29

Eina-e

Matemàtica discreta 2

Maria Bras-Amorós
Oriol Farràs Ventura

[publicacions]
urv

Matemàtica discreta 2

Maria Bras-Amorós
Oriol Farràs Ventura

[publicacions]
urv

Tarragona, 2024

Publicacions de la Universitat Rovira i Virgili
Av. Catalunya, 35 - 43002 Tarragona
Tel. 977 558 474 · publicacions@urv.cat
www.publicacions.urv.cat

1a edició: abril de 2022
2a edició: octubre de 2024
ISBN (paper): 978-84-1365-004-3
ISBN (PDF): 978-84-1365-005-0

Dipòsit legal: T 570-2022

Aquest llibre és un resultat del Projecte Estratègic "HERMES: Ciberseguretat en computació descentralitzada" i de la Càtedra en Ciberseguretat INCIBE-URV, ambdós fruits de convenis de col·laboració subscrits entre l'Institut Nacional de Ciberseguretat (INCIBE) i la Universitat Rovira i Virgili. Aquestes iniciatives (finançades per la Unió Europea Next Generation- EU) es realitzen en el marc del Pla de Recuperació, Transformació i Resiliència, el projecte del Govern d'Espanya que traça el full de ruta per a la modernització de l'economia espanyola, la recuperació del creixement econòmic i la creació d'ocupació després de la crisi de la Covid-19, així com per preparar al país per afrontar els reptes de la pròxima dècada.

HERMES
FRONTIER RESEARCH IN CYBERSECURITY

Financiado por la Unión Europea NextGenerationEU
GOBIERNO DE ESPAÑA
MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA
SECRETARÍA DE ESTADO DE DIGITALIZACIÓN E INTELIGENCIA ARTIFICIAL
Plan de Recuperación, Transformación y Resiliencia
incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD
Universitat Rovira i Virgili

Cita el libro.
Consulta el libro en nuestra web.

Publicacions de la Universitat Rovira i Virgili es miembro de la Unión de Editoriales Universitarias Españolas y de la Xarxa Vives, lo que garantiza la difusión y comercialización de sus publicaciones a nivel nacional e internacional.

Índex

TEMA 1

Material de les classes de teoria i problemes

Índex

Unes matemàtiques per a les comunicacions digitals

La tecnologia actual ens ha portat a un context en què la informació es descriu amb seqüències de bits.

L'emmagatzematge i la transmissió d'aquestes dades van lligats a una sèrie de problemes:

- Els suports en els quals s'emmagatzemen les dades poden degradar-se.
- La transmissió de dades a través d'un canal sorollós pot comportar errors.
- Les dades poden ser accedides o modificades per tercers.

Objectiu: Transformar les dades per evitar aquests problemes.

- Generalment, les dades es divideixen en blocs i es processen per blocs de la forma

$$x = x_1 x_2 \dots x_k \in \{0,1\}^k.$$

- El conjunt de possibles blocs és un conjunt finit, $\{0,1\}^k$.
- Des dels anys 40 del segle XX, s'han buscat resultats matemàtics coneguts que donin recursos per treballar amb aquests blocs, i se n'han buscat de nous.
- La branca de les matemàtiques on es poden buscar aquests resultats és la **matemàtica discreta**
- Per disposar de més varietat de resultats, treballarem amb diferents **estructures algebraiques**.

- Quines operacions sabem fer amb els elements del conjunt $\{0,1\}^k$? OR, AND, XOR, SHIFT...
- Trobar solucions només amb aquestes operacions és difícil.
- Sovint identificarem els elements de $\{0,1\}^k$ amb els d'un conjunt C que sigui un **grup**, un **anell**, un **cos finit** o un **espai vectorial**.
- Un cop tenim els blocs identificats amb un element de C, podrem fer moltes més operacions.
- Resultats d'**aritmètica** i d'**àlgebra lineal** ens permetran trobar solucions més elaborades.

Aquestes transformacions es fan de manera implícita en moltes tecnologies:

- Codis de barres i QR
- DVD i Blu-ray
- ADSL, WiMAX, 5G
- RAID
- TLS, https
- WhatsApp, Skype, Teams
- Blockchain
- ...

En aquest curs aprendrem les **estructures algebraiques** emprades en comunicacions digitals i, com a aplicació, estudiarem els **codis lineals**.

- Aritmètica entera
- Aritmètica modular
- Cossos finits
- Codis lineals
- Codis cíclics
- Codis Reed-Solomon

1 Introducció a l'aritmètica

1.1 Divisió d'enters

Dividend, divisor, quocient i residu

Tenim una ampolla plena de 750 ml i copes buides de 175 ml.

Quantes copes podem omplir del tot?

Si al final ens queda una copa que no podem acabar d'omplir, quants ml de vi té?

$$\begin{array}{r|l} 750 & 175 \\ \cline{2-2} -700 & \quad 4 \\ \hline 50) & \end{array}$$

Teorema 1: Divisió d'enters

Donats dos enters qualssevol a i b, existeixen dos altres enters únics q i r tals que $a = bq + r$ amb $0 \le r < |b|$.

Exemple. $a = 5, b = 2 \to q = 2, r = 1$
$a = -7, b = 3 \to q = -3, r = 2$

Dividend, divisor, quocient, residu

L'enter a i b són, respectivament, el **dividend** i el **divisor** de la divisió. L'enter q és el **quocient** (podem omplir 4 copes senceres). L'enter r és el **residu** (a la cinquena copa només li podem posar 50 ml).

Exemple. *Agafem $a = 5600$ i $b = 1764$. A l'escola tots hem après a fer la divisió*

$$\begin{array}{r|l} 5600 & 1764 \\ \cline{2-2} -5292 & \;\;3 \\ \hline 308) & \end{array}$$

El que estem fent amb aquest algoritme és anar provant quin valor té $q \cdot 1764$ *a mesura que* q *va creixent, sense arribar mai a superar* 5600.

Al final r *serà la diferència entre* 5600 *i el màxim valor possible* $q \cdot 1764$ *que no superi* 5600.

Per com el definim, es pot comprovar que r *sempre serà positiu o zero, i sempre més petit que* 1764.

Exercici 1: Curiositat

Trobeu el quocient i el residu per a les següents parelles de valors de dividends i divisors.

