Problemes de Fonaments Matemàtics

Edició a càrrec de José Luis Ruiz
Juliol 2017

Jaume Martí
Montserrat Maureso
Mercè Mora
Francesc Prats
José Luis Ruiz
Pilar Sobrevilla
Francesc Tiñena
Joan Trias

Departament de Matemàtiques
Facultat d'Informàtica de Barcelona
Universitat Politècnica de Catalunya

ÍNDEX

PREFACI

Aquest és un recull de problemes per a l'assignatura Fonaments Matemàtics. D'aquests problemes, el professor del taller de problemes anuncia amb antelació quins problemes es resolen a cada taller. Cal que l'estudiant prepari aquests tallers fent les tasques prèvies següents:

1) llegir i comprendre els enunciats proposats,

2) estudiar els conceptes teòrics necessaris per a entendre'ls, i

3) procurar resoldre els exercicis.

És molt recomanable que cada estudiant pensi ell sol la resta de problemes i aprofiti els horaris de consulta dels seus professors per intentar resoldre els dubtes que li puguin sorgir.

CAPÍTOL 0

INTRODUCCIÓ

0.1 Expressa, amb l'ajut del símbol de sumatori i de dues maneres diferents:

a) La suma dels quadrats dels cent primers nombres senars.

b) La suma de les arrels quadrades dels cent primers nombres parells.

0.2 Calcula les sumes i els productes següents.

1) $\sum_{j=1}^{10} 2$

2) $\sum_{k=1}^{10} j$

3) $\sum_{j=1}^{10} j^2$

4) $\sum_{j=1}^{10} 2^j$

5) $\sum_{n=3}^{6} (n-1)$

6) $\sum_{n=-2}^{2} n^2$

7) $\sum_{n=-2}^{2} n(n+1)$

8) $\prod_{m=1}^{5} 3$

9) $\prod_{i=1}^{5} (i+1)$

10) $\prod_{j=-1}^{4} (j+1)$

11) $\prod_{j=1}^{5} j^2$

12) $\prod_{i=1}^{5} 2^i$

0.3 Expresseu les sumes següents en funció de S, on $S = \sum_{n=1}^{10} a_n$:

1) $\sum_{m=1}^{10} a_m$

2) $\sum_{i=0}^{9} a_i$

3) $\sum_{j=1}^{10} a_{j-1}$

0.4 Siguin m, n enters tals que $m \leq n$. Expresseu cadascuna de les sumes següents en funció de A i B, on $A = \sum_{i=m}^{n} a_i$ i $B = \sum_{i=m}^{n} b_i$:

1) $\sum_{i=m}^{n} 5a_i$

2) $\sum_{i=m}^{n} (a_i - b_i)$

3) $\sum_{i=m}^{n} (-b_i)$

4) $\sum_{i=m}^{n} (3a_i + 5b_i)$

0.5 Expresseu els productes següents en funció de $A = \prod_{i=1}^{n} a_i$:

1) $\prod_{i=1}^{n} ia_i$

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

3) $\prod_{i=1}^{n} ka_i$

0.6 Si $A = \prod_{i=1}^{n} a_i$ i $B = \prod_{i=1}^{n} b_i$, demostreu que:

1) $\prod_{i=1}^{n} a_i b_i = AB$

2) $\prod_{i=1}^{n}\prod_{j=1}^{n} a_i b_j = A^n B^n$

0.7

a) Escriviu la suma $\sum_{k=1}^{n+1} \frac{1}{k^2}$ com la suma d'un sumatori i l'últim terme.

b) Escriviu la suma $\sum_{k=1}^{n+1} 2^k$ com la suma d'un sumatori i els dos últims termes.

0.8 Proveu que si $n \geq 0$, llavors $\sum_{k=0}^{n+3} r^k - \sum_{k=0}^{n} r^k = r^n(r^3 + r^2 + r)$.

0.9 Calculeu la suma $\sum_{k=1}^{n}(k+3)^2$, sabent que:

$$\sum_{k=1}^{n} k = \frac{n(n+1)}{2}, \qquad \sum_{k=1}^{n} k^2 = \frac{n(n+1)(2n+1)}{6}$$

Observació: aquestes dues fórmules es demostraran més endavant aplicant el principi d'inducció.

0.10 Expresseu la suma $\sum_{k=-29}^{n} (k+28)^2$ en la forma $\sum_{j=1}^{m} a_j$.

0.11 Expresseu cada una de les sumes següents amb un únic sumatori.

1) $\sum_{k=1}^{n}(6k-3) + \sum_{k=1}^{n}(4-5k)$

2) $2\sum_{k=1}^{n}(3k^2-4) + 3\sum_{k=1}^{n}(3k^2+1)$

3) $\sum_{i=1}^{100}(2i-1)^2 + \sum_{i=0}^{99}(2i+1)^2$

4) $\sum_{i=1}^{100}(4i-1)^2 + \sum_{i=1}^{100}(4i+1)^2$

5) $\sum_{i=0}^{99}(7i-1)^2 + \sum_{j=1}^{100}(7j+6)^2$

CAPÍTOL 1

RAONAMENT

1.1 Suposem que p, q i r tenen els valors de veritat 1, 1 i 0, respectivament. Quin és el valor de veritat de $\neg(p \vee q) \wedge (q \to r)$?

1.2 Si $p \to q$ i p prenen valor de veritat 1, quin és el valor de veritat de q?

1.3 Usant les taules de veritat demostreu l'equivalència de les fórmules següents (α, β, γ són fórmules proposicionals).

1) $\alpha \to \beta \equiv \neg\alpha \vee \beta$

2) $\alpha \leftrightarrow \beta \equiv (\alpha \to \beta) \wedge (\beta \to \alpha)$

3) $\neg(\alpha \wedge \beta) \equiv \neg\alpha \vee \neg\beta$, $\neg(\alpha \vee \beta) \equiv \neg\alpha \wedge \neg\beta$ (lleis de De Morgan)

4) $\neg(\alpha \to \beta) \equiv \alpha \wedge \neg\beta$

5) $\neg\beta \to \neg\alpha \equiv \alpha \to \beta$

6) $(\alpha \vee \beta) \to \gamma \equiv (\alpha \to \gamma) \wedge (\beta \to \gamma)$

7) $\alpha \to (\beta \vee \gamma) \equiv (\alpha \wedge \neg\beta) \to \gamma$

8) $\alpha \to (\beta \to \gamma) \equiv (\alpha \wedge \beta) \to \gamma \equiv \beta \to (\alpha \to \gamma)$

1.4 Siguin α, β i γ fórmules proposicionals. Usant les equivalències següents:

a) $\neg(\neg\alpha) \equiv \alpha$ b) $\alpha \to \beta \equiv \neg\alpha \vee \beta$ c) $\neg(\alpha \wedge \beta) \equiv \neg\alpha \vee \neg\beta$

i les propietats associatives, commutatives i distributives, demostreu l'equivalència de les fórmules següents (sense taules de veritat). Justifiqueu tots els passos.

1) $\neg(\alpha \vee \beta) \equiv \neg\alpha \wedge \neg\beta$

2) $\neg(\alpha \to \beta) \equiv \alpha \wedge \neg\beta$

3) $\neg\beta \to \neg\alpha \equiv \alpha \to \beta$

4) $(\alpha \vee \beta) \to \gamma \equiv (\alpha \to \gamma) \wedge (\beta \to \gamma)$

5) $\alpha \to (\beta \vee \gamma) \equiv (\alpha \wedge \neg\beta) \to \gamma$

6) $\alpha \to (\beta \to \gamma) \equiv (\alpha \wedge \beta) \to \gamma \equiv \beta \to (\alpha \to \gamma)$

1.5 Proveu que la fórmula proposicional $((p \to q) \wedge (\neg p \to q)) \to (r \to q)$ és una tautologia, on p i q són lletres proposicionals.

1.6 Siguin p, q, r, s i t lletres proposicionals.

1) Suposem que les fórmules proposicionals $(p \vee q) \to r$, $s \to p$, $s \vee q$ i $(\neg t) \to (\neg r)$ són certes. Podem deduir que t és certa?

2) Suposem que les fórmules proposicionals $p \to q$, $(\neg r) \to (\neg q)$, $s \to t$ i $p \vee s$ són certes. Podem deduir que $r \vee t$ és certa?

3) Suposem que les fórmules proposicionals $q \to (t \vee r)$, $(r \vee s) \to (q \to p)$ i $(\neg t) \wedge q$ són certes. Podem deduir que p és certa?

4) Suposem que les fórmules proposicionals $(\neg p) \to (q \to (\neg r))$, $r \to (\neg p)$, $((\neg s) \vee p) \to (\neg\neg r)$ i $\neg s$ són certes. Podem deduir que $\neg q$ és certa?

1.7 Doneu totes les subfórmules de les fórmules:

1) $\neg\neg q \wedge (p \to (q \vee r))$ 2) $(p \to \neg(q \vee \neg r)) \to ((p \wedge q) \to r)$

1.8 Considereu les connectives $\downarrow$ i $|$ definides de la manera següent:

$$p \downarrow q := \neg p \wedge \neg q, \quad p|q := \neg p \vee \neg q$$

1) Feu la taula de veritat de les fórmules $p|q$ i $(p \downarrow p) \downarrow (q \downarrow q)$ i doneu una fórmula equivalent a $p|q$ que només contingui les connectives $\neg$ i $\downarrow$.

2) Feu la taula de veritat de les fórmules $p \downarrow q$ i $(p|p)|(q|q)$ i doneu una fórmula equivalent a $p \downarrow q$ que només contingui les connectives $\neg$ i $|$.

3) Doneu una fórmula equivalent a $p|q$ que només contingui la connectiva $\downarrow$.

4) Doneu una fórmula equivalent a $p \downarrow q$ que només contingui la connectiva $|$.

1.9 Trobeu una fórmula equivalent a $p \leftrightarrow q$ on hi apareguin exclusivament:

1) Les connectives $\neg$ i $\vee$. 2) Les connectives $\neg$ i $\wedge$. 3) Les connectives $\neg$ i $\to$.

1.10 Considerem les dues connectives lògiques X i O definides per les taules de veritat que segueixen:

p	q	pXq	pOq
0	0	1	1
0	1	1	0
1	0	1	0
1	1	0	0

1) Expresseu la connectiva $\wedge$ en funció únicament de la connectiva X.

2) Expresseu la connectiva $\vee$ en funció únicament de la connectiva X.

3) Expresseu la connectiva $\to$ en funció únicament de la connectiva X.

4) Expresseu la connectiva $\wedge$ en funció únicament de la connectiva O.

5) Expresseu la connectiva $\vee$ en funció únicament de la connectiva O.

6) Expresseu la connectiva $\to$ en funció únicament de la connectiva O.

7) Expresseu la connectiva X en funció únicament de la connectiva O.

8) Expresseu la connectiva O en funció únicament de la connectiva X.

1.11 En un cert llenguatge de programació, la instrucció:

```
if p then I endif
```

significa que si la condició p és certa, llavors s'executa el conjunt d'instruccions I; i si p és falsa, llavors no s'executa cap instrucció i el programa continua. La instrucció:

```
if p then I1 else I2 endif
```

significa que si la condició p és certa, llavors s'executa el conjunt d'instruccions I_1; i si p és falsa, llavors s'executa el conjunt d'instruccions I_2.

Una condició és un enunciat que pot ser vertader o fals. Per exemple, '$x > 3$' és una condició. Si el valor emmagatzemat a 'x' és més gran que tres, llavors la condició '$x > 3$' es complirà (és a dir, l'enunciat serà vertader); si el valor emmagatzemat a 'x' no és més gran que tres, llavors la condició no es complirà (l'enunciat serà fals). Les condicions, doncs, des d'un punt de vista veritatiu, es comporten igual que les proposicions. I això fa que puguem combinar condicions com ho fem amb les proposicions (fer negacions: '`not` p', conjuncions: 'p `and` q', disjuncions: 'p `or` q'). Les condicions, com '$3 = 3$', que sempre són vertaderes es representen genèricament per '`true`'. De manera anàloga '`false`' és la condició que no es compleix mai.

Especifiqueu en quines circumstàncies s'executen cadascun dels conjunts d'instruccions en les instruccions següents.

1)
```
if p then I1 else (if q then I2 endif) endif
```

2)
```
if p then I1 else (if q then I2 else I3 endif) endif
```

3)
```
if p then I1
   else if q then I2
           else (if r then I3 else I4 endif)
        endif
endif
```

4)
```
if p then (if q then I1 else I2 endif)
   else
     I3
endif
```

5)
```
if p then
      if (p and q) then I1
         else (if (not q) then I2 endif)
      endif
endif
```

6)
```
if p then (if (p or q) then I1 endif)
   else if ((q or (not p)) and false) then I2
           else I3
        endif
endif
```

7)
```
if (p or true) then
                (if (p and true) then I1 else I2 endif)
   else I3
endif
```

1.12 Considerem els següents predicats:

D: saber dibuixar
E: saber escriure
J: saber jugar
N: ser nen

Considerem les proposicions següents:

a) $\forall x(N(x) \wedge J(x) \to \neg D(x))$

b) $\exists x(N(x) \wedge E(x) \wedge \neg D(x))$

Realitzeu les tasques següents en l'ordre que s'indica:

1) expresseu en català les proposicions a) i b);

2) negueu directament en català les frases que obtingueu al punt 1);

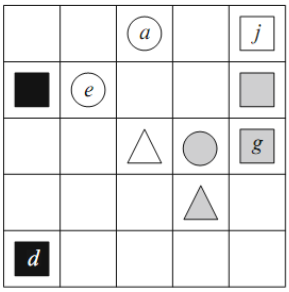


Figura 1.1: Món de Tarski

3) formalitzeu les frases que obtingueu al punt 2) usant els predicats del principi;

4) negueu les proposicions a) i b), expresseu el resultat en català i compareu els resultats amb els obtinguts al punt 3).

Considerem les frases següents:

a) Tots els nens que saben dibuixar i escriure també saben jugar.

b) Hi ha nens que saben jugar però no saben ni dibuixar ni escriure.

Realitzeu les tasques següents en l'ordre que s'indica:

1) formalitzeu les frases a) i b) usant els predicats donats al principi;

2) negueu les proposicions que heu obtingut al punt 1);

3) expresseu en català les proposicions que obteniu al punt 2);

4) negueu directament en català les frases a) i b), formalitzeu els resultats i compareu-los amb els results del punt 3).

1.13 Un món de Tarski està format per una graella i diverses formes geomètriques que poden portar una etiqueta i un color. Considerem el predicats següents:

$T(x)$: x és un triangle
$C(x)$: x és un cercle
$Q(x)$: x és un quadrat
$B(x)$: x és blanc
$N(x)$: x és negre
$G(x)$: x és gris
$E(x, y)$: x està a l'esquerra de y
$S(x, y)$: x està a sobre de y
$K(x, y)$: x té el mateix color que y

Donat el món de la figura 1.1 i usant els predicats indicats, formalitzeu les frases següents:

a) Hi ha un quadrat negre.

b) Tots els cercles són blancs;

c) No hi ha cap cercle negre.

d) a està a sobre de e.

e) Tots els cercles estan a sobre de d.

f) Hi ha un cercle que té el mateix color que d.

g) d està a l'esquerra de qualsevol cercle.

h) Alguna forma geomètrica és blanca.

i) Algun cercle és blanc.

j) Tots els quadrats són negres.

k) Tots els triangles estan a l'esquerra de d.

l) Hi ha un triangle a l'esquerra de d.

m) Hi ha un triangle que està a sobre de d però no a l'esquerra de a.

n) Algun triangle no és gris.

o) Tot triangle està o bé a l'esquerra de a o a sobre de b.

p) Cap quadrat té el mateix color que b.

