(p-1)}{3} = \frac{p(p-1)(2p^2+3p+1)}{6}.$$

I si volem els mònics només hem de dividir per $p-1$,

$$I^m = \frac{p(2p^2+3p+1)}{6}.$$

Vegeu el problema 1h).

132. Sigui $f(x) = a_0 + a_1x + \cdots + a_nx^n \in \mathbb{Q}[x]$ amb coeficients a $\mathbb{Z}$, i siguin $r, s \in \mathbb{Z}$ tals que $\text{mcd}(r,s) = 1$. Proveu que

$$f\left(\frac{r}{s}\right) = 0 \Longrightarrow r|a_0 \text{ i } s|a_n$$

$$f\left(\frac{r}{s}\right) = 0 \Longrightarrow (r-s)\,|f(1) \text{ i } (r+s)\,|f(-1)$$

Solució: *Utilitzarem el resultat general que diu:* Siguin $a, b, c \in \mathbb{Z}$ tals que $a|bc$. Si a i b són coprimers, aleshores $a|c$.
De la igualtat

$$f(\frac{r}{s}) = a_0 + a_1\frac{r}{s} + \cdots + a_n(\frac{r}{s})^n = 0,$$

multiplicant per s^n, *obtenim*

$$a_0 s^n = \dot{r},$$

i com r *i* s *són coprimers, i* r *divideix* $a_0 s^n$, *ha de ser que* r *divideixi* a_0, $r|a_0$.
Però de la mateixa igualtat

$$a_0 s^n + a_1 r s^{n-1} + \cdots + a_{n-1} r^{n-1} s + a_n r^n = 0,$$

obtenim

$$a_n r^n = \dot{s},$$

que s *divideix* $a_n r^r$, *i per tant,* $s|a_n$.
La condició $f(\frac{r}{s}) = 0$ *també implica, com en el cas d'arrels enteres, que* $f(x)$ *és divisible per* $(x - \frac{r}{s})$ *a* $\mathbb{Q}[x]$. *Concretament*

$$f(x) = (x - \frac{r}{s})q(x)$$

on $q(x)$ *és un polinomi de coeficients racionals,* $q(x) \in \mathbb{Q}[x]$.
En particular

$$f(1) = \frac{s-r}{s}q(1).$$

Però si revisem l'algorisme de la divisió veurem que en dividir $f(x)$ *entre* $(x - \frac{r}{s})$ *el polinomi quocient que apareix,* $q(x)$, *té per coeficients expressions polinòmiques on només apareixen els* $a_i \in \mathbb{Z}$ *i* $\frac{r}{s}$. *Així en calcular* $q(1)$ *obtenim una fracció de la forma*

$$q(1) = \frac{m}{s^k}, \qquad \text{per a una certa } m \in \mathbb{Z}, \text{ i una certa } k \in \mathbb{N}.$$

Així

$$f(1) = \frac{s-r}{s} \cdot \frac{m}{s^k},$$

i per tant,

$$s^{k+1} f(1) = (s-r)m.$$

Com $(s - r)$ *és coprimer amb* s^{k+1}, *ha de ser que* $(s - r)|f(1)$.
El mateix argument permet demostrar que $(r + s)|f(-1)$. *Hem assumit* $f(1)$ *i* $f(-1)$ *diferents de zero.*

133. Useu l'exercici anterior per trobar les arrels dels polinomis següents de $\mathbb{Q}[x]$:

(a) $x^3 - 2x^2 + x + 15$. (b) $2x^4 + 3x^3 + 6x + 9$. (c) $36x^4 - 36x^3 + 5x^2 + 4x - 1$.