- 9 i 1
- 98 i 12
- 987 i 123
- 9876 i 1234
- 98765 i 12345
- 987654 i 123456
- 9876543 i 1234567
- 98765432 i 12345678
- 987654321 i 123456789

Divisors

Múltiples i divisors

Si en la divisió entera de a entre b el residu és 0, aleshores diem que

- a és un **múltiple** de b,
- b és un **divisor** d'a,
- b **divideix** a.

Escrivim $b \mid a$ i denotem el quocient per $\frac{a}{b}$.

Si b és un divisor de a, com que tindrem $a = b \cdot q$, aleshores $q := \frac{a}{b}$ també és un divisor de a.

Exercici 2

Comproveu que 12345679 és un divisor de 111111111. Deduïu que 12345679 és un divisor de 222222222, 333333333, 444444444, etc.

El cas del 0 i de l'1

El 0 és múltiple de qualsevol enter i l'1 és un divisor de qualsevol enter.

▸ ***Divisors de* 12**

Mirem els residus de dividir 12 entre els enters positius més petits o iguals que ell.

enter	q	r
1	12	0
2	6	0
3	4	0
4	3	0
5	2	2
6	2	0
7	1	5
8	1	4
9	1	3
10	1	2
11	1	1
12	1	0

Observem que el residu és zero només per als enters $1, 2, 3, 4, 6, 12$. Aquest és el conjunt dels divisors positius de 12.

▸ ***Divisors de* 16**

Repetim l'experiment amb l'enter 16.

enter	q	r
⋮	⋮	⋮
10	1	6
11	1	5
12	1	4
13	1	3
14	1	2
15	1	1
16	1	0

El conjunt de divisors positius de 16 és, doncs, $\{1, 2, 4, 8, 16\}$.

▸ ***Propietats dels divisors***

Exercici 3

Comproveu que si $a \mid b$ i $b \mid c$, aleshores $a \mid c$. Solució (p.22)

Exercici 4

Comproveu que si $a \mid b$ i existeix d tal que $d \mid a$ i $d \mid b$, aleshores $\frac{a}{d} \mid \frac{b}{d}$. Solució (p.22)

Exercici 5

Demostreu que si $a \mid b$ i $a \mid c$, aleshores
- $a \mid -b$
- $a \mid b + c$
- $a \mid b - c$

Solució (p.22)

Exercici 6

Demostreu que si $a = bq + r$ amb $0 \le r < |b|$ i d és un divisor comú de a i b, aleshores també és un divisor de r. Solució (p.22)
(Més endavant veurem l'aplicació d'aquest resultat al càlcul del mcd.)

Exercici 7

Demostreu que si $d > 1$, aleshores d no és divisor de $qd + 1$ per cap enter q. Solució (p.22)

▸ ***Aparellem divisors***

El conjunt de divisors positius d'un enter positiu els podem agrupar per parelles de manera que el producte de cada parella ens dona l'enter.

$$\begin{array}{ccccccc} 1 & & & \cdot & & & 12 & = 12 \\ & 2 & & \cdot & & 6 & & = 12 \\ & & 3 & \cdot & 4 & & & = 12 \end{array}$$

Si el nombre de divisors positius és senar, aleshores l'enter intermedi es multiplica per ell mateix. Per tant, en aquest cas l'enter és un quadrat.

$$\begin{array}{ccccccc} 1 & & & \cdot & & & 16 & = 16 \\ & 2 & & \cdot & & 8 & & = 16 \\ & & 4 & \cdot & 4 & & & = 16 \end{array}$$

Criteris de divisibilitat

A l'escola tots hem après aquests criteris:

Criteri de divisibilitat del 2

Un nombre és divisible per 2 si acaba en $0, 2, 4, 6$ o 8.

Criteri de divisibilitat del 3

Un nombre és divisible per 3 si la suma de les seves xifres és divisible entre 3.

Criteri de divisibilitat del 4

Un nombre és divisible per 4 si les seves dues últimes xifres són un múltiple de 4.

Criteri de divisibilitat del 5

Un nombre és divisible per 5 si acaba en 0 o 5.

Criteri de divisibilitat del 6

Un nombre és divisible per 6 si ho és per 2 i per 3.

Criteri de divisibilitat del 7

??? No se'n coneix cap.

$$\vdots$$

Criteri de divisibilitat del 10

Un nombre és divisible per 10 si acaba en 0.

Exercici 8

Intenteu demostrar per inducció els criteris de divisibilitat del 2, el 5 i el 10. Intenteu demostrar el criteri del 4.

Observem que tots aquests criteris són específics per a valors molt concrets i molt petits. En general no hi ha criteris de divisibilitat per a nombres grans.

1.2 Màxim comú divisor

Màxim comú divisor

Màxim comú divisor

El **màxim comú divisor** de dos enters és el màxim dels divisors que tenen en comú.

Coprimers

Diem que dos enters són primers entre ells o **coprimers** si el seu màxim comú divisor és 1.

▸ ***Propietats del mcd***

Observem que per a tot enter a es compleix que $\mathrm{mcd}(0,a) = a$, $\mathrm{mcd}(1,a) = 1$, exactament al revés que les taules de multiplicar del 0 i l'1.

Exercici 9

Demostreu que si $a = bq + r$ amb $0 \leq r < |b|$, aleshores $\mathrm{mcd}(a, b) = \mathrm{mcd}(b, r)$.
Solució (p.22)

Mínim comú múltiple

El **mínim comú múltiple** de dos enters és el mínim dels múltiples no nuls que tenen en comú. Denotem el mínim comú múltiple de a, b per $\mathrm{mcm}(a, b)$.

Exercici 10

1. Demostreu que si M és múltiple de a i múltiple de b, aleshores M també és múltiple de $\mathrm{mcm}(a, b)$.
2. Demostreu que, per a qualsevol parella d'enters a, b,
$$\mathrm{mcm}(a, b) \cdot \mathrm{mcd}(a, b) = ab.$$

Algoritme d'Euclides

▸ ***Mètode de càlcul del mcd seguint la definició***

Una primera manera de trobar el màxim comú divisor, aplicant la definició, és buscant la llista de divisors positius dels dos enters, trobant la seva intersecció i seleccionant el més gran de tots els divisors de la intersecció.

Per exemple, per trobar $\mathrm{mcd}(12, 16)$ calculem les llistes de divisors positius de 12 i 16:

- Divisors positius de 12: $\{1, 2, 3, 4, 6, 12\}$
- Divisors positius de 16: $\{1, 2, 4, 8, 16\}$
- Intersecció dels dos conjunts: $\{1, 2, 4\}$
- Màxim de la intersecció: 4
- Per tant, $\mathrm{mcd}(12, 16) = 4$.