Per a cadascuna d'aquestes proposicions, trobeu la seva negació de dues maneres diferents: negant directament la proposició en llenguatge natural i després negant la formalització obtinguda. Compareu els resultats.

1.14 Donat el món de la figura 1.1 i usant els predicats del problema 1.13, expresseu en llenguatge natural les proposicions següents i determineu si són certes o falses:

a) $\forall x\,(B(x) \to (T(x) \vee Q(x))$

b) $\forall x\,(N(x) \to (T(x) \vee Q(x))$

c) $\exists y\,(C(y) \wedge \neg S(y,d))$

d) $\exists y\,(C(y) \wedge S(y,d))$

e) $\exists y\,(C(y) \wedge \neg E(y,g))$

f) $\forall x\,(T(x) \to \exists y\,(Q(y) \wedge K(x,y)))$

Per a cadascuna d'aquestes proposicions, trobeu la seva negació i expresseu aquesta negació en llenguatge natural.

1.15 En aquest exercici suposem que totes les variables prenen valors enters. A més de les variables, connectives lògiques i quantificadors, podeu utilitzar només els símbols següents:

$$|, \quad <, \quad \cdot, \quad =, \quad +, \quad P, \quad Q, \quad 0,1,2,3,\ldots$$

$x|y$ per a formalitzar 'x divideix y' (o 'y és múltiple de x'); $P(x)$ formalitza 'x és primer'; $Q(x)$ formalitza 'x és un quadrat'.

Formalitzeu els enunciats següents.

1) 1 no és primer.

2) Tot enter múltiple de 6 és també múltiple de 3 i de 2.

3) Tot enter múltiple de 3 i de 5 és múltiple de 15.

4) x és un nombre parell (amb una variable lliure: la x).

5) 2 és primer i és parell.

6) Cap nombre primer és un quadrat.

7) Tot quadrat parell és múltiple de 4.

8) Hi ha nombres senars que són primers i d'altres senars que no són primers.

9) La suma de dos senars és parell.

10) Tot nombre parell més gran que 2 és suma de dos primers.

11) Tot enter positiu és suma de quatre quadrats.

1.16 En aquest exercici suposem que totes les variables prenen valors enters. A més de les variables, connectives lògiques i quantificadors, **només** podeu utilitzar els símbols següents:

$$<\,, \quad \cdot, \quad =\,, \quad +\,, \quad 0, 1, 2, 3, \ldots$$

Formalitzeu els enunciats següents:

1) x divideix y (x, y són variables lliures).

2) x és un quadrat (x variable lliure).

3) x és un nombre primer (x variable lliure).

4) 2 és l'únic nombre primer parell.

5) 2 és el nombre primer més petit.

6) Hi ha infinits nombres primers (pista: sempre n'hi un més gran que un donat).

7) Tots els apartats de l'exercici 1.15.

1.17 Quins dels enunciats següents són certs i quins són falsos? Justifiqueu les respostes.

1) $\exists x \in \mathbb{R}\,(x > 2 \wedge x < 5)$;

2) $\exists x \in \mathbb{R}\,(x < 3 \wedge x > 6)$;

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

4) $\exists x \in \mathbb{Z}\,(x$ és senar $\wedge$ x és un cub perfecte);

5) $\forall x, y \in \mathbb{R}\,(x > 0 \to (\exists\, n \in \mathbb{Z}\,(y \leq nx)))$;

6) $\forall\, x \in \mathbb{Z}\, \exists\, y \in \mathbb{R}\,(x = y^2)$.

Negueu cada un dels enunciats anteriors.

1.18 Determineu si els enunciats següents són certs o falsos i justifiqueu les respostes:

1) $\forall x \in \mathbb{Z}\, \exists y \in \mathbb{Z}\,(xy = 0)$;

2) $\forall x \in \mathbb{Z}\, \exists y \in \mathbb{Z}\,(xy = 1)$;

3) $\exists y \in \mathbb{Z}\, \forall x \in \mathbb{Z}\,(xy = 1)$;

4) $\exists y \in \mathbb{Z}\, \forall x \in \mathbb{Z}\,(xy = x)$;

5) $\forall x \in \mathbb{Q}\, \exists y \in \mathbb{Q}\,(xy = 1)$;

6) $\exists y \in \mathbb{Q}\, \forall x \in \mathbb{Q} - \{0\}\,(xy = 1)$.

Negueu cada un dels enunciats anteriors.

1.19 Digueu quines dels enunciats següents són certes i justifiqueu les respostes.

1) $\forall n, m \in \mathbb{Z}\,(\ nm$ és senar $\ \to\ n$ és senar $\wedge\ m$ és senar)'.

2) $\forall n, m \in \mathbb{Z}\,(\ n$ és senar $\wedge\ m$ és senar $\ \to\ nm$ és senar)'.

3) $\forall\, a, b \in \mathbb{Z}\,(a \cdot b$ parell $\ \to\ a$ parell $\wedge\ b$ parell).

4) $\forall\, b, c \in \mathbb{Z}\,(b + c$ parell $\ \to\ b$ senar $\wedge\ c$ senar).

1.20 Demostreu les implicacions següents, on n és un nombre enter.

1) Si n és un nombre enter senar, llavors n^2 és també un nombre enter senar.

2) Si n és un nombre enter parell, llavors n^2 és també un nombre enter parell.

3) Si n^2 és un nombre enter parell, llavors n també és un nombre enter parell.

4) Si n^2 és un nombre enter senar, llavors n també és un nombre enter senar.

1.21 Proveu que:

1) el producte de dos nombres parells és un nombre parell;

2) el producte de dos nombres senars és un nombre senar;

3) el producte d'un nombre senar per un de parell és un nombre parell;

4) la suma de dos nombres racionals és un nombre racional;

5) el producte de dos nombres racionals és un nombre racional.

1.22 Proveu que la suma d'un nombre irracional i un nombre racional és un nombre irracional, usant la reducció a l'absurd.

1.23 Usant el mètode de reducció a l'absurd, proveu que la suma dels cubs de dos nombres enters consecutius no pot ser igual al cub de l'enter següent.

1.24 Siguin x, y nombres reals. És cert o fals que $||x| - |y|| = |x - y|$? Raoneu la resposta.

1.25 Demostreu que els nombres a i b són les solucions de l'equació $x^2 + px + q = 0$ si, i només si, $a + b = -p$ i $ab = q$.

1.26 Demostreu que $\sqrt{2}$ és irracional (demostreu que no hi ha cap nombre racional que elevat al quadrat doni 2).

1.27 Sigui n un nombre enter múltiple de 3. Demostreu que n és senar o un múltiple de 6.

1.28 Siguin n, m enters positius. Demostreu que els enunciats següents són equivalents.

a) $n < m$ b) $n^2 < m^2$

1.29 El valor absolut d'un nombre real x es defineix com:

$$|x| = \begin{cases} x & \text{si } x \geq 0 \\ -x & \text{si } x < 0 \end{cases}$$

Siguin n, m enters no nuls. Proveu que són equivalents:

a) $|n + m| = |n| + |m|$;

b) $n \cdot m > 0$;

c) $n \cdot |m|$ i $m \cdot |n|$ tenen el mateix signe.

1.30 Siguin x, y dos nombres reals positius. La mitjana aritmètica de x i y es defineix com $(x + y)/2$ i la mitjana geomètrica de x i y com $\sqrt{xy}$.

1) Demostreu que si $x < y$, llavors $x < \frac{x+y}{2} < y$ i $x < \sqrt{xy} < y$.

2) Suposem que m representa la mitjana aritmètica de x i y. Proveu que si $m = x$ o $m = y$, llavors $x = y$. Feu també el mateix amb la mitjana geomètrica.

3) Proveu que si $x \neq y$, llavors la mitjana geomètrica és estrictament menor que la mitjana aritmètica.

CAPÍTOL 2

INDUCCIÓ

2.1 Demostreu per inducció les fórmules següents:

1) $1+2+3+\cdots+n=\frac{n(n+1)}{2}$, si $n\geq 1$.

2) $1+2+2^2\cdots+2^n=2^{n+1}-1$, si $n\geq 0$.

3) $2-2\cdot 5+2\cdot 5^2-2\cdot 5^3+\cdots+2\cdot(-5)^{n-1}=\frac{1-(-5)^n}{3}$, si $n\geq 1$.

4) $1^2+2^2+\cdots+n^2=\frac{n(n+1)(2n+1)}{6}$, si $n\geq 1$.

2.2 Demostreu per inducció les desigualtats següents:

1) $n^2<2^n$, si $n\geq 5$.

2) $3^n<n!$, si $n\geq 7$.

3) $n!<n^n$, si $n\geq 2$.

4) $n^2-5n+6\geq 0$, si $n\geq 0$.

5) $\sum_{k=1}^{n}\frac{1}{k^2}<2-\frac{1}{n}$, si $n>1$.

6) $\sum_{k=1}^{2^n}\frac{1}{k}\leq n+1$, si $n\geq 0$.

2.3 Demostreu per inducció que:

1) 3 divideix a n^3+2n, per a tot n no negatiu;

2) 6 divideix a n^3-n, per a tot $n\geq 0$.

2.4 Demostreu per inducció que l'enter n^3+3n^2+2n és divisible per 6, per a tot enter $n\geq 0$.

2.5 Demostreu per inducció la fórmula $\displaystyle\prod_{k=2}^{n}\left(1-\frac{1}{k}\right)=\frac{1}{n}$, si $n\geq 2$.

2.6 Demostreu per inducció la fórmula $\displaystyle\sum_{k=1}^{n}k2^k=(n-1)2^{n+1}+2$, si $n>1$.

2.7 Demostreu per inducció les fórmules següents.

1) $\displaystyle\sum_{i=1}^{n}i\cdot i!=(n+1)!-1$, si $n\geq 1$.

2) $\displaystyle\sum_{\ell=1}^{n}\frac{1}{\ell(\ell+1)}=\frac{n}{n+1}$, si $n\geq 1$.

3) $\displaystyle\sum_{k=1}^{n}\frac{1}{(2k-1)(2k+1)}=\frac{n}{2n+1}$, si $n\geq 1$.

4) $\displaystyle\sum_{i=0}^{n}\frac{1}{2i+1}<\frac{n}{3}+1$, $n\geq 2$.

2.8 Proveu per inducció que si $n\geq 1$, llavors $\dfrac{(2n)!}{n!2^n}\in\mathbb{Z}$.

2.9 Una progressió aritmètica és una successió $(a_n)_{n\geq 0}$ de nombres reals tal que cada terme a_n s'obté sumant al terme anterior a_{n-1} un nombre real fix d (la diferència de la progressió). És a dir: $a_n=a_{n-1}+d$, per a tot $n\geq 1$.

1) Trobeu el terme general $a_n = f(n)$ en funció de n i demostreu per inducció que és correcta.

2) Demostreu per inducció la fórmula següent per la suma dels n primers termes d'una progressió aritmètica:

$$\sum_{k=0}^{n-1} a_k = \frac{(a_0 + a_{n-1})n}{2}.$$

2.10 Una progressió geomètrica és una successió $(a_n)_{n\geq 0}$ de nombres reals tal que cada terme a_n s'obté multiplicant el terme anterior a_{n-1} per un nombre real fix r (la raó de la progressió). És a dir: $a_n = a_{n-1} \cdot r$, per a tot $n \geq 1$.

1) Trobeu el terme general $a_n = f(n)$ en funció de n i demostreu per inducció que és correcta.

2) Demostreu per inducció la fórmula següent per la suma dels n primers termes d'una progressió geomètrica:

$$\sum_{k=0}^{n-1} a_k = \frac{a_{n-1}r - a_0}{r-1},$$

si $r \neq 1$. Quan val aquesta suma si $r = 1$?

2.11 Demostreu per inducció que la suma dels angles interiors d'un polígon convex de n costats és $180°(n-2)$, si $n \geq 3$.

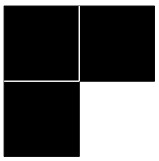
2.12 Proveu per inducció que el nombre de diagonals d'un polígon convex de $n \geq 4$ costats és $n(n-3)/2$.

2.13 Calculeu les potències A^n de la matriu següent per $1 \leq n \leq 5$:

$$A = \begin{bmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 1 & 1 & 1 \end{bmatrix}$$

Trobeu una expressió per A^n i demostreu per inducció que és correcta.

2.14 Sigui n un enter positiu. Demostreu per inducció que si d'un taulell d'escacs de mida $2^n \times 2^n$ traiem un quadrat 1×1, llavors el taulell que resulta es pot recobrir utilitzant peces com les de la figura:



2.15 Considereu la successió recurrent $u_0 = 0$, $u_1 = 1$, $u_n = 5u_{n-1} - 6u_{n-2}$, si $n \geq 2$. Proveu per inducció que $u_n = 3^n - 2^n$, per a tot $n \geq 0$.

2.16 Demostreu per inducció que els termes de la successió de Fibonacci:

$$F_0 = 0, \quad F_1 = 1, \quad F_n = F_{n-1} + F_{n-2}, \quad n \geq 2,$$

satisfan la fórmula $F_n = (\alpha^n - \beta^n)/\sqrt{5}$, si $n \geq 0$, on $\alpha = (1+\sqrt{5})/2$ i $\beta = (1-\sqrt{5})/2$.

2.17 Sigui $n \geq 2$. Sigui S una variable on acumulem els resultats d'unes operacions. Comencem amb $S = 0$ i escrivim $n = n_1 + n_2$ (suma de dos summands), on $n_1, n_2 \in \mathbb{N}$, i afegim a S el producte $n_1 \cdot n_2$. Ara fem el mateix amb $n_1 = n_{1,1} + n_{1,2}$ i $n_2 = n_{2,1} + n_{2,2}$, on $n_{i,j} \in \mathbb{N}$, i afegim a S els productes $n_{1,1} \cdot n_{1,2}$ i $n_{2,1} \cdot n_{2,2}$. I així successivament fins que només quedin uns com a summands. Proveu que si $n \geq 2$, llavors la suma S és igual a $n(n-1)/2$.

Exemple: $n = 7 = 4 + 3$, $S = 12$; $4 = 2 + 2$ i $3 = 1 + 2$, $S = 12 + 4 + 2 = 18$; finalment, $2 = 1 + 1$, $2 = 1 + 1$, $2 = 1 + 1$ i $S = 18 + 1 + 1 + 1 = 21 = 7 \cdot (7-1)/2$.

CAPÍTOL 3

CONJUNTS

3.1 Determineu si els enunciats següents són certs o falsos:

1) $\exists x(x \in \emptyset)$ 2) $\forall x(x \in \emptyset)$ 3) $\forall x(x \notin \emptyset)$ 4) $\exists x(x \notin \emptyset)$

3.2 L'enunciat 'Existeix un conjunt A tal que $A \subseteq \emptyset$':

1) és cert, per exemple $A = \emptyset$.
2) és fals, perquè $\emptyset$ no té elements.
3) és fals, perquè $\emptyset$ no té subconjunts.
4) és cert, ja que tot conjunt A és subconjunt de $\emptyset$.