Solució: *(a) Com aquest polinomi és mònic, si té una arrel racional, aquesta és automàticament entera, ja que sabem, pel problema anterior, que si r/s és solució, llavors s divideix al coeficient de major grau, que és 1, i per tant, $s = \pm 1$.*
Les possibles arrels enteres són divisors del terme independent, $\pm 1, \pm 3, \pm 5, \pm 15$.
Els podem comprovar un per un i veure que cap d'ells és arrel. O podem observar, per la segona part del problema anterior, que la possible arrel entera r ha de complir $r + s|11$ i $r - s|15$, ja que $f(1) = 15$ i $f(-1) = 11$, on $f(x)$ és el polinomi donat. I això, per als possibles valors de r abans considerats i amb $s = \pm 1$ és impossible.

b) Sigui $\frac{r}{s}$ una arrel d'aquest polinomi. Llavors, r ha de dividir 9, i s ha de dividir 2. És a dir, $r = \pm 1; \pm 3; \pm 9$, i $s = \pm 1; \pm 2$.
Però, a més, com que $f(1)$ i $f(-1)$ no són zero (1 i -1 no són arrels del polinomi $f(x)$ donat), ha de passar que $(r - s)|20$, ja que $f(1) = 20$, i $(r + s)|2$, ja que $f(-1) = 2$.
Estudiem les possibles combinacions de r i s. Com que 1 i -1 no són arrels els casos $r = \pm s$ queden eliminats. També els valors $r = \pm 9$ queden eliminats, ja que $r + s = \pm 1 \pm 2$.
Tenim doncs

r	s	r+s	r-s
3	1	4	2
-3	1	-2	-4
3	-1	2	4
-3	-1	-4	-2
1	2	3	-1
-1	2	1	-3
3	2	5	1
-3	2	-1	-5
1	-2	-1	3
-1	-2	-3	1
3	-2	1	5
-3	-2	-5	-1

Els valors de la columna $r + s$ només poden ser ± 1 o ± 2. La columna $r - s$ ha de dividir a 20. Així la taula queda

r	s	r+s	r-s
-3	1	-2	-4
3	-1	2	4
-3	2	-1	-5
3	-2	1	5

Les úniques possibles solucions són -3 (que no ho és) i $-\dfrac{3}{2}$ que sí que ho és.
Això permet factoritzar el polinomi com

$$2x^4 + 3x^3 + 6x + 9 = 2(x^2 - 3^{1/3}x + 3^{2/3})(x + 3^{1/3})(x + \frac{3}{2}).$$

c) Sigui $\frac{r}{s}$ una arrel d'aquest polinomi. Llavors, r ha de dividir -1, i s ha de dividir 36. És a dir, $r = \pm 1$, i $s = \pm 1; \pm 2; \pm 3; \pm 4; \pm 6; \pm 9; \pm 12; \pm 18; \pm 36$.
Però, a més, com que $f(1)$ i $f(-1)$ no són arrels, ha de passar que $(r-s)|8$, ja que $f(1) = 8$, i $(r+s)|72$, ja que $f(-1) = 72$. ($f(x)$ és el polinomi donat).
Notem que el fet de que $f(1)$ i $f(-1)$ no siguin arrels elimina els casos $r = \pm s$.
Estudiem els casos possibles. Descartem els valors $|s| \geq 4$, ja que $r - s = |8$, i els cassos $r = \pm s$. Tenim doncs

r	*s*	*r+s*	*r-s*
1	*2*	*3*	*-1*
1	*-2*	*-1*	*3*
1	*3*	*4*	*-2*
1	*-3*	*-2*	*4*
-1	*2*	*1*	*-3*
-1	*-2*	*-3*	*1*
-1	*3*	*2*	*-4*
-1	*-3*	*-4*	*2*

Els valors de la columna $r - s$ han de ser divisors de 8. Així la taula queda

r	*s*	*r+s*	*r-s*
1	*2*	*3*	*-1*
1	*3*	*4*	*-2*
1	*-3*	*-2*	*4*
-1	*-2*	*-3*	*1*
-1	*3*	*2*	*-4*
-1	*-3*	*-4*	*2*