Aquest mètode ens obliga a calcular la llista de tots els divisors dels dos nombres, la qual cosa pot ser molt costosa, especialment per a nombres grans.

▸ ***Mètode de càlcul del mcd que havíem après a l'escola***

Recordem el mètode que fèiem servir a l'escola. Es basa en l'existència i la unicitat de la descomposició de tot enter en producte de primers, que veurem en la secció següent.

Suposem que volem calcular $\mathrm{mcd}(5600, 1764)$.

Descomponem els enters en producte de primers.

$$\begin{array}{r|l}
5600 & 2 \\
2800 & 2 \\
1400 & 2 \\
700 & 2 \\
350 & 2 \\
175 & 5 \\
35 & 5 \\
7 & 7 \\
1 &
\end{array}
\qquad
\begin{array}{r|l}
1764 & 2 \\
882 & 2 \\
441 & 3 \\
147 & 3 \\
49 & 7 \\
7 & 7 \\
1 &
\end{array}$$

$$5600 = 2^5 \cdot 5^2 \cdot 7 \qquad 1764 = 2^2 \cdot 3^2 \cdot 7^2$$

Deduïm que $\mathrm{mcd}(5600, 1764) = 2^2 \cdot 7 = 28$.

Buf! I això que hem fet servir regles de divisibilitat, que només coneixem per alguns enters petits.

▸ ***Alternativa d'Euclides***

Utilitzarem el resultat de l'Exercici 9.

Dividim 5600 entre 1764. Ens queda quocient $q = 3$, residu $r = 5600 - 5292 = 308$. Tenim

$$\mathrm{mcd}(5600, 1764) = \mathrm{mcd}(1764, 308).$$

Més fàcil, no? Doncs ho repetim.

Dividim 1764 entre 308. Ens queda quocient $q = 5$ i residu $r = 1764 - 1540 = 224$. Per tant,

$$\mathrm{mcd}(5600, 1764) = \mathrm{mcd}(1764, 308) = \mathrm{mcd}(308, 224).$$

Dividim 308 entre 224. Ens queda quocient $q = 1$, residu $r = 84$. Per tant,

$$\mathrm{mcd}(5600, 1764) = \mathrm{mcd}(308, 224) = \mathrm{mcd}(224, 84).$$

Dividim 224 entre 84. Ens queda quocient $q = 2$, residu $r = 224 - 168 = 56$. Per tant,

$$\mathrm{mcd}(5600, 1764) = \mathrm{mcd}(224, 84) = \mathrm{mcd}(84, 56).$$

Dividim 84 entre 56. Ens queda quocient $q = 1$, residu $r = 84 - 56 = 28$. Per tant,

$$\mathrm{mcd}(5600, 1764) = \mathrm{mcd}(84, 56) = \mathrm{mcd}(56, 28).$$

Dividim 56 entre 28. Ens queda quocient $q = 2$, residu $r = 0$. Per tant,

$$\mathrm{mcd}(5600, 1764) = \mathrm{mcd}(56, 28) = \mathrm{mcd}(28, 0) = 28.$$

De tot aquest procediment hem deduït que

$$\mathrm{mcd}(5600, 1764) = 28.$$

Ho podem resumir en aquesta taula:

quocients			3	5	1	2	1	2
residus	5600	1764	308	224	84	56	28	0

El màxim comú divisor és el darrer residu abans del 0.

Suposem que volem calcular $\mathrm{mcd}(a, b)$:

Algoritme

Input: a, b
Anomenem $r_{-2} = a$, $r_{-1} = b$.
Sigui $i = -1$.
Mentres $r_i \neq 0$,

- incrementem i en un,
- definim q_i, r_i com el quocient i el residu de la divisió de r_{i-2} entre r_{i-1}.

Output: r_{i-1}.

Nota (p.24)

Identitat de Bézout

Utilitzant la notació de l'algoritme d'Euclides podem posar la taula d'aquesta forma:

i	-2	-1	0	1	2	3	4	5
q_i			3	5	1	2	1	2
r_i	5600	1764	308	224	84	56	28	0

A cada pas tenim

$$r_i = r_{i-2} - q_i r_{i-1}.$$

Si ara definim $\lambda_{-2} = 1$, $\mu_{-2} = 0$, es compleix

$$r_{-2} = \lambda_{-2} \cdot 5600 + \mu_{-2} \cdot 1764$$

i si definim $\lambda_{-1} = 0$, $\mu_{-1} = 1$, es compleix

$$r_{-1} = \lambda_{-1} \cdot 5600 + \mu_{-1} \cdot 1764.$$

Suposem que fins al pas $k = i - 1$ es compleix que

$$r_k = \lambda_k \cdot 5600 + \mu_k \cdot 1764.$$

Podem continuar definint recursivament a cada pas

$$\lambda_i = \lambda_{i-2} - q_i \lambda_{i-1},$$

$$\mu_i = \mu_{i-2} - q_i \mu_{i-1}.$$

Això ens permet escriure

$$\begin{aligned} r_i &= r_{i-2} - q_i r_{i-1} \\ &= (\lambda_{i-2} \cdot 5600 + \mu_{i-2} \cdot 1764) - q_i(\lambda_{i-1} \cdot 5600 + \mu_{i-1} \cdot 1764) \\ &= (\lambda_{i-2} - q_i \lambda_{i-1}) \cdot 5600 + (\mu_{i-2} - q_i \mu_{i-1}) \cdot 1764 \\ &= \lambda_i \cdot 5600 + \mu_i \cdot 1764 \end{aligned}$$

Aquest procediment ens permet obtenir l'anomenada **identitat de Bézout**.

Teorema 2: Identitat de Bézout

Donats dos enters a i b, definim $r_{-2} = a$, $r_{-1} = b$ i, per $i \geq 0$, definim recursivament r_i i q_i com el residu i el quocient de dividir r_{i-2} entre r_{i-1}. A més a més, definim $\lambda_{-2} = 1$, $\mu_{-2} = 0$, $\lambda_{-1} = 0$, $\mu_{-1} = 1$ i, per $i \geq 0$ definim

$$\lambda_i = \lambda_{i-2} - q_i \lambda_{i-1} \qquad \mu_i = \mu_{i-2} - q_i \mu_{i-1}$$

Aleshores,

- Existeix $k \geq 0$ tal que $r_{k+1} = 0$.
- Es compleix $\mathrm{mcd}(a, b) = r_k$.
- Per tot $i \geq 0$ es compleix $\lambda_i a + \mu_i b = r_i$.