3.3 Sigui $A_1 = \{1, \{2\}\}$, $A_2 = \{1, 2\}$, $A_3 = \{\{1\}, \{2\}\}$, $A_4 = \{1\}$, $A_5 = \{1, \{1\}, \{2\}\}$, $A_6 = \{1, \emptyset\}$. Quins d'aquests conjunts estan inclosos en algun altre? N'hi ha algun que sigui element d'un altre?

3.4 Siguin $X = \{1, 2, 3, 4\}$, $Y = \{\{1, 2\}, \{3, 4\}\}$, $Z = \{\{1\}, \{2, 3\}, \{4\}\}$. Quines de les següents afirmacions són vertaderes i quines són falses?

1) $1 \in X$, $1 \in Y$, $1 \in Z$
2) $\{1\} \in X$, $\{1\} \in Y$, $\{1\} \in Z$, $\{1\} \subseteq X$, $\{1\} \subseteq Y$, $\{1\} \subseteq Z$
3) $\{3, 4\} \in X$, $\{3, 4\} \in Y$, $\{3, 4\} \in Z$, $\{3, 4\} \subseteq X$, $\{3, 4\} \subseteq Y$, $\{3, 4\} \subseteq Z$

3.5 Siguin S i T conjunts. Relacioneu les propietats de l'esquerra amb les propietats de la dreta.

a) Tot objecte de qualsevol d'ells és de l'altre.
b) Existeix un x de T.
c) Tot objecte de S és de T.
d) No hi ha cap x de T que sigui de S.
e) No hi ha cap x en T.

1) $T \neq \emptyset$
2) $T = \emptyset$
3) $S \cap T = \emptyset$
4) $S \subseteq T$
5) $S = T$

3.6 Formula en llenguatge natural la negació de cada una de les afirmacions següents:

1) El conjunt A té, almenys, dos elements.
2) El conjunt A no té cap element.
3) El conjunt A té elements.
4) El conjunt A no té cap element del conjunt B.
5) El conjunt A i el conjunt B tenen elements en comú.

Escriu les frases anteriors usant la notació conjuntista; és a dir, usant $=$, $\in$, quantificadors i connectius lògics.

3.7 Sigui $X = \{\emptyset, 1, \{1\}, 2, \{1, 2\}\}$. Calculeu tots els elements del conjunt:

$\{x : x \in X \wedge x \subseteq X\}$.

3.8 Siguin A, B, C conjunts arbitraris. Indiqueu si els enunciats que segueixen són vertaders o falsos. Doneu una demostració si l'enunciat és vertader i un contraexemple si és fals.

1) Si $A \cup B = \emptyset$, llavors $A = B = \emptyset$

2) Si $A \cap B = \emptyset$, llavors $A = \emptyset$ o $B = \emptyset$

3) Si $A \cap B = A \cap C$, llavors $B = C$

4) Si $A \cup B = A \cup C$, llavors $B = C$

5) Si $A \cap B = C \cap D$, llavors $(A = C \wedge B = D)$ o $(A = D \wedge B = C)$

6) $A \setminus (A \cap B) = A \setminus B$

7) $A \cap (A \setminus B) = A \setminus B$

8) $A \setminus (A \setminus B) = A \cap B$

9) $(A \setminus B) \cup B = A \cup B$

10) $(A \cup B) \setminus B = A$

11) $(A \cup B) \setminus (A \setminus B) = B$

12) $(A \cup B) \setminus (A \cap B) = (A \setminus B) \cup (B \setminus A)$

13) $A \setminus (B \cup C) = (A \setminus B) \cup (A \setminus C)$

14) $A \setminus (B \cap C) = (A \setminus B) \cap (A \setminus C)$

3.9 Siguin A, B, C subconjunts d'un conjunt Ω. Indiqueu si els enunciats que segueixen són vertaders o falsos. Doneu una demostració si l'enunciat és vertader i un contraexemple si és fals.

1) $(A \setminus B) \cup B^c = A \cup B^c$

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

3) $A \subseteq B$ si, i només si, $A^c \cup B = \Omega$

4) $(A \setminus B)^c = A^c \cup B$

3.10 Siguin A i B conjunts tals que $A \cup B = A \cap B = B$. Què podem dir de A i de B? Justifiqueu la resposta.

3.11 Sigui Ω un conjunt no buit i $A \subseteq \Omega$ i $B \subseteq \Omega$ tals que $A \cap B = \emptyset$, $A \cup B = \Omega$. Què podem dir de A i de B? Justifiqueu la resposta.

3.12 Demostreu que:

1) $A \times (B \cap C) = (A \times B) \cap (A \times C)$

2) $A \times (B \cup C) = (A \times B) \cup (A \times C)$

3) $A \times (B \setminus C) = (A \times B) \setminus (A \times C)$

3.13 Calculeu els conjunts $\mathcal{P}(X)$, $\mathcal{P}(\mathcal{P}(X))$ i $\mathcal{P}(\mathcal{P}(\mathcal{P}(X)))$, si $X = \{a\}$.

3.14 Sigui $A = \{0, 1, \{1\}\}$. Calculeu $\mathcal{P}(A)$.

3.15 Demostreu que el nombre de subconjunts d'un conjunt de cardinal n és 2^n.

1) Feu una demostració per inducció.

2) Feu una demostració utilitzant els nombres binomials.

3.16 Siguin A i B conjunts no buits.

1) Proveu que $\mathcal{P}(A \cap B) = \mathcal{P}(A) \cap \mathcal{P}(B)$.

2) Proveu que $\mathcal{P}(A) \cup \mathcal{P}(B) \subseteq \mathcal{P}(A \cup B)$. És certa la igualtat? Justifiqueu la resposta.

3) És cert que $\mathcal{P}(A - B) = \mathcal{P}(A) - \mathcal{P}(B)$? Justifiqueu la resposta.

3.17 Considerem R la següent relació definida a $\mathbb{Z}$: aRb si, i només si, $ab \neq 0$. Estudieu quines propietats té R.

3.18 Determineu totes les particions del conjunt $X = \{a, b, c, d\}$. *Pista*: hi ha 15 particions diferents.

3.19 Sigui A un conjunt no buit. Definiu una relació d'equivalència en A tal que totes les classes d'equivalència tinguin exactament un element; és a dir, per a tot $a \in A$, $[a] = \{a\}$. Quin és el conjunt quocient?

3.20 Sigui A un conjunt no buit. Definiu una relació d'equivalència en A respecte de la qual només hi hagi exactament una classe d'equivalència. Quin és el conjunt quocient?

3.21 Sigui $A = \mathbb{Z} \setminus \{0\}$. Definim a A la relació:

$$xRy \iff x \cdot y > 0, \qquad (x, y \in A)$$

1) Proveu que R és una relació d'equivalència a A.

2) Descriviu classes d'equivalència i el conjunt quocient A/R.

3.22 Definim a $\mathbb{R}$ la relació:

$$xRy \iff x - y \in \mathbb{Z}.$$

1) Proveu que R és una relació d'equivalència a $\mathbb{R}$.

2) Descriviu les classes d'equivalència i el conjunt quocient $\mathbb{R}/R$.

3.23 Definim a $\mathbb{Z} \times \mathbb{Z}$ la relació:

$$(x, y)R(x', y') \iff xy = x'y'.$$

1) Proveu que R és una relació d'equivalència a $\mathbb{Z} \times \mathbb{Z}$.

2) Descriviu les classes d'equivalència i el conjunt quocient $(\mathbb{Z} \times \mathbb{Z})/R$.

3.24 Sigui $\mathcal{P}$ el conjunt de punts del pla i fixem un punt $O \in \mathcal{P}$. Definim a $\mathcal{P}^* = \mathcal{P} \setminus \{O\}$ la relació:

$$P \sim P' \iff O, P, P' \text{ estan alineats.}$$

1) Proveu que $\sim$ és una relació d'equivalència a $\mathcal{P}^*$.

2) Descriviu les classes d'equivalència i el conjunt quocient $\mathcal{P}^*/\sim$.

3.25 Siguin X i U dos conjunts tals que $U \subseteq X$. A $\mathcal{P}(X)$ definim la relació:

$$A \; R \; B \iff A \cap U = B \cap U,$$

on $A, B \in \mathcal{P}(X)$.

1) Proveu que R és una relació d'equivalència a $\mathcal{P}(X)$.

2) Descriviu les classes d'equivalència.

3) Calculeu el conjunt quocient si $X = \{1, 2, 3, 4, 5\}$ i $U = \{1, 5\}$.

3.26 Definim a $\mathbb{Z}$ la relació:

$$a \, R \, b \iff a^2 + a = b^2 + b.$$

Proveu que és una relació d'equivalència i descriviu les classes d'equivalència.

3.27 Considerem el conjunt $A = (\mathbb{Z} - \{0\}) \times (\mathbb{Z} - \{0\})$ i la relació R sobre A definida per:

$$(a, b) \, R \, (c, d) \iff a \cdot d = b \cdot c,$$

on $(a, b), (c, d) \in A$.

1) Demostreu que R és una relació d'equivalència sobre A.

2) Trobeu la classe d'equivalència de l'element $(a, b) \in A$.

3) Doneu una descripció del conjunt quocient A/R.

3.28 Considerem en $\mathbb{R} \times \mathbb{R}$ la relació següent:

$$(x, y) R (z, t) \text{ si, i només si, } |x| + |y| = |z| + |t|.$$

1) Proveu que R és una relació d'equivalència.

2) Assenyaleu, en el pla, quins són els elements de la classe de $(1, 0)$. Raoneu la resposta.

3.29

1) Sigui A un conjunt no buit i R una relació reflexiva i transitiva en A. Demostreu que la relació S definida per:

$$x \, S \, y \iff (x \, R \, y \wedge y \, R \, x)$$

és d'equivalència.

2) Sigui $\mathcal{P}$ el conjunt de punts del pla i considerem un punt $O \in \mathcal{P}$. Definim a $\mathcal{P}$ la relació R següent:

$$X \, R \, Y \iff d(X, O) \leq d(Y, O)$$

a) Proveu que R és una relació reflexiva i transitiva.

b) Trobeu les classes d'equivalència per la relació S associada a R segons l'apartat 1).

3.30 Considerem en el conjunt $A = \mathbb{Z} - \{0\}$ la relació R següent:

$$\begin{aligned} mRn \iff & (\text{sgn}(n) = \text{sgn}(m) \wedge \text{paritat}(n) = \text{paritat}(m)) \vee \\ & (\text{sgn}(n) \neq \text{sgn}(m) \wedge \text{paritat}(n) \neq \text{paritat}(m)) \end{aligned}$$

1) Proveu que R és una relació d'equivalència.

2) Trobeu les classes d'equivalència de l'element 1 i de l'element 2. Raoneu la resposta.

3) Expliciteu el conjunt quocient A/R. Raoneu la resposta.

3.31

1) Sigui X un conjunt no buit i siguin R i S relacions d'equivalència definides sobre X. Demostreu que la relació T definida per:

$$xTy \iff xRy \wedge xSy$$

és una relació d'equivalència sobre X.

2) Sigui $X = \{n \in \mathbb{N} : 1 \leq n \leq 10\}$. Construïu dues relacions d'equivalència R i S sobre X diferents. És la següent relació U definida sobre X:

$$xUy \iff xRy \vee xSy$$

una relació d'equivalència?

3.32 Donat un punt $(x, y) \in \mathbb{R}^2$, definim:

$$\operatorname{sgn}(x,y) = \begin{cases} -1, & \text{si } xy < 0 \\ 0, & \text{si } xy = 0 \\ +1, & \text{si } xy > 0 \end{cases}$$

Definim a $\mathbb{R}^2$ la relació R següent:

$$(x,y)R(u,v) \iff \operatorname{sgn}(x,y) = \operatorname{sgn}(u,v)$$

1) Proveu que R és una relació d'equivalència.

2) Trobeu totes les classes d'equivalència.

3) Trobeu el conjunt quocient.

3.33 Sigui R una relació d'equivalència en un conjunt A. Donats a i b elements de A, demostrar l'equivalència de les afirmacions següents:

1) $[a] \cap [b] \neq \emptyset$

2) $a \in [b]$

3) $[a] \subseteq [b]$

CAPÍTOL 4

APLICACIONS

4.1 Sigui $g\colon \mathbb{R} \to \mathbb{R}$ l'aplicació definida per $g(x) = \lfloor x \rfloor$. Calculeu:

1) $g^{-1}[\{0\}]$ 2) $g^{-1}[\{-1, 0, 1\}]$ 3) $g^{-1}[\{x \in \mathbb{R} : 0 < x < 1\}]$

Recordeu que: $\lfloor x \rfloor = \max\{k \in \mathbb{Z} : k \leq x\}$, si $x \in \mathbb{R}$.

4.2 Considereu l'aplicació $f\colon \mathbb{R} \to \mathbb{R}$ definida per:

$$f(x) = \begin{cases} x^2 - 4x, & \text{si } x \geq 0 \\ x, & \text{si } x < 0 \end{cases}$$

1) Calculeu $f[S]$ si $S = \{-2, 0, 2, 4, 5\}$.

2) Calculeu $f^{-1}[\{2\}]$ i $f^{-1}[\{-3\}]$.

3) Estudieu si f és injectiva, exhaustiva, bijectiva.

4.3 Considerem l'aplicació:

$$f : \mathbb{R} \setminus \{-1, 1\} \to \mathbb{R} \setminus \{0\}, \qquad f(x) = \frac{1}{x^2 - 1}.$$

Proveu que f està ben definida. Estudieu si f és injectiva. Estudieu si f és exhaustiva.

4.4 Determineu si les aplicacions de $\mathbb{Z}$ en $\mathbb{Z}$ següents són injectives, exhaustives o bijectives.

1) $f(n) = n - 1$ 2) $f(n) = n^2 + 1$ 3) $f(n) = n^3$ 4) $f(n) = \lceil n/2 \rceil$

Recordeu que: $\lceil x \rceil = \min\{k \in \mathbb{Z} : x \leq k\}$, si $x \in \mathbb{R}$.

4.5 Definiu explícitament una aplicació de $\mathbb{Z}$ en $\mathbb{N}$ que sigui:

1) exhaustiva, però no injectiva;

2) injectiva, però no exhaustiva;

3) injectiva i exhaustiva;

4) ni injectiva ni exhaustiva.

4.6 Sigui $f : \mathbb{R} - \{7\} \to \mathbb{R} - \{5\}$ l'aplicació definida per:

$$f(x) = \frac{5x}{x - 7}$$

Proveu que és bijectiva i trobeu la seva inversa.

4.7 Siguin $f, g\colon \mathbb{Z} \to \mathbb{Z}$ les aplicacions definides per:

$$f(n) = 2n, \qquad g(n) = \begin{cases} n/2, & \text{si } n \text{ és parell} \\ 34, & \text{si } n \text{ és senar} \end{cases}$$

respectivament. Proveu que $g \circ f = \mathrm{I}_{\mathbb{Z}}$, però que f i g no són inverses una de l'altra.