Les úniques possibles solucions són $\frac{1}{2}$ (que sí que ho és), $\frac{1}{3}$ (que sí que ho és), $-\frac{1}{3}$ (que sí que ho és).
Això permet factoritzar el polinomi com

$$36x^4 - 36x^3 + 5x^2 + 4x - 1 = (x^2 - \frac{1}{9})(x - \frac{1}{2})^2.$$

134. a) Proveu que si un polinomi $f(x) = a_0 + a_1x + \cdots + a_nx^n \in \mathbb{Q}[x]$ amb coeficients a $\mathbb{Z}$ té una arrel a $\mathbb{Z}$, aleshores, el polinomi $\bar{f}(x) = \overline{a_0} + \overline{a_1}x + \cdots + \overline{a_n}x^n \in \mathbb{Z}/(n)[x]$, també tindrà una arrel a $\mathbb{Z}/(n)$, per a tot $n \in \mathbb{N}$.
b) Demostreu que el polinomi $x^5 + 693x^3 - 431x^2 - 321x + 315315$ no té cap arrel a $\mathbb{Q}$.

Solució: *a) La classe mòdul n d'una arrel de $f(x)$ és arrel de $\bar{f}(x)$.*
b) Si tingués una arrel a $\mathbb{Q}$, aquesta arrel estaria en realitat a $\mathbb{Z}$, per ser aquest polinomi mònic (vegeu problema 132). Per tant, quan mirem el polinomi donat a $\mathbb{Z}/(2)[x]$, $x^5 + x^3 - x^2 - x + 1$, aquest hauria de tenir alguna arrel a $\mathbb{Z}/2$, però clarament ni 0, ni 1 ho són.

135. Sigui $K = \mathbb{Q}$, $\mathbb{R}$ o $\mathbb{C}$. Proveu que un polinomi $f(x) \in K[x]$ té factors irreductibles múltiples si i només si $\text{mcd}(f(x), f'(x)) \neq 1$. Què podem dir sobre les arrels de $f(x)$? Què passa si prenem cossos com $K = \mathbb{Z}/(p)$?
Factoritzeu el polinomi $x^6 + 4x^4 + 2x^5 + 4x^3 + 4x^2 + 2x + 1$ a $\mathbb{C}[x]$, $\mathbb{R}[x]$ i $\mathbb{Q}[x]$.

Solució: *Descomponem $f(x)$ en factors irreductibles.*

$$f(x) = p_1^{r_1}(x) \cdot \cdots \cdot p_k^{r_k}(x).$$

Recordeu que el màxim comú divisor de polinomis està definit llevat d'escalars i la descomposició en irreductibles és única també llevat d'escalars. Podem suposar $r_i > 0$, $i = 1, 2, \ldots, k$. A partir d'ara, i simplement per comoditat, escriuré p_i en lloc de $p_i(x)$. Observem que

$$f'(x) = (r_1 p_1^{r_1 - 1} p_1')p_2^{r_2} \ldots p_k^{r_k} + p_1^{r_1}(r_2 p_2^{r_2 - 1} p_2')p_3^{r_3} \ldots p_k^{r_k} + \ldots$$

Si, per a algun $i = 1, 2, \ldots, k$, es compleix que $r_i - 1 > 0$, llavors el corresponent p_i divideix tant a $f(x)$ com a $f'(x)$ (apareix a tots els sumands de l'expressió de $f'(x)$).
Per tant, si $mcd(f(x), f'(x)) = 1$, llavors $r_i = 1$, per tot i. És a dir, que si un polinomi és coprimer amb el seu derivat llavors no te factors irreductibles múltiples.
Recíprocament, suposem que a l'anterior descomposició de $f(x)$ en factors primers tenim $r_i = 1$, per a tot $i = 1, \ldots, k$.
Llavors a cadascun dels sumands de l'expressió de $f'(x)$ falta un polinomi p_i que sí apareix a tots els demés sumands.

$$f'(x) = p_1' p_2 \ldots p_k + p_1 p_2' p_3 \ldots p_k + \ldots$$

Si p_i dividís $f'(x)$, com que apareix a tots els sumands menys un, també dividiria aquest sumand, i per tant dividiria a p_i', la qual cosa és impossible ja que el grau de p_i' és menor, en una unitat, al grau de p_i (recordeu que estem suposant que el grau de p_i és almenys 1).
Per tant, $f(x)$ i $f'(x)$ són coprimers.