En particular, si definim $\lambda = \lambda_k$ i $\mu = \mu_k$, aleshores es compleix l'anomenada **Identitat de Bézout**,

$$\lambda a + \mu b = \mathrm{mcd}(a, b).$$

Els coeficients λ i μ de la identitat de Bézout es poden trobar per la manera que acabem de descriure.

Vegem-ho en la següent taula on, per cada i a partir de $i = 0$, calculem $\lambda_i = \lambda_{i-2} - q_i \lambda_{i-1}$ i $\mu_i = \mu_{i-2} - q_i \mu_{i-1}$.

i	-2	-1	0	1	2	3	4	5
λ_i	1	0	1	-5	6	-17	23	
μ_i	0	1	-3	16	-19	54	-73	
q_i			3	5	1	2	1	2
r_i	5600	1764	308	224	84	56	28	0

Comprovem que $23 \cdot 5600 - 73 \cdot 1764 = 128800 - 128772 = 28 = \mathrm{mcd}(5600, 1764)$.

Exercici 11

Calculeu el màxim comú divisor de les següents parelles d'enters i expresseu-lo com a combinació lineal dels dos enters.

- 365 i 70 Solució (p.23)
- 2671 i 156 Solució (p.23)

Exercici 12

Sabem que donats dos enters a, b *coprimers*, n'existeixen dos més, λ i μ tals que $\lambda a + \mu b = 1$. Demostreu el recíproc, és a dir, si donats dos enters a i b, n'existeixen dos més, λ i μ tals que $\lambda a + \mu b = 1$, aleshores a i b són coprimers.

Solució (p.24)

Exercici 13

Sabem que donats dos enters a, b *qualssevol*, si d és el $\mathrm{mcd}(a, b)$, aleshores existeixen dos enters més, λ i μ tals que $\lambda a + \mu b = d$. Demostreu amb un contraexemple que no sempre és cert que si existeixen dos enters λ i μ tals que $\lambda a + \mu b = d$, aleshores $d = \mathrm{mcd}(a, b)$.

Solució (p.24)

Exercici 14

Demostreu que donats dos enters a i b *qualssevol*, els enters $\frac{a}{\mathrm{mcd}(a,b)}$ i $\frac{b}{\mathrm{mcd}(a,b)}$ són coprimers.

Solució (p.24)

1.3 Nombres primers i teorema fonamental de l'artimètica

Nombres primers

Nombres primers

Diem que un nombre positiu és **primer** si els seus divisors són exactament quatre i són ± 1 i $\pm p$.

S'exclou d'aquesta definició el nombre 1.

Aplicant la definició de nombres primers, veiem que qualsevol enter es pot descompondre en producte de nombres primers.

Del treball que hem fet amb el 12, deduïm que

$$12 = 2 \cdot 6.$$

Això és una descomposició, però no ho és en primers perquè el 6 no és primer. Per resoldre-ho descomponem també el 6 i apliquem la propietat associativa:

$$12 = 2 \cdot 6 = 2 \cdot (2 \cdot 3) = 2 \cdot 2 \cdot 3.$$

Teorema fonamental de l'aritmètica

Exercici 15

1. Utilitzeu la identitat de Bézout per demostrar que si $a \mid bc$ i $\mathrm{mcd}(a, b) = 1$, aleshores $a \mid c$.
2. Demostreu que si p és primer i $p \mid ab$ aleshores $p \mid a$ o bé $p \mid b$.
3. Demostreu que si p és primer i $p \mid a_1 \cdot a_2 \cdot \cdots \cdot a_t$, aleshores existeix algun i entre 1 i t tal que $p \mid a_i$.

Solució (p.24)

Teorema 3: Teorema fonamental de l'aritmètica

Qualsevol enter descompon en productes de primers i aquesta descomposició és única.

La construcció anterior justifica que existeix la descomposició. La unicitat és una conseqüència del darrer apartat de l'Exercici 15.

Exercici 16

Demostreu el Teorema Fonamental de l'Aritmètica.

Inifinitud dels nombres primers

Teorema 4

Hi ha infinits nombres primers. Nota (p.24)

Demostració. *Procedim per reducció a l'absurd.*
Suposem que $p_1 < \cdots < p_n$ *són tots els primers.*
Aleshores $p_1 \cdot \cdots \cdot p_n + 1$ *també és primer (perquè no hi ha cap primer que el divideixi, per l'Exercici 7).*
Però, en canvi, és més gran que p_n.
Això és una contradicció. □

1.4 Solucions

Solució de l'Exercici 3

Si $a \mid b$, aleshores existeix q pel qual $b = aq$.
Si $b \mid c$, aleshores existeix q' pel qual $c = bq'$.
Per tant, $c = bq' = (aq)q' = a(qq')$.

Torna a l'exercici (p.14)

Solució de l'Exercici 4

Si $a \mid b$, aleshores existeix q pel qual $b = aq$.
Si, a més a més, $d \mid a$ i $d \mid b$, aleshores existeixen $q_a = \frac{a}{d}$ i $q_b = \frac{b}{d}$ pels quals $a = dq_a$ i $b = dq_b$.
Aleshores $dq_b = dq_a q$ que, per la propietat de l'invers de $\mathbb{Z}$, implica que $q_b = q_a q$ i, per tant,

$$\frac{a}{d} \mid \frac{b}{d}.$$

Torna a l'exercici (p.14)

Solució de l'Exercici 5

- Si $a \mid b$, aleshores existeix un enter q pel qual $b = qa$. En aquest cas, $-b = -qa = (-q)a$, i, per tant, $a \mid -b$.
- Si $a \mid b$ i $a \mid c$, aleshores existeixen enters q_0 i q_1 pels quals $b = q_0 a$ i $c = q_1 a$. Per tant, $b + c = (q_0 + q_1)a$ i $b - c = (q_0 - q_1)a$, el que implica que $a \mid b + c$ i $a \mid b - c$.

Torna a l'exercici (p.15)

Solució de l'Exercici 6

Podem fer servir el fet que $r = a - bq$. Com que a i bq són divisibles per d, r també ho és (per l'exercici anterior).