4.8 Considerem el conjunt $X = \{n \in \mathbb{N} : 1 \leq n \leq 100\}$ i l'aplicació $f\colon X \to X$ definida per:

$$f(n) = \begin{cases} 2n, & \text{si } 1 \leq n \leq 50 \\ 2(n-51)+1, & \text{si } 51 \leq n \leq 100 \end{cases}$$

1) Proveu que f és una aplicació bijectiva.

2) Calculeu $f^{-1}[S]$, si $S = \{n \in X : n \text{ senar}\}$. Justifiqueu la resposta.

3) Comproveu que $f[f^{-1}[P]] = P$, si $P = \{n \in X : n \text{ parell}\}$. Justifiqueu la resposta.

4.9 Considerem l'aplicació $f\colon \mathbb{N} \to \mathbb{N}$ definida per:

$$f(n) = \begin{cases} n, & \text{si } n \text{ és parell} \\ n+1, & \text{si } n \text{ és senar} \end{cases}$$

1) Proveu que $f \circ f = f$.

2) Calculeu $f[\{1,2,3,4\}]$. Deduïu que f no és injectiva.

3) Calculeu $f^{-1}[\{0,1,2\}]$. Deduïu que f no és exhaustiva.

4.10 Considerem l'aplicació $f\colon \mathbb{Z} \to \mathbb{N}$ definida per:

$$f(n) = \begin{cases} 2n-1, & \text{si } n > 0 \\ -2n, & \text{si } n \leq 0 \end{cases}$$

1) Calculeu $f[\{-2,-1,0,1,2\}]$ i $f[\{-5,-3,0,3,5\}]$.

2) Calculeu $f^{-1}[\{0,1,2\}]$ i $f^{-1}[\{0,3,6\}]$

3) Proveu que f és injectiva.

4) Proveu que f és exhaustiva.

4.11 Sigui $f : \mathbb{N} \to \mathbb{N}$ l'aplicació definida per:

$$f(n) = \begin{cases} n+1, & \text{si } n \text{ és parell} \\ 2n, & \text{si } n \text{ és senar} \end{cases}$$

1) Calculeu $f \circ f$.

2) Proveu que f és injectiva.

3) Proveu que f no és exhaustiva.

4) Calculeu $f^{-1}[\{m\}]$, per a $m \in \mathbb{N}$.

4.12 Siguin A, B conjunts no buits. Proveu que l'aplicació $g\colon A \times B \to A$ definida per $g\big((x,y)\big) = x$ és exhaustiva.

4.13 Siguin A, B conjunts no buits i $b_0 \in B$ un element fix. Proveu que l'aplicació $h\colon A \to A \times B$ definida per $h(x) = (x, b_0)$ és injectiva.

4.14 Doneu exemples d'aplicacions $f\colon A \to B$ i $g\colon B \to C$ tals que:

1) la composició $g \circ f$ és injectiva, però g no ho és;

2) la composició $g \circ f$ és exhaustiva, però f no ho és.

4.15 Siguin A i B conjunts no buits i $f : A \to B$ una aplicació de A en B. Definim, en A, la relació següent: $xRx' \iff f(x) = f(x')$.

1) Demostreu que R és una relació d'equivalència.

2) Considerem l'aplicació $f : \mathbb{R} \to \mathbb{R}$ definida per $f(x) = \lfloor x \rfloor$ (part entera). Descriviu les classes d'equivalència i el conjunt quocient $\mathbb{R}/R$ en aquest cas. Establiu una aplicació bijectiva entre $\mathbb{R}/R$ i $\mathbb{Z}$.

4.16

1) Siguin $f : \mathbb{N} \to \mathbb{N}$ una aplicació injectiva. Demostreu que l'aplicació $g : \mathbb{N} \to \mathbb{N}$ definida per $g(n) = 2f(n)$ també és injectiva.

2) Sigui $f : \mathbb{Z} \to \mathbb{Z}$ una aplicació exhaustiva. Demostreu que l'aplicació $g : \mathbb{Z} \to \mathbb{Z}$ definida per $g(n) = f(n+1)$ també és exhaustiva.

CAPÍTOL 5

ENTERS: DIVISIBILITAT

5.1 Per a cadascuna de les divisions següents, doneu el quocient i el residu.

1) 19 entre 7;
2) 0 entre 27;
3) -1 entre 8;
4) -111 entre 11;
5) -111 entre -13;
6) 1325 entre -15.

5.2 Descomponeu en factors primers els enters següents:

1) 143 2) 101 3) 289 4) 899 5) 15!

5.3 Quins dels enters següents són nombres primers?

509, 5767, 29947, $2^{70}-1$, 12533

5.4 Trobeu el màxim comú divisor dels enters següents.

1) 10!, 3^{10}
2) 2^{100}, 100^2

5.5 Calculeu el màxim comú divisor dels nombres que s'indiquen i els coeficients x i y de la identitat de Bézout associada i comproveu que es corresponen amb els resultats de la taula.

a	b	$\mathrm{mcd}(a,b)$	x	y
7658	3853	1	-883	1755
9191	6987	1	-1975	2598
5548	1727	1	80	-257
3614	7752	2	1435	-669
1084	4904	4	-95	21
7084	3563	7	-85	169

a	b	$\mathrm{mcd}(a,b)$	x	y
9176	7084	4	640	-829
3419	9168	1	4403	-1642
7119	6966	9	-91	93
3643	8590	1	-3353	1422
1628	9613	1	-124	21
8304	1274	2	-83	541

5.6 Quin és el menor nombre enter positiu més gran que 7 que dividit per 8, 12 i 15 dóna residu 7?

5.7 Siguin p, q, r tres nombres primers diferents dos a dos. Calculeu tots els divisors positius del nombre enter pq^2r^3.

5.8 Prenem cinc nombres naturals qualssevol. Demostreu que sempre nŠhi ha almenys dos que donen el mateix residu en ser dividits per 4.

5.9 Demostreu que si 2^n-1 és un nombre primer, llavors n és un nombre primer. [Indicació: Useu la igualtat $2^{ab}-1=(2^a-1)(2^{a(b-1)}+2^{a(b-2)}+\cdots+2^a+1)$]

5.10 Diem que un nombre enter és *perfecte* si és igual a la suma dels seus divisors positius diferents d'ell.

1) Comproveu que 6 i 28 són nombres perfectes.

2) Demostreu que si $2^p - 1$ és primer, aleshores $2^{p-1}(2^p - 1)$ és un nombre perfecte.

5.11 Calculeu $\mathrm{mcd}(a, b)$ en els casos següents.

1) $b = 1$
2) $b = a + 1$
3) $b = a^2$
4) $b = na$
5) $b = a$
6) $b \mid a$
7) $b = a^n$
8) $b = \mathrm{mcd}(a, c)$
9) b és primer.

5.12 Calculeu $\mathrm{mcd}(a + b, a^2 - b^2)$, on a i b són enters.

5.13 Si $\mathrm{mcd}(a, b) = p$, on p és un nombre primer, digueu i justifiqueu quins són els possibles valors de $\mathrm{mcd}(a^2, b)$, $\mathrm{mcd}(a^3, b)$ i $\mathrm{mcd}(a^2, b^3)$. Si $\mathrm{mcd}(a, b) = p^3$, i p és un nombre primer, calculeu $\mathrm{mcd}(a^2, b^2)$.

5.14 Proveu que si n és un enter, llavors:

$$\mathrm{mcd}(n, n + 2) = \begin{cases} 1, & \text{si } n \text{ és senar;} \\ 2, & \text{si } n \text{ és parell.} \end{cases}$$

5.15 Proveu que $\mathrm{mcd}(2n + 5, 3n + 7) = 1$, si $n \geq 0$.

5.16 Calculeu els enters positius a, b tals que $a + b = 57$ i $\mathrm{mcm}(a, b) = 680$. [Indicació: proveu primer que $\mathrm{mcd}(a, b) = 1$.]

5.17 Siguin $a, n, p \in \mathbb{Z}$ tals que p és un nombre primer i $n > 0$.

1) Demostreu que si $p \mid a^n$, llavors $p \mid a$.

2) Demostreu que si $p \mid a^n$, llavors $p^n \mid a^n$.

Són certes les proposicions anteriors si p és un nombre compost?

5.18 Demostreu que si $a, b \in \mathbb{Z}$ i $3a^2 = b^2$, aleshores $3 \mid a$ i $3 \mid b$.

5.19 Siguin $a, b, c \in \mathbb{Z}$. Proveu l'equivalència següent:

$$\mathrm{mcd}(a, c) = 1 \wedge \mathrm{mcd}(b, c) = 1 \iff \mathrm{mcd}(ab, c) = 1.$$

5.20 Proveu que les proposicions següents són falses:

1) Per a tot $a, b, c \in \mathbb{Z}$, si $\mathrm{mcd}(a, b) = 1$ i $\mathrm{mcd}(b, c) = 1$, llavors $\mathrm{mcd}(a, c) = 1$.

2) Per a tot $a, b, c \in \mathbb{Z}$, si $\mathrm{mcd}(a, b) = 2$ i $\mathrm{mcd}(b, c) = 2$, llavors $\mathrm{mcd}(a, c) = 2$.

5.21 Si $a \in \mathbb{N}$ i p és un nombre primer, proveu que les afirmacions següents són equivalents:

1) $\mathrm{mcd}(a, p) = p$
2) $p|a$
3) $p|a^2$
4) $p^2|a^2$

5.22 Proveu que per a tot $n \in \mathbb{Z}$, existeixen enters a, b tals que $n = 5a + 7b$.

5.23 Proveu que si $a, b, c \in \mathbb{Z}$, llavors $\mathrm{mcd}(a, b) = \mathrm{mcd}(bc - a, b)$.

5.24 Siguin m, n enters positius.

1) Proveu que, en general, $\mathrm{mcd}(m, n) \neq \mathrm{mcd}(m - n, m + n)$.

2) Proveu que una condició suficient perquè $\mathrm{mcd}(m,n) = \mathrm{mcd}(m-n, m+n)$ és que m i n tinguin paritat diferent.

3) Proveu que la condició esmentada a l'apartat anterior no és necessària.

5.25 Considerem l'aplicació $f : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ definida per $f(x,y) = 52x + 21y$.

1) Comproveu que $\mathrm{mcd}(52, 21) = 1$ i escriviu la corresponent identitat de Bézout. Justifiqueu tots els passos.

2) Proveu que f és exhaustiva. (Pista: podeu feu servir l'apartat anterior.)

5.26 Si $n \in \mathbb{Z}$, definim el conjunt $M_n = \{x \in \mathbb{Z} : n \mid x\}$.

1) Siguin p i q nombres primers diferents. Proveu que $M_p \cap M_q = M_{pq}$.

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

3) És cert que per a tot enter n i tot enter m, es compleix $M_n \cap M_m = M_{nm}$? Justifiqueu la resposta.

5.27 Resoleu les equacions diofàntiques següents.

1) $12x + 18y = 30$
2) $2x + 3y = 4$
3) $6x + 8y = 25$
4) $22x - 31y = 41$
5) $12x + 13y = 14$
6) $28x - 91y = 119$
7) $1076x + 2076y = 3076$
8) $1776x - 1976y = 4152$
9) $-2x - 6y = 18$

5.28 Els graus Fahrenheit F i Celsius C estan relacionats per la fórmula:

$$F = \frac{9}{5}C + 32$$

Trobeu totes les solucions d'aquesta equació amb F i C enteres. *Indicació*: el zero absolut es correspon amb $-273.15°C$.

5.29 Calculeu totes les solucions enteres de l'equació $13x - 47y = 10$. Trobeu la solució (x, y) de l'equació anterior tal que y té el valor negatiu més gran possible.

5.30 Descomponeu de totes les maneres possibles el nombre racional $230/247$ en suma de dues fraccions positives de denominadors 19 i 13.

5.31 S'ha de començar a jugar un partit de futbol i només disposem de dos rellotges de sorra que mesuren 6 i 11 minuts, respectivament. És possible mesurar exactament els 45 minuts que ha de durar cada part? En cas afirmatiu, indiqueu totes les maneres possibles de fer-ho.

5.32 Li demaneu a un amic que multipliqui el dia que va néixer per 12 i el número del mes per 31 i que us digui el resultat de la suma d'aquestes quantitats. El resultat és 500. Esbrineu la data del seu aniversari.

CAPÍTOL 6

ENTERS: CONGRUÈNCIES

6.1

1) Classifiqueu els enters següents mòdul 4: $-12, -11, -9, -6, -4, -1, 0, 1, 2, 3, 4, 5, 7, 10$.

2) Classifiqueu els enters següents mòdul 7: $2, 16, 0, 43, 6, 97, -3, 32, -9, 13, -4, 235$.

6.2 Avalueu les quantitats següents:

1) $-17 \bmod 2$;
2) $-101 \bmod 13$;
3) $144 \bmod 4$;
4) $199 \bmod 19$;
5) $13 \bmod 3$;
6) $155 \bmod 19$;
7) $-97 \bmod 11$;
8) $-221 \bmod 23$.

6.3 Trobeu tots els nombres naturals m tals que $91 \equiv 271 \pmod{m}$.

6.4 Sigui p un nombre primer i $a, b \in \mathbb{Z}$.

1) Demostreu que si $a^2 \equiv b^2 \pmod{p}$, llavors $p \mid (a+b)$ o $p \mid (a-b)$.

2) Deduïu que les solucions de la congruència $x^2 \equiv 1 \pmod{p}$ són els enters x tals que $x \equiv 1 \pmod{p}$ o $x \equiv -1 \pmod{p}$.

3) És certa aquesta propietat si p és un nombre compost?

6.5

1) Proveu que si p és un primer senar, llavors $p \equiv 1 \pmod{4}$ o $p \equiv 3 \pmod{4}$.

2) Proveu que si $p \geq 5$ és un primer, llavors $p \equiv 1 \pmod{6}$ o $p \equiv 5 \pmod{6}$.

6.6 Demostreu les regles de divisibilitat següents:

1) n és múltiple de 3 si, i només si, la suma dels dígits de n mòdul 3 és 0.

2) n és múltiple de 5 si, i només si, el dígit de les unitats de n és 0 o 5.

3) n és múltiple de 9 si, i només si, la suma dels dígits de n mòdul 9 és 0.

4) n és múltiple de 11 si, i només si, la suma dels dígits de n que ocupen un lloc parell menys la suma dels dígits que ocupen un lloc senar és múltiple de 11.

6.7

1) Quina xifra entre 0 i 9 s'ha de posar en el lloc de la z en el nombre $9z86$ perquè en dividir-lo per 11 el residu sigui 5?

2) Quins valors entre 0 i 9 s'han de posar en el lloc de a i de b perquè el nombre $5a8b$ sigui divisible alhora per 2, 3, 5 i 11?