Què podem dir sobre les arrels de $f(x)$? *Si α és arrel, llavors a la descomposició de $f(x)$ en factors primers apareix el polinomi $(x - \alpha)^r$, per algun r.*
Per tant, podem reescriure l'apartat anterior dient: $f(x)$ té arrels múltiples si i només si $f(x)$ i $f'(x)$ no són coprimers.

Què passa si prenem cossos com $K = \mathbb{Z}/(p)$?
El resultat és igualment cert, però la part final de la demostració anterior podria no funcionar, ja que existeixen polinomis no constants amb derivada 0. Per exemple, $p(x) = x^p$. Si això passés per algun dels p_i de la demostració anterior, el sumand de $f'(x)$ on hi apareix aquest p_i' s'anul·laria, i l'argument no funcionaria.
Tenim però el lema següent (vegeu ACM, p. 362) que ens assegura que aquesta situació no es pot donar.

Lema. *Sigui $g(x)$ un polinomi de grau ≥ 1 sobre un cos K finit de característica p. Si $g'(x) = 0$ (i.e., $g'(x)$ és el polinomi 0), llavors existeix $h(x) \in K[x]$ tal que*

$$g(x) = (h(x))^p.$$

Com a corol·lari obtenim que si $g(x)$ és irreductible, ha de ser $g'(x) \neq 0$ (és a dir, $g'(x)$ no pot ser el polinomi 0).
En particular els p_i' que apareixen a l'expressió de $f'(x)$ són no nuls.
Això fa, com hem comentat abans, que la demostració que havíem fet per a $\mathbb{R}, \mathbb{Q}, \mathbb{C}$ valgui també per a $\mathbb{Z}/(p)$, o qualsevol altre cos finit de característica p.

Factoritzeu el polinomi $f(x) = x^6 + 4x^4 + 2x^5 + 4x^3 + 4x^2 + 2x + 1$ a $\mathbb{C}[x]$, $\mathbb{R}[x]$ i $\mathbb{Q}[x]$.
Ho fem només sobre $\mathbb{R}[x]$. Calculem el $mcd(f(x), f'(x))$.
En dividir $f(x)$ entre $f'(x)$ obtenim quocient $\frac{1}{6}x + \frac{1}{18}$ i resta $\frac{1}{9}(7x^4 + 10x^3 + 18x^2 + 11x + 8)$.
En dividir $f'(x)$ entre $7x^4 + 10x^3 + 18x^2 + 11x + 8$, obtenim quocient $\frac{6}{7}x + \frac{10}{49}$ i resta $\frac{18}{49}(-4x^3 - 3x^2 - 3x + 1)$.
En dividir $7x^4 + 10x^3 + 18x^2 + 11x + 8$ entre $-4x^3 - 3x^2 - 3x + 1$ obtenim quocient $-\frac{7}{4}x - \frac{19}{16}$ i resta $\frac{147}{16}(x^2 + x + 1)$.
En dividir $-4x^3 - 3x^2 - 3x + 1$ entre $x^2 + x + 1$ obtenim quocient $-4x + 1$ i resta 0.
Per tant, $mcd(f(x), f'(x)) = x^2 + x + 1$.
Si efectuem la divisió obtenim

$$f(x) = (x^2 + x + 1)(x^4 + x^3 + 2x^2 + x + 1)$$

Però sabem que $f(x)$ té un factor irreductible múltiple. Mirem si és el factor irreductible que acabem de trobar, és a dir, $x^2 + x + 1$, dividint $x^4 + x^3 + 2x^2 + x + 1$ entre ell. Obtenim

$$x^4 + x^3 + 2x^2 + x + 1 = (x^2 + x + 1)(x^2 + 1).$$

Per tant,

$$f(x) = (x^2 + x + 1)^2(x^2 + 1).$$

136. Factoritzeu a $\mathbb{C}[x], \mathbb{R}[x], \mathbb{Q}[x]$ i a $\mathbb{Z}/(2)[x]$ els polinomis

$$a)\ x^2 + x + 1; \quad b)\ x^4 + 4; \quad c)\ x^6 - 1; \quad d)\ x^8 - 1; \quad e)\ x^4 + x^2 + 1.$$