Torna a l'exercici (p.15)

Solució de l'Exercici 7

Podem demostrar-ho per reducció a l'absurd. Suposem que un enter $d > 1$ és divisor de $qd + 1$. Aleshores existeix q' pel qual $q'd = qd + 1$. Per l'exercici anterior, d és divisor de 1. Per tant, d és 1 o -1, fet que contradiu $d > 1$.

Torna a l'exercici (p.15)

Solució de l'Exercici 9

És suficient veure que un enter divideix a i b si i només si divideix b i r.

- Si $d \mid a$ i $d \mid b$, aleshores $d \mid r$ per l'Exercici 6.
- Si $d \mid b$ i $d \mid r$, aleshores existeixen b' i r' pels quals $b = db'$ $r = dr'$. Per tant, $a = bq + r = db'q + dr' = d(b'q + r')$.

Torna a l'exercici (p.17)

Solució de l'Exercici 11

i	-2	-1	0	1	2	3
λ_i	1	0	1	-4	5	
μ_i	0	1	-5	21	-26	
q_i			5	4	1	2
r_i	365	70	15	10	5	0

Pas base

$r_{-2} = 365$ $\lambda_{-2} = 1$ $\mu_{-2} = 0$

$r_{-1} = 70$ $\lambda_{-1} = 0$ $\mu_{-1} = 1$

Pas 0

$365 = 70 \times 5 + 15$

$r_0 = 15$, $q_0 = 5$

$\lambda_0 = \lambda_{-2} - q_0\lambda_{-1} = 1 - 5(0) = 1$

$\mu_0 = \mu_{-2} - q_0\mu_{-1} = 0 - 5(1) = -5$

Pas 1

$70 = 15 \times 4 + 10$

$r_1 = 10$, $q_1 = 4$

$\lambda_1 = \lambda_{-1} - q_1\lambda_0 = 0 - 4(1) = -4$

$\mu_1 = \mu_{-1} - q_1\mu_0 = 1 - 4(-5) = 21$

Pas 2

$15 = 10 \times 1 + 5$

$r_2 = 5$, $q_2 = 1$

$\lambda_2 = \lambda_0 - q_2\lambda_1 = 1 - 1(-4) = 5$

$\mu_2 = \mu_0 - q_2\mu_1 = -5 - 1(21) = -26$

Pas 3

$10 = 5 \times 2 + 0$

Identitat de Bézout buscada

$5 \times 365 + (-26) \times 70 = \text{mcd}(365, 70)$

En efecte,

$5 \times 365 + (-26) \times 70 = 1825 - 1820 = 5$

Torna a l'exercici (p.20)

Solució de l'Exercici 1.2

i	-2	-1	0	1	2	3	4
λ_i	1	0	1	-8	33	-41	
μ_i	0	1	-17	137	-565	702	
q_i			17	8	4	1	3
r_i	2671	156	19	4	3	1	0

Identitat de Bézout buscada:

$(-41) \times 2671 + (702) \times 156 = \text{mcd}(2671, 156) = 1$

En efecte,

$(-41) \times 2671 + (702) \times 156 = -109511 + 109512 = 1$

Torna a l'exercici (p.20)

Solució de l'Exercici 12

Suposem que existeixen dos enters λ i μ tals que

$$\lambda a + \mu b = 1.$$

Si $\mathrm{mcd}(a, b) \neq 1$, aleshores ha d'existir un divisor $d > 1$ comú de a i de b. Aleshores existeixen enters q_a i q_b tals que $a = dq_a$ i $b = dq_b$ i, per tant, $\lambda dq_a + \mu dq_b = 1$. Deduïm que

$$d(\lambda q_a + \mu q_b) = 1.$$

Com que tant d com $\lambda q_a + \mu q_b$ són enters, la igualtat anterior només serà possible si $d = 1$. Per tant, a i b han de ser coprimers.

Torna a l'exercici (p.20)

Solució de l'Exercici 13

Per exemple, $5, 7$ són coprimers i $6 \cdot 5 + (-4) \cdot 7 = 2 \neq \mathrm{mcd}(5, 7)$.

Torna a l'exercici (p.20)

Solució de l'Exercici 14

Per la identitat de Bézout sabem que existeixen enters λ i μ tals que

$$\lambda a + \mu b = \mathrm{mcd}(a, b).$$

Per tant, tenim que els mateixos enters λ i μ compleixen

$$\lambda \frac{a}{\mathrm{mcd}(a, b)} + \mu \frac{b}{\mathrm{mcd}(a, b)} = 1.$$

Ara, per l'Exercici 12 deduïm que $\frac{a}{\mathrm{mcd}(a,b)}$ i $\frac{b}{\mathrm{mcd}(a,b)}$ són coprimers.

Torna a l'exercici (p.20)

Solució de l'Exercici 15

1. Per la identitat de Bézout sabem que existeixen λ i μ tals que $\lambda a + \mu b = 1$. Multipliquem la igualtat per c i obtenim $\lambda ac + \mu bc = c$. Com que $a \mid bc$, deduïm que $a \mid c$.
2. Si $p \nmid a$, aleshores $\mathrm{mcd}(a, p) = 1$ i, pel punt anterior, deduïm que $p \mid b$.
3. Es pot demostrar per inducccció sobre t utilitzant els passos anteriors.

Torna a l'exercici (p.21)

1.5 Notes històriques

- Aquest algoritme per calcular el mcd s'atribueix a Euclides (300 aC aprox.). Euclides va desenvolupar una gran tasca a l'Alexandria Ptolomeica estudiant i recopilant els resultats matemàtics que es coneixien en aquell moment. Tot aquest saber es va exposar magistralment en un tractat compost de tretze volums conegut com els Elements d'Euclides.
  Torna (p.19)
- Teorema 4: Aquest resultat i aquesta demostració també apareixen als Elements d'Euclides. De fet, també és conegut com el teorema d'Euclides. Torna (p.21)

2 Aritmètica modular

2.1 Congruències

Relació de congruència

Definició

Si r és el residu de dividir a per m, aleshores diem que r és la **reducció de a mòdul m**. Escriurem

$$a = r \mod m.$$

Lema 1

Donats dos enters a, b i $m > 0$, és equivalent:

- Els residus de dividir a i b entre m coincideixen.
- $a - b$ és un múltiple de m.