6.8 Calculeu un invers de:

1) 3 mòdul 11 2) 15 mòdul 28 3) 124 mòdul 141 4) 184 mòdul 223

6.9 Resoleu les congruències següents:

1) $8x \equiv 5 \pmod 9$
2) $3x \equiv 11 \pmod{17}$
3) $12x \equiv 7 \pmod{73}$
4) $553x \equiv 254 \pmod{400}$
5) $12x - 6 \equiv 7 \pmod{35}$
6) $x \equiv 6x + 4 \pmod{336}$
7) $48x \equiv 39 \pmod{17}$
8) $19x \equiv 29 \pmod{16}$
9) $132x+25 \equiv 2x+45 \pmod{131}$

6.10 Resoleu l'equació $\overline{31} \cdot \overline{x} = \overline{1}$ en el conjunt $\mathbb{Z}_{101}$.

6.11 Trobeu un enter x tal que $x \equiv -4 \pmod{17}$ i $x \equiv 3 \pmod{23}$.

6.12 Proveu que $11 \cdot 14^n + 1$ és compost, per a tot enter $n \geq 0$.

6.13 Proveu que, per a cap $n \in \mathbb{Z}$, l'enter $5n + 3$ és un quadrat.

6.14 Siguin a, m enters tals que $\mathrm{mcd}(a, m) = 2$. Proveu que existeix un enter x tal que $ax \equiv 2 \pmod m$.

6.15

1) Justifiqueu que $\mathbb{Z}_{173}$ és un cos.
2) Calculeu la classe inversa de $\overline{140} \in \mathbb{Z}_{173}$. Doneu el representant enter positiu més petit de la classe que heu trobat.
3) Resoleu el sistema d'equacions lineals següent a $\mathbb{Z}_{173}$:

$$\begin{aligned} \overline{22} \cdot \overline{x} + \overline{51} \cdot \overline{y} &= \overline{4} \\ \overline{12} \cdot \overline{x} - \overline{13} \cdot \overline{y} &= \overline{5} \end{aligned}$$

6.16 Proveu que per a tot $n \geq 0$ es compleix que:

1) $3^{2n+2} - 8n - 9$ és divisible per 64;
2) $7^{2n} - 48n - 1$ és divisible per 2304.

6.17 Proveu que per a tot $n \geq 1$ es compleix que:

1) $3 \cdot 4^n \equiv 3 \pmod 9$;
2) $9^n - 8n - 1 \equiv 0 \pmod{64}$;
3) $5^n + 2 \cdot 3^{n-1} + 1 \equiv 0 \pmod 4$;
4) $2n^3 + 3n^2 + n \equiv 0 \pmod 6$.

6.18 Sigui $A_n = 2^n + 2^{2n} + 2^{3n}$. Demostreu que per a tot $n > 0$ el nombre $A_{n+3} - A_n$ és múltiple de 7. Calculeu el residu de dividir A_{2011} per 7.

6.19 Sigui $n \geq 1$ un enter. Demostreu que si $\mathrm{mcd}(a, n) = 1$, aleshores l'aplicació:

$$f\colon \mathbb{Z}_n \to \mathbb{Z}_n, \qquad f(\overline{x}) = \overline{a} \cdot \overline{x}$$

és bijectiva.

6.20 Considerem l'aplicació $f\colon \mathbb{Z}_{29} \to \mathbb{Z}_{29}$ definida per $f(\overline{x}) = \overline{22} \cdot \overline{x} + \overline{7}$

1) Proveu que f és bijectiva i trobeu la seva inversa.

2) Considerem l'alfabet de 29 símbols indicat a continuació i assignem a cada símbol el nombre que té a la dreta:

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

(espai)

Codifiquem cada frase escrita en l'alfabet anterior aplicant la regla de codificació $x \mapsto 22x+7 \pmod{29}$ al valor numèric corresponent a cadascun dels símbols. Per exemple 'AVUI' és '0 21 20 8' i es codificaria en '7 5 12 9', o sigui 'HFMJ', ja que $0 \mapsto 7$, $21 \mapsto 5$, $20 \mapsto 12$, $8 \mapsto 9$.

Si el resultat d'una codificació ha estat el missatge 'KZRT,AI' (el que hi ha entre les cometes), quin era el missatge original?

6.21

1) Proveu que la classe $\overline{2957}$ és invertible a $\mathbb{Z}_{4096}$ i trobeu la seva classe inversa. Justifiqueu i expliciteu tots els càlculs que feu per a arribar al resultat.

2) Comproveu que les aplicacions:

$$f\colon \mathbb{Z}_{4096} \to \mathbb{Z}_{4096}, \qquad f(\overline{x}) = \overline{2957} \cdot \overline{x}$$
$$g\colon \mathbb{Z}_{4096} \to \mathbb{Z}_{4096}, \qquad g(\overline{x}) = \overline{3909} \cdot \overline{x}$$

són inverses una de l'altra.

6.22 Trobeu totes les solucions de l'equació $\overline{x}^4 + \overline{10} \cdot \overline{x}^3 + \overline{3} \cdot \overline{x}^2 - \overline{9} \cdot \overline{x} - \overline{3} = \overline{0}$ a $\mathbb{Z}_{29}$.

6.23 Trobeu el residu de les potències indicades mòdul l'enter donat.

1) $3^{247} \pmod{17}$
2) $3^{181} \pmod{17}$
3) $23^{1001} \pmod{17}$
4) $2^{340} \pmod{341}$
5) $19^{1976} \pmod{23}$
6) $11^{2013} \pmod{13}$
7) $949794^{25863} \pmod{211}$
8) $34773^{4969} \pmod{151}$
9) $25^{1025} \pmod{251}$

6.24 Trobeu els dos últims digits decimals dels nombres 1776^{1976} i 1829^{1829} i l'últim digit de $1943^{1642^{1053}}$.

6.25 Calculeu:

1) $11^{16} + 17^{10}$ mòdul 187;
2) $13^{18} + 19^{12}$ mòdul 247.

6.26 Resoleu els sistemes lineals de congruències següents.

1) $x \equiv 2 \pmod 5$; $x \equiv 3 \pmod 7$
2) $x \equiv 3 \pmod 4$; $x \equiv 5 \pmod 9$
3) $x \equiv 4 \pmod 9$; $x \equiv 5 \pmod{13}$; $x \equiv 4 \pmod{17}$
4) $x \equiv 2 \pmod 3$; $x \equiv 4 \pmod 5$; $x \equiv 5 \pmod 7$
5) $x \equiv 1 \pmod 3$; $x \equiv 3 \pmod 4$; $x \equiv 4 \pmod 7$; $x \equiv 7 \pmod{11}$
6) $x \equiv 2 \pmod 4$; $x \equiv 3 \pmod 5$; $x \equiv 4 \pmod 9$; $x \equiv 5 \pmod{13}$

6.27 Una banda de 13 pirates s'apodera d'una caixa de monedes d'or. Després de repartir-les equitativament queda un residu de 8 monedes. Moren 2 pirates, es torna a repartir i es té un residu de 3 monedes. Desapareixen 3 pirates més, es torna a repartir i es té un residu de 5 monedes. Quin és, com a mínim, el botí dels pirates?

6.28 En una nau espacial hi viatgen 13 astronautes, amb por de marejar-se. Per això s'emporten pastilles contra el mareig. Veuen que si se les reparteixen entre tots en sobre 5. Quan passen per una estació espacial, baixen 5 astronautes que no s'emporten cap pastilla. Els que continuen el viatge veuen que si ara reparteixin les pastilles també en sobrarien 5. A l'altura de Saturn, un d'ells es mareja, es pren una pastilla i mor. Si els que queden es repartissin les pastilles en sobraria 1. Més tard, descobreixen que la mort va ser deguda a una al·lèrgia. Hi ha 2 astronautes que també en són d'al·lèrgics. Si els no al·lèrgics es reparteixen les pastilles no en sobra cap. Quin és el mínim nombre de pastilles?

6.29 Suposem que en un cert processador l'aritmètica amb enters més petits que 256 és fa de manera més ràpida que amb enters grans. Podem restringir els càlculs a enter més petits que 256 si representem els enters usant els seus residus mòdul un parell d'enters primers entre ells i més petits que 256.

Per exemple, podem usar els enters 255 i 254 com a mòduls per a representar de manera única tots els enters més petits que $255 \cdot 254 = 64770$, usant el teorema xinès dels residus. Així, 33221 es representa com el parell $(71, 201)$, ja que $33221 \equiv 71 \pmod{255}$ i $33221 \equiv 201 \pmod{254}$; i 22119 es representa com el parell $(189, 21)$. Per a calcular la suma de 33221 i 22113, treballem amb els parells en lloc de directament amb els enters: $(71, 201) + (189, 21) = (71 + 189 \mod 255, 201 + 21 \mod 254) = (5, 221)$. Ara, per a calcular quin enter està representat pel parell $(5, 221)$, hem de resoldre el sistema de congruències:

$$\begin{aligned} x &\equiv 5 \pmod{255} \\ x &\equiv 221 \pmod{254} \end{aligned}$$

1) Usant aquest mètode, calculeu $12345 + 23451$.

2) Desenvolupeu un mètode anàleg per a fer aritmètica amb enters més petits que $16386810 = 255 \cdot 254 \cdot 253$.

3) És possible fer el mateix amb els enters més petits que $4129476120 = 255 \cdot 254 \cdot 253 \cdot 252$? Per què?

CAPÍTOL 7

SOLUCIONS

7.1 Raonament

1.1 Fals.

1.2 1.

1.5 Siguin p, q, r lletres proposicionals. Que $((p \to q) \wedge (\neg p \to q)) \to (r \to q)$ sigui una tautologia vol dir que és certa sempre; és a dir, per a qualsevol valor de veritat que prenguin p, q i r. Podem fer, doncs, la taula de veritat i comprovar que la columna corresponent té sempre el valor 1 (cert).

p	q	r	$p \to q$	$\neg p \to q$	$(p \to q) \wedge (\neg p \to q)$	$r \to q$	t
0	0	0	1	0	0	1	1
0	0	1	1	0	0	0	1
0	1	0	1	1	1	1	1
0	1	1	1	1	1	1	1
1	0	0	0	1	0	1	1
1	0	1	0	1	0	0	1
1	1	0	1	1	1	1	1
1	1	1	1	1	1	1	1

Una altra solució: tenim les equivalències següents:

$$\begin{aligned}(p \to q) \wedge (\neg p \to q) &\equiv (\neg p \vee q) \wedge (p \vee q) && (1)\\ &\equiv (\neg p \wedge p) \vee q && (2)\\ &\equiv 0 \vee q && (3)\\ &\equiv q && (4)\end{aligned}$$

(1): hem usat que $a \to b \equiv \neg a \vee b$; (2): per la propietat distributiva; (3): $\neg p \wedge p$ és sempre falsa i la denotem per 0; (4): $0 \vee a \equiv a$.

Finalment, tenim:

$$\begin{aligned}((p \to q) \wedge (\neg p \to q)) \to (r \to q) &\equiv q \to (r \to q) && (1)\\ &\equiv \neg q \vee (\neg r \vee q) && (2)\\ &\equiv (\neg q \vee q) \vee \neg r && (3)\\ &\equiv 1 \vee \neg r && (4)\\ &\equiv 1\end{aligned}$$

(1): pel que acabem de veure més a dalt; (2): propietats commutativa i associativa de la disjunció; (3): $\neg q \vee q$ és una tautologia i la denotem per 1; (4): $1 \vee a \equiv 1$.

1.9 Tenim en compte les equivalències:

$$(p \leftrightarrow q) \equiv (p \to q) \wedge (q \to p),$$

$$(p \to q) \equiv (\neg p \vee q),$$
$$(p \wedge q) \equiv (p \wedge \neg\neg q) \equiv \neg(p \to \neg q)$$

i les lleis de De Morgan:

1)

$$\begin{aligned} p \leftrightarrow q &\equiv (p \to q) \wedge (q \to p) \\ &\equiv (\neg p \vee q) \wedge (\neg q \vee p) \\ &\equiv \neg(\neg(\neg p \vee q) \vee \neg(\neg q \vee p)) \end{aligned}$$

2)

$$\begin{aligned} p \leftrightarrow q &\equiv (p \to q) \wedge (q \to p) \\ &\equiv (\neg p \vee q) \wedge (\neg q \vee p) \\ &\equiv \neg(p \wedge \neg q) \wedge \neg(q \wedge \neg p) \end{aligned}$$

3) $p \leftrightarrow q \equiv (p \to q) \wedge (q \to p) \equiv \neg((p \to q) \to \neg(q \to p))$

1.10 Primer observem que $\neg p \equiv pXp \equiv pOp$.

a) $p \wedge q \equiv \neg(pXq) \equiv (pXq)X(pXq)$.

b) $p \vee q \equiv (\neg p)X(\neg q) \equiv (pXp)X(qXq)$.

c) $p \to q \equiv pX(\neg q) \equiv pX(qXq)$.

d) $p \wedge q \equiv (\neg p)O(\neg q) \equiv (pOp)O(qOq)$.

e) $p \vee q \equiv \neg(pOq) \equiv (pOq)O(pOq)$.

f) $p \to q \equiv \neg((\neg p)Oq) \equiv \neg((pOp)Oq) \equiv ((pOp)Oq)O((pOp)Oq))$.

g)

$$\begin{aligned} pXq &\equiv \neg((\neg p)O(\neg q)) \\ &\equiv \neg((pOp)O(qOq)) \\ &\equiv ((pOp)O(qOq))O((pOp)O(qOq)) \end{aligned}$$

h)

$$\begin{aligned} pOq &\equiv \neg((\neg p)X(\neg q)) \\ &\equiv \neg((pXp)X(qXq)) \\ &\equiv ((pXp)X(qXq))X((pXp)X(qXq)) \end{aligned}$$

1.11 1) Si p és certa, llavors s'executa I_1. Si $\neg p \wedge q$ és certa, s'executa I_2.

1.18 Les propietats 1 i 4 són certes. La primera diu que donat un enter x qualsevol, podem trobar un enter y tal que $xy = 0$. Efectivament, $y = 0$: donat x, llavors $x \cdot 0 = 0$. La quarta propietat diu que hi ha un enter y que compleix $xy = x$, per a qualsevol enter x. Efectivament, $y = 1$: $x \cdot 1 = x$, per a qualsevol enter x.

1.30

1) Suposem que $0 < x < y$. Llavors tenim:

$$x < y \Rightarrow 2x = x + x < x + y < y + y = 2y \Rightarrow x < \frac{x+y}{2} < y$$
$$0 < x < y \Rightarrow x^2 = x \cdot x < x \cdot y < y \cdot y = y^2 \Rightarrow x < \sqrt{xy} < y \quad (1)$$

(1): hem aplicat que tant x com y són positius i que l'arrel quadrada és una funció estrictament creixent.

2) Suposem que $m = (x+y)/2 = x$. Llavors $2x = x + y$, d'on $x = y$. El cas $m = (x+y)/2 = y$ es fa anàlogament. Suposem ara que $m = \sqrt{xy} = x$. Llavors $x^2 = xy$ i, per tant, $x = y$ (ja que $x > 0$). Anàlogament si $m = \sqrt{xy} = y$.

3) Demostrem la forma contra-recíproca; és a dir, si $\sqrt{xy} \geq (x+y)/2$, llavors $x = y$. Suposem que $\sqrt{xy} \geq (x+y)/2$. Llavors, com que es tracta de nombres positius, elevant al quadrat els dos membres obtenim $xy \geq (x+y)^2/4$. És a dir, $4xy \geq x^2 + 2xy + y^2$. D'aquí se segueix que: $x^2 - 2xy + y^2 = (x-y)^2 \leq 0$ i, com que un quadrant sempre és positiu, deduïm que $(x-y)^2 = 0$; és a dir, $x = y$.