Solució: *a) Només observo que sobre $\mathbb{Z}/(2)$ és irreductible ja que ni 0 ni 1 són arrels. Sobre $\mathbb{Q}[x]$ i $\mathbb{R}[x]$ també és irreductible, ja que aquest polinomi té dues arrels complexes.*

b) Per trobar les arrels complexes hem de calcular l'arrel quarta de -4.

$$x = \sqrt[4]{-4} = \sqrt[4]{4_\pi} = (\sqrt[4]{4})_{\frac{\pi + 2k\pi}{4}}; \quad k = 0, 1, 2, 3.$$

A $\mathbb{C}[x]$ factoritza com

$$x^4 + 4 = \prod_{k=0}^{3} (x - \sqrt[4]{4} \cdot e^{i(\pi + 2k\pi)/4}) = \prod_{k=0}^{3} \left(x - \sqrt{2}(\cos(\frac{\pi}{4} + \frac{k\pi}{2}) + i \sin(\frac{\pi}{4} + \frac{k\pi}{2})) \right).$$

Aparellant les arrels conjugades fem desaparèixer els nombres complexos. Per exemple,

$$\begin{aligned}(x-\sqrt{2}(\frac{\sqrt{2}}{2}+i\frac{\sqrt{2}}{2}))(x-\sqrt{2}(\frac{\sqrt{2}}{2}-i\frac{\sqrt{2}}{2})) &= ((x-1)-i)((x-1)+i))\\ &= (x-1)^2+1\\ &= x^2-2x+2.\end{aligned}$$

Així, a $\mathbb{R}[x]$ *(i automàticament a* $\mathbb{Q}[x]$*) tenim*

$$x^4+4=(x^2-2x+2)(x^2+2x+2).$$

Observem que a $\mathbb{Z}/(2)[x]$ *tenim* $x^4+4=x^4$*, i és clar que* x^4 *només té l'arrel* 0*, amb multiplicitat* 4*.*

c) Per trobar les arrels complexes hem de calcular l'arrel sisena de 1*. Per tant*

$$x^6-1=\prod_{k=0}^{5}(x-e^{i2k\pi/6})$$

Si $k=0$ *o* $k=3$ *els números complexos corresponents són en realitat reals (*1 *i* -1*), de manera que l'anterior igualtat s'escriu com*

$$x^6-1=(x-1)(x+1)(x-(\frac{1}{2}+i\frac{\sqrt{3}}{2}))(x-(\frac{1}{2}-i\frac{\sqrt{3}}{2}))(x-(-\frac{1}{2}+i\frac{\sqrt{3}}{2}))(x-(-\frac{1}{2}-i\frac{\sqrt{3}}{2}))$$

Aparellant les arrels conjugades fem desaparèixer els nombres complexos. Per exemple,

$$\begin{aligned}(x-(\frac{1}{2}+i\frac{\sqrt{3}}{2}))(x-(\frac{1}{2}-i\frac{\sqrt{3}}{2})) &= ((x-\frac{1}{2})-i\frac{\sqrt{3}}{2})((x-\frac{1}{2})+i\frac{\sqrt{3}}{2}))\\ &= (x-\frac{1}{2})^2+\frac{3}{4}\\ &= x^2-x+1.\end{aligned}$$

Finalment, sobre $\mathbb{R}[x]$ *tenim*

$$x^6-1=(x-1)(x+1)(x^2-x+1)(x^2+x+1).$$

És la mateixa descomposició que tenim a $\mathbb{Q}[x]$ *ja que els coeficients han sortit directament racionals. I també la mateixa a* $\mathbb{Z}/(2)[x]$*, però ara és millor escriure-la com*

$$x^6-1=(x+1)^2(x^2+x+1)^2.$$

ja que $1=-1\in\mathbb{Z}/(2)$*.*

d) Exercici similar als anteriors.

e) Fem el canvi de variable $t=x^2$*, trobem les arrels de* $t^2+t+1=0$*, que són*

$$t=\frac{-1\pm\sqrt{-3}}{2}=\frac{-1\pm i\sqrt{3}}{2},$$

i ara resolem

$$x = \sqrt{-\frac{1}{2} + i\frac{\sqrt{3}}{2}} = \sqrt{1_{2\pi/3}} = 1_{\frac{2\pi/3+2k\pi}{2}}, \quad k = 0, 1.$$