Exemple. *Exemple amb* $m = 7$

Si dos nombres tenen el mateix residu quan els divideixo entre 7*,*

(Exemple: $52 = 7 \times 7 + 3$*,* $73 = 7 \times 10 + 3$*)*

aleshores la seva diferència és un múltiple de 7*.*

(Exemple: $52 - 73 = -21$ *és un múltiple de* 7*)*

Al revés també és cert.

Si la diferència entre dos nombres és un múltiple de 7*,*

(Exemple: $149 - 100 = 49$*)*

aleshores els dos nombres tenen el mateix residu quan els divideixo entre 7*.*

(Exemple: $149 = 7 \times 21 + 2$*,* $100 = 7 \times 14 + 2$*)*

Demostració. (sketch)
$a = q_a m + r$ *i* $b = q_b m + r$ *implica que* $a - b = (q_a - q_b)m$.
$a - b$ *és un múltiple de* m, $a = q_a m + r_a$ *i* $b = q_b m + r_b$, *implica* $(q_a - q_b)m + (r_a - r_b)$ *és un múltiple de* m *i, per tant,* $r_a - r_b$ *és un múltiple de* m. □

Congruència

Dos enters a i b són **congruents mòdul** un enter m si es compleixen les condicions equivalents del lema 1. Escrivim indistintament $a \equiv b \mod m$ o bé $a \equiv b(m)$.

En el cas anterior, diríem

$52 \equiv 73(7)$ o $52 \equiv 73 \mod 7$

i

$149 \equiv 100(7)$ o $149 \equiv 100 \mod 7$

Exemple. *Les congruències mòdul* 7 *les utilitzem en el calendari. Dos dies del mateix mes cauen en el mateix dia de la setmana si són congruents mòdul* 7*.*

Exemple. *També fem congruències mòdul 7 en la interpretació de les notes musicals. Dues notes separades per 7, 14, 21, etc. salts de nota són la mateixa llevat d'un canvi d'octava.*

Exemple. *Estem molt familiaritzats amb les congruències mòdul 2. Els nombres només poden ser o bé congruents amb 0 o bé congruents amb 1 mòdul 2. En el primer cas es tracta dels nombres parells, mentre que en el segon cas es tracta dels senars.*

Exercici 17

Demostreu que si $a \equiv b \mod m$ i d divideix m, aleshores $a \equiv b \mod d$. Solució (p.41)

Exemple. *Vegem un exemple del resultat de l'exercici:*

$$8726 \equiv 26 \mod 100$$

Aleshores també tindrem

$$98726 \equiv 26 \mod 50, \qquad 98726 \equiv 26 \mod 10, \ldots$$

El contrari no és cert. Per exemple,

$$1 \equiv 51 \mod 50$$

però, en canvi,

$$1 \not\equiv 51 \mod 100$$

Lema 2

La relació de congruència és una **relació d'equivalència**. És a dir, satisfà les propietats següents:

- **reflexiva** ($a \equiv a \mod m$ per tot a i tot m enters),
- **simètrica** ($a \equiv b \mod m$ si i només si $b \equiv a \mod m$),
- **transitiva** (si $a \equiv b \mod m$ i $b \equiv c \mod m$, aleshores $a \equiv c \mod m$).

Diem que a i a' són de la mateixa **classe d'equivalència** mòdul m si $a \equiv a' \mod m$.

Operacions amb congruències

Lema 3: La suma i el producte de classes queden ben definits

Si $a_1 \equiv a_2 \mod m$ i $b_1 \equiv b_2 \mod m$, aleshores

$$a_1 + b_1 \equiv a_2 + b_2 \mod m,$$

$$a_1 \cdot b_1 \equiv a_2 \cdot b_2 \mod m.$$

Per exemple, tenim que

$$\begin{aligned} 5 &\equiv 12 \mod 7 \\ 11 &\equiv -3 \mod 7 \end{aligned}$$

El que ens diu el lema és que, aleshores,

$$\begin{aligned} 5+11 &\equiv 12-3 \mod 7 \\ 5\cdot 11 &\equiv 12\cdot(-3) \mod 7 \end{aligned}$$

Les classes d'equivalència ens permetran fer els càlculs de manera més fàcil. Per exemple, si vull calcular la reducció mòdul 3 de

$$754 + 389 \quad , \quad 754 \cdot 389 \quad \text{o} \quad 754^{1000}$$

puc reduir primer els operands:

$$\begin{aligned} 754 &= 1 \mod 3 \\ 389 &= 2 \mod 3, \end{aligned}$$

i les operacions em queden reduïdes a

$$1+2 \equiv 0 \mod 3 \quad , \quad 1\cdot 2 \equiv 2 \mod 3 \quad \text{i} \quad 1^{1000} \equiv 1 \mod 3$$

Una altra conseqüència del lema 3, és que si $a \equiv b \mod m$, aleshores $ka \equiv kb \mod m$.

Però el recíproc no és cert.

La simplificació no queda ben definida.

És a dir, pot ser que $ka \equiv kb \mod m$, però, en canvi, $a \not\equiv b \mod m$.

Per exemple, $2 \cdot 1 \equiv 2 \cdot 3 \mod 4$, però, en canvi, $1 \not\equiv 3 \mod 4$.

Lema 4

Si $\text{mcd}(k, m) = 1$, aleshores podem simplificar:

$$ka \equiv kb \mod m \Longleftrightarrow a \equiv b \mod m.$$

Demostració. *Suposem que* $\mathrm{mcd}(k,m)=1$.

$$\begin{aligned} ka \equiv kb \mod m &\iff m \mid k(a-b) \\ &\iff m \mid a-b \\ &\iff a \equiv b \mod m \end{aligned}$$

□

Lema 5

En general, agafant $k' = \frac{k}{\mathrm{mcd}(k,m)}$ i $m' = \frac{m}{\mathrm{mcd}(k,m)}$, podem simplificar:

$$ka \equiv kb \mod m \iff k'a \equiv k'b \mod m'.$$

Demostració.

$$\begin{aligned} ka \equiv kb \mod m &\iff m \mid k(a-b) \\ &\iff \frac{m}{\mathrm{mcd}(k,m)} \mid \frac{k}{\mathrm{mcd}(k,m)}(a-b) \\ &\iff k'a \equiv k'b \mod m'. \end{aligned}$$

□

Resolució de congruències lineals

Donats enters a, b, m, amb $m > 0$, volem saber per quins valors de x, mòdul m, es compleix que

$$ax \equiv b \mod m.$$

Per exemple, suposem que volem resoldre les congruències lineals següents:

1. $35x \equiv 20(60)$.
2. $32x \equiv 58(60)$.
3. $47x \equiv 17(60)$.
4. $39x \equiv 18(60)$.
5. $51x \equiv 26(60)$.
6. $8x \equiv 8(60)$.