7.2 Inducció

2.4 Pas inicial: $n = 0$. Efectivament, $0^3 + 3 \cdot 0^2 + 2 \cdot 0 = 0 = 6 \cdot 0$.
Pas d'inducció: fixem un enter $m \geq 0$ i suposem (hipòtesi d'inducció) que:

$$m^3 + 3m^2 + 2m = 6k,$$

per a cert enter k. Volem demostrar que $(m+1)^3 + 3(m+1)^2 + 2(m+1)$ és un múltiple de 6. Tenim:

$$\begin{aligned}(m+1)^3 + 3(m+1)^2 + 2(m+1) &= (m^3 + 3m^2 + 3m + 1) \\ &\quad + 3(m^2 + 2m + 1) + 2m + 2 \\ &= (m^3 + 3m^2 + 2m) + (3m^2 + 9m + 6)\end{aligned}$$

apliquem l'hipòtesi d'inducció:

$$= 6k + (3m^2 + 9m + 6)$$

Ara observem que $3m^2 + 9m + 6 = 3m(m+3) + 6$. Com que m i $m+3$ tenen paritat diferent, el seu producte sempre és parell. Per tant, $3m(m+3)$ és múltiple de 6. És a dir, $3m^2 + 9m + 6 = 6k'$, per a cert enter k'.

2.7

1) **Cas inicial:** $n = 1$**.**

$$\sum_{i=1}^{1} i \cdot i! = 1 \cdot 1! = 1 = (1+1)! - 1 = 2 - 1$$

Pas d'inducció: Fixem un enter $n \geq 1$ i suposem que $\sum_{i=1}^{n} i \cdot i! = (n+1)! - 1$ (hipòtesi d'inducció). Volem demostrar:

$$\sum_{i=1}^{n+1} i \cdot i! = (n+2)! - 1$$

Ara tenim:

$$\begin{aligned}\sum_{i=1}^{n+1} i \cdot i! &= \sum_{i=1}^{n} i \cdot i! + (n+1)(n+1)! \\ &= (n+1)! - 1 + (n+1)(n+1)! \qquad \text{per H.I.} \\ &= (n+1)!(1+n+1) - 1 \\ &= (n+1)!(n+2) - 1 = (n+2)! - 1\end{aligned}$$

Per tant, pel principi d'inducció, la propietat és certa per a tot $n \geq 1$.

2) **Cas inicial:** $n = 1$**.**

$$\sum_{\ell=1}^{1} \frac{1}{\ell(\ell+1)} = \frac{1}{1+1} = \frac{1}{2}$$

Pas d'inducció: Fixem un enter $n \geq 1$ i suposem que $\sum_{\ell=1}^{n} \frac{1}{\ell(\ell+1)} = \frac{n}{n+1}$ (hipòtesi d'inducció). Volem demostrar:

$$\sum_{\ell=1}^{n+1} \frac{1}{\ell(\ell+1)} = \frac{n+1}{n+2}$$

Ara tenim:

$$\begin{aligned}
\sum_{\ell=1}^{n+1} \frac{1}{\ell(\ell+1)} &= \sum_{\ell=1}^{n} \frac{1}{\ell(\ell+1)} + \frac{1}{(n+1)(n+2)} \\
&= \frac{n}{(n+1)} + \frac{1}{(n+1)(n+2)} \qquad \text{per H.I.} \\
&= \frac{n^2+2n+1}{(n+1)(n+2)} \\
&= \frac{(n+1)^2}{(n+1)(n+2)} \\
&= \frac{n+1}{n+2}
\end{aligned}$$

Per tant, pel principi d'inducció, la propietat és certa per a tot $n \geq 1$.

3) **Cas inicial:** $n = 1$**.**

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

Pas d'inducció: Fixem un enter $n \geq 1$ i suposem que $\sum_{i=1}^{n} \frac{1}{(2i-1)(2i+1)} = \frac{n}{2n+1}$ (hipòtesi d'inducció). Volem demostrar:

$$\sum_{i=1}^{n+1} \frac{1}{(2i-1)(2i+1)} = \frac{n+1}{2n+3}$$

Tenim:

$$\begin{aligned}
\sum_{i=1}^{n+1} \frac{1}{(2i-1)(2i+1)} &= \sum_{i=1}^{n} \frac{1}{(2i-1)(2i+1)} + \frac{1}{(2n+1)(2n+3)} \\
&= \frac{n}{2n+1} + \frac{1}{(2n+1)(2n+3)} \qquad \text{per H.I.} \\
&= \frac{n(2n+3)+1}{(2n+1)(2n+3)} \\
&= \frac{2n^2+3n+1}{(2n+1)(2n+3)} \\
&= \frac{(n+1)(2n+1)}{(2n+1)(2n+3)} \\
&= \frac{n+1}{2n+3}
\end{aligned}$$

Per tant, pel principi d'inducció, la propietat és certa per a tot $n \geq 1$.

4) **Pas base:** si $n = 2$, tenim que:

$$\sum_{i=0}^{2} \frac{1}{2i+1} = 1 + \frac{1}{3} + \frac{1}{5} = \frac{23}{15}$$

que és més petit que $\frac{2}{3} + 1 = \frac{5}{3}$.

Pas inductiu: sigui $n \geq 2$ un enter i suposem que es compleix:

$$\sum_{i=0}^{n} \frac{1}{2i+1} < \frac{n}{3} + 1 \quad \text{(hipòtesi d'inducció)}.$$

Volem demostrar que la propietat es compleix també per l'enter $n+1$; és a dir:

$$\sum_{i=0}^{n+1} \frac{1}{2i+1} < \frac{n+1}{3} + 1.$$

Tenim:

$$\sum_{i=0}^{n+1} \frac{1}{2i+1} = \sum_{i=0}^{n} \frac{1}{2i+1} + \frac{1}{2n+3} < \frac{n}{3} + 1 + \frac{1}{2n+3},$$

aquesta última desigualtat per hipòtesi d'inducció. Ara hem de demostrar que:

$$\frac{n}{3} + 1 + \frac{1}{2n+3} < \frac{n+1}{3} + 1.$$

Com que $n \geq 2$, tenim que $2n + 3 \geq 7$ i, per tant, $1/(2n+3) \leq 1/7 < 1/3$. D'aqui deduïm:

$$\frac{n}{3} + 1 + \frac{1}{2n+3} < \frac{n}{3} + 1 + \frac{1}{3} = \frac{n+1}{3} + 1.$$

Pel principi d'inducció, la propietat és certa per a tot enter $n \geq 2$.

2.8

Cas inicial: $n = 1$**:** $2!/1!2 = 1 \in \mathbb{Z}$.

Pas d'inducció: Fixem un enter $m \geq 1$ i suposem que $(2m)!/m!2^m = k \in \mathbb{Z}$ (hipòtesi d'inducció). Volem demostrar que:

$$\frac{(2(m+1))!}{(m+1)!2^{m+1}} = \frac{(2m+2)!}{(m+1)!2^{m+1}} \in \mathbb{Z}.$$

Tenim:

$$\frac{(2m+2)!}{2^{m+1}} = \frac{(2m+2)(2m+1)(2m)!}{(m+1)m!2 \cdot 2^m} = (2m+1)k \in \mathbb{Z}$$

Per tant, pel principi d'inducció, la propietat és certa per a tot $n \geq 1$.

7.3 Conjunts

3.1 Fals, fals, cert, cert.

3.2 Només 1 és correcta.

3.3 $A_1 \subset A_5$; $A_3 \subset A_5$; $A_4 \subset A_1$; $A_4 \subset A_2$; $A_4 \subset A_5$; $A_4 \subset A_6$.

3.7 $\{\emptyset, \{1\}, \{1,2\}\}$.

3.27

1) Hem de provar que és reflexiva, simètrica i transitiva.

   Reflexiva: $ab = ba$. Per tant: $(a,b)\ R\ (a,b)$.
   Simètrica: $(a,b)\ R\ (c,d) \Rightarrow a \cdot d = b \cdot c \Rightarrow c \cdot b = d \cdot a \Rightarrow (c,d)\ R\ (a,b)$.
   Transitiva: si $(a,b)\ R\ (c,d)$ i $(c,d)\ R\ (e,f)$, llavors $ad = bc$ i $cf = de$. Per tant, $adf = bcf = bde$. Simplificant per d, que és diferente de 0, per hipòtesi, obtenim que $af = be$. És a dir, $(a,b)\ R\ (e,f)$.

2) La classe d'equivalència d'un element és el conjunt dels elements que estan relacionats amb ell.

$$[(a,b)] = \{(x,y) : ay = bx\} = \{(x,y) : \frac{y}{x} = \frac{b}{a}\}$$

   Recordem que per hipòtesi, $a \neq 0$ i $x \neq 0$. Per tant, els elements de la classe de (a,b) són els parells que donen el quocient $b/a \in \mathbb{Q}$.

3) El conjunt quocient és el conjunt que té per elements les classes d'equivalència:

$$A/R = \{[(a,b)] : (a,b) \in A\}.$$

   Com hem vist a l'apartat anterior, cada classe d'equivalència ve *donada* per un quocient b/a d'enters no nuls. Per tant, hi ha tantes classes com possibles quocients d'enters no nuls.

3.28

1)
- R és reflexiva: donat $(x,y) \in \mathbb{R} \times \mathbb{R}$, tenim que $|x| + |y| = |x| + |y|$; és a dir, $(x,y)R(x,y)$;
- R és simètrica: si $(x,y)R(z,t)$, llavors $|x|+|y| = |z|+|t|$, i, per tant, tenim que $|z|+|t| = |x|+|y|$. És a dir, $(z,t)R(x,y)$;
- R és transitiva: si $(x,y)R(z,t)$ i $(z,t)R(u,v)$, llavors $|x| + |y| = |z| + |t|$ i $|z| + |t| = |u| + |v|$. Per tant, $|x| + |y| = |u| + |v|$ i llavors $(x,y)R(u,v)$.

2) Per definició de classe d'equivalència:

$$[(0,1)] = \{(x,y) : (x,y)R(0,1)\} = \{(x,y) : |x| + |y| = 1\}$$

   Per tant, hem de dibuixar el conjunt de punts (x,y) del pla tals que $|x| + |y| = 1$. Distingim quatre casos:

   a) si $x \geq 0, y \geq 0$, llavors dibuixem el segment determinat per la recta $x + y = 1$ al primer quadrant;
   b) si $x \geq 0, y \leq 0$, llavors dibuixem el segment determinat per la recta $x - y = 1$ al quart quadrant;
   c) si $x \leq 0, y \geq 0$, llavors dibuixem el segment determinat per la recta $-x + y = 1$ al segon quadrant;
   d) si $x \leq 0, y \leq 0$, llavors dibuixem el segment determinat per la recta $-x - y = 1$ al tercer quadrant;

   És a dir, la classe d'equivalència de $(0,1)$ és el conjunt de punts que estan sobre el perímetre del quadrat de vèrtexs $(0,1), (-1,0), (0,-1), (1,0)$.

3.29

1) S és reflexiva. Per definició de S, $x\ S\ x \iff x\ R\ x \wedge x\ R\ x$; però $x\ R\ x$ és cert perquè R és reflexiva.

   S és simètrica. Suposem que $x\ S\ y$; és a dir, $x\ R\ y \wedge y\ R\ x$. Com que la conjunció de proposicions és commutativa, deduïm que $y\ R\ x \wedge x\ R\ y$. És a dir, $y\ S\ x$.

   S és transitiva. Suposem que $x\ S\ y$ i $y\ S\ z$. Llavors tenim que $x\ R\ y \wedge y\ R\ x$ i $y\ R\ z \wedge z\ R\ y$. Com que R és transitiva i sabem que $x\ R\ y$ i $y\ R\ z$, deduïm que $x\ R\ z$. D'altra banda, també de la transitivitat de R i de que sabem que $y\ R\ x$ i $z\ R\ y$, deduïm que $z\ R\ x$. Per tant, tenim que $x\ R\ z$ i $z\ R\ x$. És a dir, $x\ S\ z$.

2) R és reflexiva. Per definició de R, $X\ R\ X \iff d(O,X) \leq d(O,X)$, i $d(O,X) \leq d(O,X)$ és cert.

R és transitiva. Suposem que $X\ R\ Y$ i $Y\ R\ Z$. És a dir, $d(O,X) \leq d(O,Y)$ i $d(O,Y) \leq d(O,Z)$. Per la transitivitat de la relació d'ordre $\leq$ deduïm que $d(O,X) \leq d(O,Z)$, és a dir $X\ R\ Z$.

Si apliquem l'apartat anterior, tenim que la corresponent relació S és d'equivalència. Però $X\ S\ Y \iff d(O,X) \leq d(O,Y) \wedge d(O,Y) \leq d(O,X) \iff d(O,X) = d(O,Y)$. És a dir, dos punts estan relacionats si, i només si, estan a la mateixa distància del punt O. És a dir, si, i només si, estan sobre la mateixa circumferència de centre O. Per tant, les classes d'equivalència són les circumferències del pla de centre O.

3.30

1) Provem que R és reflexiva, simètrica i transitiva.

Reflexiva: si $n \in A$, llavors $\operatorname{sgn}(n) = \operatorname{sgn}(n)$ i $\operatorname{paritat}(n) = \operatorname{paritat}(n)$. Per tant nRn.

Simètrica: en efecte, ja que la definió de la relació R queda igual si intercanviem n per m.

Transitiva: suposem que nRm i mRt. Distingim quatre casos:

a) n i m tenen el mateix signe i paritat; m i t tenen el mateix signe i paritat. En aquest cas deduïm que n i t tenen el mateix signe i paritat i, per tant, nRt.

b) n i m tenen el mateix signe i paritat; m i t tenen signe i paritat diferents. En aquest cas deduïm que n i t tenen signe diferent i paritat diferent. Per tant, nRt.

c) n i m tenen signe i paritats diferents; m i t tenen signe i paritats diferents. Llavors n i t tenen el mateix signe i la mateixa paritat. Per tant, nRt.

d) n i m tenen signe i paritat diferents; m i t tenen el mateix signe i la mateixa paritat. Aquest cas és similar al segon cas. Per tant, nRt.

2) Trobem la classe d'equivalència de l'element $1 \in A$. Un element n està relacionat amb 1 si o bé és positiu i senar o bé és negatiu i parell:

$$[1] = \{n \in A : nR1\} = \{1, 3, 5, \ldots\} \cup \{-2, -4, -6, \ldots\}$$

Anàlogament, els elements que estan relacionats amb el 2 són els positius i parells o bé els negatius i senars:

$$[2] = \{n \in A : nR2\} = \{2, 4, 6, \ldots\} \cup \{-1, -3, -5, \ldots\}$$

3) A l'apartat anterior observem que qualsevol elements de A (és a dir, qualsevol enter no nul) o bé pertany a la classe de 1 o bé pertany a la classe de 2. Per tant, no hi ha més classes. Això vol dir que el conjunt quocient és:

$$A/R = \{[1], [2]\}.$$

3.31

1)
- T és reflexiva: sigui $x \in A$; com que R i S són reflexives, tenim que xRx i xSx. Per tant, xTx.
- T és simètrica: siguin $x, y \in A$ i suposem que xTy. Llavors, xRy i xSy. Com que R i S són simètriques, tenim que yRx i ySx. Per tant, yTx.
- T és transitiva: siguin $x, y, z \in A$ i suposem que xTy i yTz. Llavors tenim que xRy, xSy, yRz i yTz. Com que R i S són transitives, deduïm que xRz i xSz.