És a dir,

$$x = \frac{1}{2} + i\frac{\sqrt{3}}{2}, \qquad x = -\frac{1}{2} - i\frac{\sqrt{3}}{2}$$

Però també hem de resoldre

$$x = \sqrt{-\frac{1}{2} - i\frac{\sqrt{3}}{2}} = \sqrt{1_{4\pi/3}} = 1_{\frac{4\pi/3+2k\pi}{2}}, \quad k = 0, 1.$$

És a dir,

$$x = -\frac{1}{2} + i\frac{\sqrt{3}}{2}, \qquad x = \frac{1}{2} - i\frac{\sqrt{3}}{2}$$

Per tant, sobre $\mathbb{C}[x]$,

$$x^4 + x + 1 = (x - \frac{1}{2} - i\frac{\sqrt{3}}{2})(x - \frac{1}{2} + i\frac{\sqrt{3}}{2})(x + \frac{1}{2} - i\frac{\sqrt{3}}{2})(x + \frac{1}{2} + i\frac{\sqrt{3}}{2})$$

Sobre $\mathbb{R}[x]$ *(agrupant els conjugats)*

$$x^4 + x + 1 = (x^2 - x + 1)(x^2 + x + 1)$$

que és també la descomposició a $\mathbb{Q}[x]$.
A $\mathbb{Z}/(2)[x]$,

$$x^4 + x + 1 = (x^2 - x + 1)^2.$$

137. Trobeu[2] un polinomi de grau 3, $P(x)$, amb coeficients enters, tal que $P(a) = P(b) = P(c)$, on $a, b, c \in \mathbb{R}$ són tals que

$$\begin{aligned} a + b + c &= 2 \\ a^2 + b^2 + c^2 &= 2 \end{aligned}$$

Solució: *Observem que*

$$2(ab + bc + ca) = (a + b + c)^2 - (a^2 + b^2 + c^2) = 2.$$

Per tant a, b, c *són les arrels del polinomi* $x^3 - 2x^2 + x - abc$. *En particular, el polinomi de grau* 3, $f(x) = x^3 - 2x^2 + x$ *compleix* $f(a) = f(b) = f(c) = abc$.

[2]Olimpíada Matemàtica Britànica Femenina 2011.

138. Siguin x_1, x_2, x_3 les arrels (desconegudes) de $x^3 - x^2 - 1 = 0$. Trobeu un polinomi que tingui arrels $y_1 = x_2 + x_3$, $y_2 = x_1 + x_3$, $y_3 = x_1 + x_2$.

Solució: *El polinomi demanat és*

$$x^3 - (y_1 + y_2 + y_3)x^2 + (y_1y_2 + y_2y_3 + y_3y_1)x - y_1y_2y_3.$$

Pel mateix motiu, les arrels x_1, x_2, x_3 compleixen

$$\begin{aligned} x_1x_2x_3 &= 1 \\ x_1x_2 + x_2x_3 + x_3x_1 &= 0 \\ x_1 + x_2 + x_3 &= 1 \end{aligned}$$

Elevant la tercera al quadrat i tenint en compte la segona tenim

$$x_1^2 + x_2^2 + x_3^2 = 1.$$

Multiplicant la segona per x_1 i tenint en compte la primera tenim

$$x_1^2y_1 + 1 = 0.$$

Ara ja podem calcular els coeficients del polinomi buscat.

$$y_1 + y_2 + y_3 = 2(x_1 + x_2 + x_3) = 2.$$

També observem que

$$y_1y_2 = x_3^2, \quad y_2y_3 = x_1^2, \quad y_3y_1 = x_2^2.$$

De manera que

$$y_1y_2 + y_2y_3 + y_3y_1 = 1.$$

Finalment

$$y_1y_2y_3 = y_1x_1^2 = -1.$$

El polinomi buscat és doncs

$$x^3 - 2x^2 + x + 1.$$