- ***Existeixen solucions?***

Es pot demostrar, utilitzant la identitat de Bézout, que existiran solucions si i només si $\mathrm{mcd}(a,m)$ divideix b.

Vegem si tenen solució les congruències anteriors:

1. $35x \equiv 20(60)$ té solució perquè $\mathrm{mcd}(35, 60) = 5$ divideix 20.
2. $32x \equiv 58(60)$ no té solució perquè $\mathrm{mcd}(32, 60) = 4$ no divideix 58.
3. $47x \equiv 17(60)$ té solució perquè $\mathrm{mcd}(47, 60) = 1$ divideix 17.
4. $39x \equiv 18(60)$ té solució perquè $\mathrm{mcd}(39, 60) = 3$ divideix 18.
5. $51x \equiv 26(60)$ no té solució perquè $\mathrm{mcd}(51, 60) = 3$ no divideix 26.
6. $8x \equiv 8(60)$ té solució perquè $\mathrm{mcd}(8, 60) = 4$ divideix 8.

▸ ***Podem simplificar?***

Si $\mathrm{mcd}(a, m)$ divideix b, aleshores podem dividir tots els paràmetres entre $\mathrm{mcd}(a, m)$.

Vegem com queden simplificades les congruències anteriors, de la forma $a'x \equiv b' \mod m'$, amb $\mathrm{mcd}(a', m') = 1$:

1. $35x \equiv 20(60)$ queda simplificada com $7x \equiv 4(12)$.
2. $32x \equiv 58(60)$ no té solució.
3. $47x \equiv 17(60)$ no es pot simplificar més.
4. $39x \equiv 18(60)$ queda simplificada com $13x \equiv 6(20)$.
5. $51x \equiv 26(60)$ no té solució.
6. $8x \equiv 8(60)$ queda simplificada com $2x \equiv 2(15)$.

▸ ***Un cop hem simplificat, com podem trobar* una *solució?***

Com que ara $\mathrm{mcd}(m', a') = 1$, per la identitat de Bézout existiran λ i μ tals que $\mu a' = 1 - \lambda m' \equiv 1 \mod m'$.

Busquem, doncs, aquest paràmetre μ de la identitat de Bézout.

Un cop tenim el paràmetre μ tal que
$$\mu a' \equiv 1 \mod m',$$
deduïm que
$$(b'\mu)a' \equiv b' \mod m'$$
i, per tant,
$$x \equiv b'\mu$$
és una primera solució.

1. $35x \equiv 20(60)$ queda simplificada com
$$7x \equiv 4(12)$$
i per això resolem primer $7x' \equiv 1(12)$:

λ	1	0	1	−1	3	
μ	0	1	−1	2	−5	
quocients			1	1	2	
residus	12	7	5	2	1	0

Deduïm que $(12)\cdot(3)+(7)\cdot(-5)=1$ i, per tant,

$$7\cdot 7\equiv 1 \mod 12.$$

Multiplicant-ho tot per 4, es complirà

$$\begin{aligned} 7(7\cdot 4) &\equiv 1\cdot 4 \mod 12\\ 7\cdot 28 &\equiv 4 \mod 12\\ 7\cdot 4 &\equiv 4 \mod 12. \end{aligned}$$

Per tant,

$$x\equiv 4(12)$$

és *una* solució.

2. $32x\equiv 58(60)$ no té solució.
3. $47x\equiv 17(60)$ no es pot simplificar més. Resolem primer $47x'\equiv 1(60)$:

λ	1	0	1	−3	4	−7	11	−18	
μ	0	1	−1	4	−5	9	−14	23	
quocients			1	3	1	1	1	1	
residus	60	47	13	8	5	3	2	1	0

Deduïm que $(60)\cdot(-18)+(47)\cdot(23)=1$ i, per tant,

$$47\cdot 23\equiv 1 \mod 60.$$

Multiplicant-ho tot per 17, es complirà

$$\begin{aligned} 47(23\cdot 17) &\equiv 1\cdot 17 \mod 60\\ 47\cdot 391 &\equiv 17 \mod 60\\ 47\cdot 31 &\equiv 17 \mod 60. \end{aligned}$$

Per tant,

$$x\equiv 31(60)$$

és *una* solució.

4. $39x\equiv 18(60)$ queda simplificada com

$$13x\equiv 6(20)$$

i per això resolem primer $13x'\equiv 1(20)$:

λ	1	0	1	−1	2	
μ	0	1	−1	2	−3	
quocients			1	1	1	
residus	20	13	7	6	1	0

Deduïm que $(20)\cdot(2)+(13)\cdot(-3)=1$ i, per tant,

$$13\cdot 17\equiv 1 \mod 20.$$

Multiplicant-ho tot per 6, es complirà

$$\begin{aligned} 13(17\cdot 6) &\equiv 1\cdot 6 \mod 20 \\ 13\cdot 102 &\equiv 6 \mod 20 \\ 13\cdot 2 &\equiv 6 \mod 20. \end{aligned}$$

Per tant,

$$x \equiv 2(20)$$

és *una* solució.

5. $51x \equiv 26(60)$ no té solució.

6. $8x \equiv 8(60)$ queda simplificada com

$$2x \equiv 2(15)$$

i per això resolem primer $2x' \equiv 1(15)$:

λ	1	0	1	
μ	0	1	−7	
quocients			7	
residus	15	2	1	0

Deduïm que $(15)\cdot(1) + (2)\cdot(-7) = 1$ i, per tant,

$$2\cdot 8 \equiv 1 \mod 15.$$

Multiplicant-ho tot per 2, es complirà

$$\begin{aligned} 2(8\cdot 2) &\equiv 1\cdot 2 \mod 15 \\ 2\cdot 16 &\equiv 2 \mod 15 \\ 2\cdot 1 &\equiv 2 \mod 15. \end{aligned}$$

Per tant,

$$x \equiv 1(15)$$

és *una* solució.