2) Hi ha diverses respostes possibles i per a algunes U serà d'equivalència i per d'altres no.

- Sigui R la relació d'igualtat: $xRy \iff x = y$, que òbviament és una relació d'equivalència. Sigui S la relació total (és a dir, dos elements qualssevol estan relacionats). Llavors la relació U coincideix amb la relació S i, per tant, és d'equivalència.

- Sigui R la relació: $xRy \iff x \equiv y \pmod 2$ (x, y tenen la mateixa paritat). Ja sabem que R és una relació d'equivalència. Sigui S la relació donada per la partició de X: $\{A, B\}$, on $A = \{1, 2, 3, 4, 5\}$, $B = \{6, 7, 8, 9, 10\}$ (dos elements estan relacionats si estan al mateix conjunt d'aquesta partició). Llavors la relació U es descriu així: xUy si, i només si, x i y tenen la mateixa paritat o $x, y \in A$ o $x, y \in B$. Llavors U no és una relació transitiva. Per exemple, $2U6$ i $6U9$, però el 2 i el 9 no estan relacionats per U.

3.33 Es tracta de demostrar que tres proposicions són equivalents. Demostrarem que $1 \Rightarrow 2$, $2 \Rightarrow 3$ i $3 \Rightarrow 1$.

Recordem la definició de classe d'equivalència: $[a] = \{x \in A : xRa\}$.

$1 \Rightarrow 2$) Hipòtesi: $[a] \cap [b] \neq \emptyset$. Volem demostrar: $a \in [b]$.

Per hipòtesi, existeix un element $x \in [a] \cap [b]$. Per definició de classe d'equivalència, tenim que xRa i xRb. Per la propietat simètrica, si xRa, llavors aRx. Per la propietat transitiva, si aRx i xRb, llavors aRb. Per tant, $a \in [b]$.

$2 \Rightarrow 3$) Hipòtesi: $a \in [b]$. Volem demostrar: $[a] \subseteq [b]$. És a dir, hem de veure que, per a tot x, si $x \in [a]$, llavors $x \in [b]$.

Sigui $x \in [a]$. Per definició de classe d'equivalència, xRa. Però, per hipòtesi, $a \in [b]$; és a dir, aRb. Per la propietat transitiva, si xRa i aRb, llavors xRb. Per tant, $x \in [b]$.

$3 \Rightarrow 1$) Hipòtesi: $[a] \subseteq [b]$. Volem demostrar: $[a] \cap [b] \neq \emptyset$.

Com que $[a] \subseteq [b]$, resulta que $[a] \cap [b] = [a]$ (propietat de la intersecció de conjunts). Ara bé, una classe sempre té un element, com a mínim: $a \in [a]$ (per la propietat reflexiva). Per tant, $[a] \cap [b] = [a] \neq \emptyset$.

7.4 Aplicacions

4.1 1) $g^{-1}[\{0\}] = [0, 1)$; 2) $g^{-1}[\{-1, 0, 1\}] = [-1, 2)$; 3) $\emptyset$.

4.2

1) $f[S] = \{-2, 0, -4, 5\}$.

2) $f^{-1}[\{2\}] = \{2 + \sqrt{6}\}$, $f^{-1}[\{-3\}] = \{-3, 1, 3\}$.

4.6 f és injectiva. Hem de veure que si $x, x' \in \mathbb{R} - \{7\}$ i $f(x) = f(x')$, llavors $x = x'$. Tenim:

$$\begin{aligned} f(x) = f(x') &\Rightarrow \frac{5x}{x-7} = \frac{5x'}{x'-7} \\ &\Rightarrow 5x(x'-7) = 5x'(x-7) \\ &\Rightarrow xx' - 7x = x'x - 7x' \\ &\Rightarrow -7x = -7x' \\ &\Rightarrow x = x' \end{aligned}$$

Per tant, f és injectiva.

f és exhaustiva. Hem de veure que per a tot $y \in \mathbb{R} - \{5\}$, existeix una $x \in \mathbb{R} - \{7\}$ tal que $f(x) = y$. Plantegem l'equació $f(x) = y$ i aïllem la x:

$$\begin{aligned} y = \frac{5x}{x-7} &\Rightarrow y(x-7) = 5x \\ &\Rightarrow yx - 5x = (y-5)x = 7y \qquad (y \neq 5) \\ &\Rightarrow x = \frac{7y}{y-5} \end{aligned}$$

A més, aquesta x no pot ser igual a 7, ja que si $7y/(y-5) = 7$, llavors $y = y - 5$, que és absurd. Per tant, f és exhaustiva.

Així, f és injectiva i exhaustiva. Per tant, f és bijectiva. L'expressió anterior ens dóna la fórmula de la funció inversa:

$$f^{-1}(x) = \frac{7x}{x-5}$$

4.8

1) Comprovem primer que f és una aplicació de X en X. Si $1 \leq n \leq 50$, llavors $2 \leq f(n) = 2n \leq 100$ i si $51 \leq n \leq 100$, llavors $1 \leq f(n) = 2(n-51)+1 \leq 99$. És a dir, si $n \in X$, llavors hi ha un únic $m \in X$ tal que $f(n) = m$. En segon lloc, observem que donat $n \in A$, si $1 \leq n \leq 50$, llavors $f(n)$ és parell i si $51 \leq n \leq 100$, llavors $f(n)$ és senar. És a dir, pel contrarecíproc, si $f(n)$ és senar, llavors n està entre 51 i 100 i si $f(n)$ és parell, llavors n està entre 1 i 50.

   Per a demostrar que f és bijectiva, hem de provar que f és injectiva i exhaustiva.

   Injectivitat: suposem que $n, m \in A$ i que $f(n) = f(m)$. Si $f(n)$ és parell, llavors $f(m)$ també és parell, n i m estan entre 1 i 50 i, per tant, $f(n) = 2n = 2m = f(m)$, d'on $n = m$. Si $f(n)$ és senar, llavors $f(m)$ també és senar, n i m estan entre 51 i 100 i, per tant $f(n) = 2(n-51)+1 = 2(m-51)+1 = f(m)$, d'on també deduïm que $n = m$.

   Exhaustivitat: sigui $k \in A$. Hem de trobar un $n \in A$ tal que $f(n) = k$. Si k és parell, llavors $k/2 \in A$ i $1 \leq k/2 \leq 50$ i $f(k/2) = 2(k/2) = k$. Si k és senar, llavors $51 + (k-1)/2$ és enter i està entre 51 i 100. Per tant, $f(51 + (k-1)/2) = k$.

2) De l'observació del principi se segueix que la imatge d'un element de A és senar si, i només si, l'element està entre 51 i 100. És a dir:

$$f^{-1}[S] = \{n \in A : f(n) \in S\} = \{n \in A : 51 \leq n \leq 100\}$$

4.9

1) a) Si n és parell, llavors $f(n) = n$ i $f(f(n)) = f(n) = n$,

   b) Si n és senar, llavors $f(n) = n+1$ i $f(f(n)) = f(n+1)$; com ara $n+1$ és parell, $f(f(n)) = f(n+1) = n+1$.

   En tots els casos $f \circ f = f$.

2) $f[\{1,2,3,4\}] = \{2,4\}$. f no és injectiva ja que $f(2k) = f(2k-1)$.

3) $f^{-1}[\{0,1,2\}] = \{0,1,2\}$. f no és exhaustiva ja que el nombres senars no tenen antiimatge.

4.10

1) $f[\{-2,-1,0,1,2\}] = \{4,2,0,1,3\}$. $f[\{-5,-3,0,3,5\}] = \{10,6,0,5,9\}$.

2) $f^{-1}[\{0,1,2\}] = \{-1,0,1\}$. $f^{-1}[\{0,3,6\}] = \{-3,0,2\}$.

3) Hem de veure que si $f(n_1) = f(n_2)$, llavors $n_1 = n_2$. Notem que si $f(n_1) = f(n_2)$, llavors $n_1, n_2 > 0$ o $n_1, n_2 \leq 0$, ja que si $n_1 > 0$ i $n_2 \leq 0$, llavors tindríem que un nombre és parell i senar a la vegada.

   a) si $n_1, n_2 > 0$, llavors $2n_1 - 1 = 2n_2 - 1$, i $n_1 = n_2$,

   b) si $n_1, n_2 \leq 0$, llavors $-2n_1 = -2n_2$, i $n_1 = n_2$.

   En tots els casos $n_1 = n_2$.

4) Hem de veure que per a tot $m \in \mathbb{N}$ existeix $n \in \mathbb{Z}$ tal que $f(n) = m$:

   a) si m és parell, $m = 2k$ amb $k \geq 0$, llavors $f(-k) = m$,

   b) si m és senar, $m = 2k - 1$ amb $k \geq 1$, llavors $f(k) = m$.

4.12 Hem de provar que donat qualsevol $x \in A$, existeix un element $(a, b) \in A \times B$ tal que $g(a, b) = x$. Però $g(a, b) = a$, per tant, podem prendre l'element (x, b), on $b \in B$ és arbitrari. Fixem-nos que aquest b existeix perquè B és un conjunt no buit.

4.13 Siguin $x, y \in A$. Si $h(x) = h(y)$, llavors $(x, b_0) = (y, b_0)$. Per tant, donat que tenim parells ordenats, deduïm que $x = y$ i $b_0 = b_0$. És a dir, h és injectiva.

4.15

1) *Reflexiva*: per a tot $x \in A$, xRx, ja que $f(x) = f(x)$. *Simètrica*: si xRx', llavors $f(x) = f(x')$ i, per tant, $x'Rx$. *Transitiva*: si xRx' i $x'Rx''$, llavors $f(x) = f(x') = f(x'')$, d'on xRx''.

2) A cada classe d'equivalència tots els elements tenen la mateixa imatge per la funció part entera, i aquesta imatge és un nombre enter (comú per a tots els elements de la classe). La funció part entera pren tots els valors enters i només aquests. Per tant, cada nombre enter k determina una única classe d'equivalència; si $x \in \mathbb{R}$ i $\lfloor x \rfloor = k$, llavors:

   $$[x]_R = \{x' \in \mathbb{R} : \lfloor x' \rfloor = \lfloor x \rfloor\} = [k, k + 1)$$

   (interval tancat per l'esquerra, obert per la dreta). És a dir, hi ha una classe per a cada nombre enter k formada pels nombres reals que tenen part entera igual a k.

   Podem definir doncs l'aplicació $g : \mathbb{R}/R \to \mathbb{Z}$

   $$g([x]_R) = \lfloor x \rfloor$$

   Dir d'una altra manera, si la classe $[x]_R$ és l'interval $[k, k + 1)$, amb $k \in \mathbb{Z}$, llavors $g([x]_R) = k$. Per les consideracions que hem fet abans, està clar que aquesta aplicació és una bijecció.

4.16

1) Siguin $n, n' \in \mathbb{N}$ tals que $g(n) = g(n')$. És a dir, $2f(n) = 2f(n')$. D'aquí deduïm que $f(n) = f(n')$ i, com que f és injectiva, $n = n'$. Per tant, g és injectiva.

2) Siguin $m \in \mathbb{Z}$. Volem provar que existeix un $n \in \mathbb{Z}$ tal que $g(n) = m$. Però f és exhaustiva, per tant hi ha un $k \in \mathbb{Z}$ tal que $f(k) = m$. Si prenem $n = k - 1$, llavors $g(n) = g(k - 1) = f(k) = m$. Per tant, g és exhaustiva.

7.5 Enters: divisibilitat

5.1

1) $q = 2$, $r = 5$
2) $q = r = 0$
3) $q = -1$, $r = 7$
4) $q = -11$, $r = 10$
5) $q = 9$, $r = 6$
6) $q = -88$, $r = 5$

5.2 $143 = 11 \cdot 13$; 101 és primer; $289 = 17^2$; $899 = 29 \cdot 31$.

5.3 1) primer; 2) compost; 3) primer; 4) compost; 5) primer.

5.4 1) 3^4, 2) 2^4.

5.6 127

5.22 Efectivament, 5 i 7 són primers entre ells, és a dir, $\mathrm{mcd}(5, 7) = 1$. Per la identitat de Bézout, existeixen enters r, s tals que $1 = 5r + 7s$. Donat un enter n qualsevol, escrivim: $n = 5rn + 7sn$ i prenem $a = rn$ i $b = sn$.

5.23 Posem $d_1 = \mathrm{mcd}(a, b)$ i $d_2 = \mathrm{mcd}(bc - a, b)$. Anem a provar que $d_1 \mid d_2$ i que $d_2 \mid d_1$.

- Tenim: $d_1 = \mathrm{mcd}(a, b) \Rightarrow d_1 \mid a \wedge d_1 \mid b$. Per la linealitat: $d_1 \mid bc - a$, per a qualsevol $c \in \mathbb{Z}$. És a dir, d_1 és un divisor comú de b i de $bc - a$. Per definició de mcd, $d_1 \mid d_2$.
- Tenim: $d_2 = \mathrm{mcd}(bc - a, b) \Rightarrow d_2 \mid bc - a \wedge d_2 \mid b$. Per la linealitat: $d_2 \mid (bc - (bc - a))$. És a dir, $d_2 \mid a$ i $d_2 \mid b$. Per definició de mcd: $d_2 \mid d_1$.

Ara bé, d_1 i d_2 són positius, per definició de mcd, i cadascun divideix a l'altre. Per tant: $d_1 = d_2$.

5.24

1) Per a demostrar que la propietat $\mathrm{mcd}(m, n) = \mathrm{mcd}(m - n, m + n)$ no és certa, en general, hem de trobar un contraexemple. Si prenem $m = 5$ i $n = 3$, llavors tenim $m + n = 8$ i $m - n = 2$. Per tant:

$$\mathrm{mcd}(m, n) = \mathrm{mcd}(5, 3) = 1, \qquad \mathrm{mcd}(m - n, m + n) = \mathrm{mcd}(2, 8) = 2.$$

2) Hem de provar que:

$$\forall m, n \in \mathbb{Z} \ \ (m \text{ i } n \text{ tenen paritat diferent} \Rightarrow \mathrm{mcd}(m, n) = \mathrm{mcd}(m - n, m + n))$$

Denotem per $d_1 = \mathrm{mcd}(m, n)$ i $d_2 = \mathrm{mcd}(m - n, m + n)$. Veiem que $d_1 | d_2$ i que $d_2 | d_1$ i com que ambdós són positius, han de ser iguals.

- $d_1 | m \wedge d_1 | n \Rightarrow d_1 | (m - n) \wedge d_1 | (m + n) \Rightarrow d_1 | \mathrm{mcd}(m - n, m + n) = d_2$. A la primera implicació hem aplicat la propietat de la linealitat de la divisibilitat i a la segona la definició de màxim comú divisor.
- Per hipòtesi, m i n tenen paritat diferent. Per tant, $m - n$ i $m + n$ són nombres enters senars. Conseqüentment, $d_2 = \mathrm{mcd}(m - n, m + n)$ ha de ser senar. Com que $d_2 | (m - n)$ i $d_2 | (m + n)$, es dedueix que $d_2 | (m - n) + (m - n) = 2m$, per la propietat de linealitat de la divisibilitat. Però d_2 és senar; és a dir, $\mathrm{mcd}(d_2, 2) = 1$. Per tant, pel lema de Gauss, $d_2 | m$. Anàlogament, tenim que $d_2 | (m + n) - (m - n) = 2n$ (també per linealitat) i de la mateixa manera veiem que $d_2 | n$. Per tant, $d_2 | \mathrm{mcd}(m, n) = d_1$.

3) Hem de veure que la proposició:

$$\forall m, n \in \mathbb{Z} \ \ (\mathrm{mcd}(m, n) = \mathrm{mcd}(m - n, m + n) \Rightarrow m \text{ i } n \text{ tenen paritat diferent})$$

és falsa. És a dir, hem de trobar un contraexemple: dos enters m i n tals que $\mathrm{mcd}(m, n) = \mathrm{mcd}(m - n, m + n)$ i que tinguin la mateixa paritat. Per exemple $m = 4$ i $n = 2$ tenen la mateixa paritat. A més, resulta que $\mathrm{mcd}(m, n) = \mathrm{mcd}(4, 2) = 2$ i $\mathrm{mcd}(m - n, m + n) = \mathrm{mcd}(2, 6) = 2$.

5.25

1) Apliquem l'algorisme d'Euclides estès:

X	1	0	1	-2
Y	0	1	-2	5
Q		2	2	10
R	52	21	10	1
	10	1	0	

on la fila Q conté els quocients de les divisions; la fila R conté els residus; i les entrades de la fila X es calculen aplicant la recurrència: $x_{k+1} = x_{k-1} - x_k q_k$ (i anàlogament per la fila Y).

Per tant, $\mathrm{mcd}(52, 21) = 1$ i l'identitat de Bézout és:

$$52 \cdot (-2) + 21 \cdot 5 = 1$$

2) Hem de provar que per a tot enter n, existeixen enters x, y tals que $f(x, y) = n$. És a dir, per a tot $n \in \mathbb{Z}$, existeixen $x, y \in \mathbb{Z}$ tals que $52x + 21y = n$.

Però per l'apartat anterior, sabem que $52 \cdot (-2) + 21 \cdot 5 = 1$. Si multipliquem aquesta igualtat per n, obtenim:

$$52 \cdot (-2n) + 21 \cdot (5n) = n$$

Per tant, donat un enter n, tenim que $f(-2n, 5n) = n$. És a dir, f és exhaustiva.

5.26

a) Volem demostrar que $M_p \cap M_q = M_{pq}$. Podríem demostrar que cada conjunt està inclòs a l'altre, però en aquest cas es pot demostrar directament que $x \in M_p \cap M_q$ és equivalent a $x \in M_{pq}$:

$x \in M_p \cap M_q \Leftrightarrow x \in M_p \wedge x \in M_q$	definició d'intersecció
$\Leftrightarrow p \mid x \wedge q \mid x$	definició de M_p i de M_q
$\Leftrightarrow \mathrm{mcm}(p, q) \mid x$	propietat del mcm
$\Leftrightarrow pq \mid x$	$\mathrm{mcm}(p, q) = pq$, perquè són primers diferents
$\iff x \in M_{pq}$	definició de M_{pq}

Conclusió: $M_{pq} = M_p \cap M_q$.

b) Hem de veure que $M_{p^2} \subset M_p$, on p és un nombre primer. És a dir, hem de provar: 1) que tot element de M_{p^2} és un element de M_p i, a més, 2) que són diferents (és dir, que hi ha un element a M_p que no pertany a M_{p^2}).

Sigui $x \in M_{p^2}$. Llavors per definició d'aquest conjunt: $p^2 \mid x$. Però $p \mid p^2$ i, per la propietat transitiva de la divisibilitat, tenim que $p \mid x$. Per tant, $x \in M_p$.

Considerem el nombre p. Està clar que $p \in M_p$, ja que $p \mid p$. Però $p \notin M_{p^2}$, ja que p^2 no és un divisor de p. Per tant, $M_{p^2} \neq M_p$.

c) No. Contraexemple: prenem $n = p$, p primer, i $m = p^2$. Llavors, per l'apartat anterior sabem que $M_{p^2} \subset M_p$; per tant, $M_p \cap M_{p^2} = M_{p^2} \neq M_{p^3}$.

5.29 En primer lloc, observem que els coeficients 13 i -47 són primers entre ells (de fet, 13 i 47 són primers). És a dir, $\mathrm{mcd}(13, -47) = 1$. Per tant, com que $1 \mid 10$, hi ha solució. Busquem una solució

particular usant l'algorisme d'Euclides i escrivint la identitat de Bézout corresponent als nombres positius 13 i 47 i després la modifiquem convenientment.

1	0	1	−1	2	−3	5
0	1	−3	4	−7	11	−18
	3	1	1	1	1	2
47	13	8	5	3	2	1

La identitat de Bézout és $13 \cdot (-18) + 47 \cdot 5 = 1$. Multiplicant per 10 i canviant de signe el coeficient de 47, i per tant també del 5, obtenim una solució particular de l'equació:

$$13 \cdot (-180) - 47 \cdot (-50) = 10$$

Per tant, la solució general és:

$$x = -180 - (-47)t = -180 + 47t$$
$$y = -50 + 13t$$

on $t \in \mathbb{Z}$.

Busquem ara la solució (x, y) que tingui la y negativa més gran possible. Volem que $y < 0$; és a dir:

$$y < 0 \iff -50 + 13t < 0 \iff t < \frac{50}{13} \approx 3,8 \iff t \leq 3$$

l'última equivalència és certa perquè t és un enter. Ara bé la funció $f(t) = -50 + 13t$ és una funció estrictament creixent (per exemple, perquè la primera derivada és sempre positiva). Per tant, si $t_1 < t_2$, llavors $y_1 = -50 + 13t_1 < y_2 = -50 + 13t_2$. Per tant, el valor negatiu més gran de y s'obté per a $t = 3$ i és $y = -11$. El valor corresponent de la x quan $t = 3$ és $x = -39$.

Una altra solució: sabem que $y = -50 + 13t$, amb $t \in \mathbb{Z}$; és a dir $y \equiv -50 \equiv 2 \pmod{13}$. I l'enter negatiu més gran congruent amb 2 mòdul 13 és $2 - 13 = -11$, que correspon al valor de $t = 3$, obtenint que $x = -39$.

7.6 Enters: congruències

6.1 1) $\{-12, -4, 0, 4\}$, $\{-11, 1, 5\}$, $\{-9, -1, 3, 7\}$, $\{-6, 2, 10\}$.

6.7 1) 9586; 2) 5280.

6.8 1) 4, 2) 15, 3) 58, 4) 40

6.9 1) 4, 2) 15, 3) 31, 4) 318, 5) 4, 6) 268

6.10 $\overline{x} = \overline{88}$.

6.11 Per exemple, 302. En general qualsevol enter de la forma $391k + 302$, $k \in \mathbb{Z}$.

6.14 Si $\mathrm{mcd}(a, m) = 2$, llavors, per la identitat de Bézout, existeixen enters x i y tals que $ax + my = 2$. Considerant aquesta igualtat mòdul m obtenim que $ax \equiv 2 \pmod{m}$.

6.15 2) $\overline{152}$. 3) Podeu aplicar les fórmules de Cramer. Les solucions són: $\overline{x} = \overline{46}, \overline{y} = \overline{82}$.

6.18 0.

6.20

1) Provem per separat que és injectiva i exhaustiva.

   - Injectiva: suposem que $f(\overline{x}) = f(\overline{y})$. Llavors:

     $$\overline{22}\cdot\overline{x}+\overline{7} = \overline{22}\cdot\overline{y}+\overline{7} \Rightarrow \overline{22}\cdot\overline{x} = \overline{22}\cdot\overline{y} \Rightarrow \overline{a}\cdot\overline{22}\cdot\overline{x} = \overline{a}\cdot\overline{22}\cdot\overline{y} \Rightarrow \overline{x} = \overline{y}$$

     on: primer hem restat a tots dos membres $\overline{7}$ i després hem multiplicat per $\overline{a}$, la classe inversa de $\overline{22}$, que existeix perquè $\mathrm{mcd}(22, 29) = 1$.
   - Sigui $\overline{y} \in \mathbb{Z}_{29}$ una classe arbitrària. Volem veure que hi ha una classe $\overline{x}$ tal que $\overline{22}\cdot\overline{x}+\overline{7} = \overline{y}$. Un altre cop, considerem la classe inversa $\overline{a}$ de $\overline{22}$. Llavors, podem aïllar la $\overline{x}$ de la igualtat anterior i obtenim: $\overline{x} = \overline{a}(\overline{y} - \overline{7})$. Per tant, és exhaustiva.

   Per trobar l'aplicació inversa hem de calcular la classe $\overline{a}$. Calculem la identitat de Bézout de 29 i 22 i obtenim: $29\cdot(-3) + 22\cdot 4 = 1$. Per tant, $\overline{a} = \overline{4}$. Així doncs: $f^{-1}(\overline{x}) = \overline{4}(\overline{x} - \overline{7}) = \overline{4}\cdot\overline{x} + \overline{1}$.

2) Per descodificar escrivim el nombre que li correspon a cada símbol i li apliquem f^{-1}:

$K \mapsto 10$	$\to f^{-1}(\overline{10}) = \overline{41} = \overline{12}$	$\mapsto M$
$Z \mapsto 25$	$\to f^{-1}(\overline{25}) = \overline{101} = \overline{14}$	$\mapsto O$
$R \mapsto 17$	$\to f^{-1}(\overline{17}) = \overline{69} = \overline{11}$	$\mapsto L$
$T \mapsto 19$	$\to f^{-1}(\overline{19}) = \overline{77} = \overline{19}$	$\mapsto T$
$, \mapsto 28$	$\to f^{-1}(\overline{28}) = \overline{113} = \overline{26}$	$\mapsto$
$A \mapsto 0$	$\to f^{-1}(\overline{0}) = \overline{1}$	$\mapsto B$
$I \mapsto 8$	$\to f^{-1}(\overline{8}) = \overline{33} = \overline{4}$	$\mapsto E$

Per tant, el missatge original és: 'MOLT BE'.

6.21

1) En primer lloc, hem de provar que $\mathrm{mcd}(4096, 2957) = 1$ i després hem d'escriure la identitat de Bézout (de fet, només necessitem el coeficient de 2957).

0	1	−1	3	−4	7	−18	169	−187
	1	2	1	1	2	9	1	21
4096	2957	1139	679	460	219	22	21	1
1139	679	460	219	22	21	1	0	

Per tant, $\mathrm{mcd}(4096, 2957) = 1$ i $\overline{2957}$ té invers a $\mathbb{Z}_{4096}$. A més, sabem que existeix un enter x tal que:

$$4096x + 2957\cdot(-187) = 1$$

És a dir $\overline{2957}^{-1} = \overline{-187} = \overline{3909}$.

2) **Solució 1.** Hem de comprovar que $f \circ g = I$ i $g \circ f = I$, on I és l'aplicació identitat de $\mathbb{Z}_{4096}$, és a dir I està definida per $I(\overline{x}) = \overline{x}$.

$$\begin{aligned}(f\circ g)(\overline{x}) &= f(g(\overline{x})) = f(\overline{3909}\cdot\overline{x})\\ &= \overline{2957}\cdot(\overline{3909}\cdot\overline{x}) = (\overline{2957}\cdot\overline{3909})\cdot\overline{x}\\ &= \overline{1}\cdot\overline{x} = \overline{x} = I(\overline{x})\end{aligned}$$

perquè a l'apartat anterior hem provat que la classe inversa de $\overline{2957}$ és $\overline{3909}$. Això demostra que $f \circ g = I$. Anàlogament es demostra l'altra propietat:

$$\begin{aligned}(g\circ f)(\overline{x}) &= g(f(\overline{x})) = g(\overline{2957}\cdot\overline{x})\\ &= \overline{3909}\cdot(\overline{2957}\cdot\overline{x}) = (\overline{3909}\cdot\overline{2957})\cdot\overline{x}\\ &= \overline{1}\cdot\overline{x} = \overline{x} = I(\overline{x})\end{aligned}$$

Solució 2. Una altra manera de demostrar el que demanen és trobar l'aplicació inversa de f i comprovar que és g. Per trobar l'inversa de f, aïllem la $\overline{x}$ de l'equació $\overline{y} = \overline{2957} \cdot \overline{x}$. És a dir, multipliquem per la classe inversa a ambdós membres. Però, per l'apartat anterior $\overline{2957}^{-1} = \overline{3909}$. És a dir:

$$\overline{y} = \overline{2957} \cdot \overline{x} \Rightarrow \overline{x} = \overline{2957}^{-1} \cdot \overline{y} \Rightarrow \overline{y} = \overline{3909} \cdot \overline{x}$$

Per tant, hem comprovat que l'aplicació inversa de f és g. I com l'aplicació inversa de l'aplicació inversa de f és f, hem provat que les dues aplicacions són mútuament inverses una de l'altra.

6.23 1) 11, 2) 5, 3) 11, 4) 1, 5) 8, 6) 8.

6.24 1) 76, 2) 69, 3) 1.

6.25 1) 1, 2) 1.

6.26 1) $x \equiv 17 \pmod{35}$, 2) $x \equiv 23 \pmod{36}$, 3) $x \equiv 616 \pmod{1989}$, 4) $x \equiv 89 \pmod{105}$, 5) $x \equiv 403 \pmod{924}$, 6) $x \equiv 1318 \pmod{2340}$.

6.26 1) $x \equiv 17 \pmod{35}$, 2) $x \equiv 23 \pmod{36}$, 3) $x \equiv 616 \pmod{1989}$, 4) $x \equiv 89 \pmod{105}$, 5) $x \equiv 403 \pmod{924}$, 6) $x \equiv 1318 \pmod{2340}$.

6.27 Sigui x la solució que busquem. Llavors x és l'enter positiu més petit que verifica el sistema de congruències següent: $x \equiv 8 \pmod{13}$, $x \equiv 3 \pmod{11}$, $x \equiv 5 \pmod{8}$. Observem que els mòduls són primers entre si dos a dos. Llavors hi ha solució, que és única mòdul el producte dels mòduls $m_1 m_2 m_3 = 1144$. Notem:

$m_1 = 13$	$M_1 = m_2 m_3 = 88$	$y_1 = 4$
$m_2 = 11$	$M_2 = m_1 m_3 = 104$	$y_2 = 9$
$m_3 = 8$	$M_3 = m_1 m_2 = 143$	$y_3 = 7$

on y_j és un invers de M_j mòdul m_j, per a $j = 1, 2, 3$, calculats usant l'algorisme d'Euclides i la identitat de Bézout. Llavors la solució és:

$$x \equiv 8M_1y_1 + 3M_2y_2 + 5M_3y_3 = 10629 \equiv 333 \pmod{1144}$$

Per tant, la solució és 333 monedes.