▸ ***Com trobem* totes *les solucions en el mòdul original?***

Si $a'x_0 \equiv b'(m')$, aleshores també

$$\begin{aligned} a'(x_0 + m') &\equiv b'(m'), \\ a'(x_0 + 2m') &\equiv b'(m'), \\ a'(x_0 + 3m') &\equiv b'(m'), \\ &\vdots \end{aligned}$$

Totes les solucions mòdul m seran

$$x_0, x_0 + m', x_0 + 2m', x_0 + 3m', \ldots, x_0 + (m - m').$$

En total n'hi haurà

$$m/m' = \mathrm{mcd}(a, m).$$

1. $35x \equiv 20(60)$ tenia solució $x \equiv 4(12)$. Totes les seves solucions mòdul 60 seran $x = 4, 16, 28, 40, 52(60)$. Observem que n'hi ha $5 = \mathrm{mcd}(35, 60)$.
2. $32x \equiv 58(60)$ no té solució.
3. $47x \equiv 17(60)$ només té una solució, ja que $\mathrm{mcd}(47, 60) = 1$. La solució és $x \equiv 31(60)$.
4. $39x \equiv 18(60)$ tenia solució $x \equiv 2(20)$. Totes les seves solucions mòdul 60 seran $x = 2, 22, 42(60)$. Observem que n'hi ha $3 = \mathrm{mcd}(39, 60)$.
5. $51x \equiv 26(60)$ no té solució.
6. $8x \equiv 8(60)$ tenia solució $x \equiv 1(15)$. Totes les seves solucions mòdul 60 seran $x = 1, 16, 31, 46(60)$. Observem que n'hi ha $4 = \mathrm{mcd}(8, 60)$.

Sumari

Lema 6

Considerem la congruència $ax \equiv b \mod m$.

1. Té solució si i només si $\mathrm{mcd}(a, m) \mid b$.
2. L'enter x és solució de $ax \equiv b \mod m$ si i només si ho és de
$$\frac{a}{\mathrm{mcd}(a,m)}x \equiv \frac{b}{\mathrm{mcd}(a,m)} \mod \frac{m}{\mathrm{mcd}(a,m)}.$$
3. Si existeix una solució x_0, aleshores n'existeixen $\mathrm{mcd}(a, m)$ i el conjunt de solucions és donat per
$$x \equiv x_0 + k\frac{m}{\mathrm{mcd}(a,m)} \mod m,$$
amb $k = 0, 1, \ldots, \mathrm{mcd}(a, m) - 1$.

Procediment per resoldre $ax \equiv b \mod m$

- Si $\mathrm{mcd}(a, m) \nmid b$, aleshores no hi ha solució.
- Si $\mathrm{mcd}(a, m) \mid b$
  - Si $\mathrm{mcd}(a, m) = 1$
    - Calculem els coeficients λ i μ de la identitat de Bézout
    $$\lambda m + \mu a = 1.$$
    - La solució és única i és $x \equiv \mu b \mod m$.
  - Si $\mathrm{mcd}(a, m) \neq 1$
    - Busquem la solució x_0 de la congruència
    $$\frac{a}{\mathrm{mcd}(a,m)}x \equiv \frac{b}{\mathrm{mcd}(a,m)} \mod \frac{m}{\mathrm{mcd}(a,m)}$$
    que compleix $\mathrm{mcd}(\frac{a}{\mathrm{mcd}(a,m)}, \frac{m}{\mathrm{mcd}(a,m)}) = 1$.
    - El conjunt de solucions serà
    $$x \equiv x_0 + k\frac{m}{\mathrm{mcd}(a,m)} \mod m,$$
    amb $k = 0, \ldots, \mathrm{mcd}(a, m) - 1$.

2.2 Aritmètica modular

Anells $\mathbb{Z}_m$

Pel lema 2 sabem que la relació de congruència és una relació d'equivalència.

Per això, podem dividir $\mathbb{Z}$ en m classes d'equivalència donades per la relació de congruència mòdul m.

Definim $\mathbb{Z}_m$ com el conjunt de les m classes d'equivalència.

Així,

$$\mathbb{Z}_m = \{[0]_m, [1]_m, \ldots, [m-1]_m\},$$

on $[r]_m$ representa la classe de tots els enters que dividits entre m tenen residu r.

Per extensió, escriurem $[a]_m = [r]_m$ si $a = qm + r$ amb $0 \leq r < m$.

Exemple. *En el cas de $\mathbb{Z}_2$, la classe de $[0]_2$ és la classe dels nombres parells, i $[1]_2$ la dels nombres imparells.*

Exemple. *En el cas de $\mathbb{Z}_3$, dividim el conjunt d'enters d'acord amb el residu de la divisió per 3:*

$$\begin{array}{c} \mathbb{Z} \\ \\ \ldots \quad -2 \quad -1 \quad 0 \quad 1 \quad 2 \quad 3 \quad 4 \quad \ldots \end{array} \quad \rightarrow \quad \begin{array}{c|c|c} [0]_3 & [1]_3 & [2]_3 \\ \vdots & \vdots & \vdots \\ -3 & -2 & -1 \\ 0 & 1 & 2 \\ 3 & 4 & 5 \\ \vdots & \vdots & \vdots \end{array}$$

Per tant,

$$\begin{aligned} [0]_3 &= \{\ldots, -3, 0, 3, 6, \ldots\} = \{3k \,:\, k \in \mathbb{Z}\} \\ [1]_3 &= \{\ldots, -2, 1, 4, 7, \ldots\} = \{3k+1 \,:\, k \in \mathbb{Z}\} \\ [2]_3 &= \{\ldots, -1, 2, 5, 8, \ldots\} = \{3k+2 \,:\, k \in \mathbb{Z}\} \end{aligned}$$

Podem veure que, en general,

$$[r]_m = \{mk + r \,:\, k \in \mathbb{Z}\}$$

El conjunt format per les classes d'equivalència d'una relació d'equivalència s'anomena **conjunt quocient**. Més endavant veurem altres conjunts quocients.

Aritmètica modular

Pel lema 3 sabem que dins de $\mathbb{Z}_m$ hi ha les dues operacions internes ben definides:

$$[r_1]_m + [r_2]_m = [r_1 + r_2]_m,$$

$$[r_1]_m \cdot [r_2]_m = [r_1 \cdot r_2]_m.$$

Ara analitzem les propietats de $(\mathbb{Z}_m, +, \cdot)$:

- L'operació suma a $\mathbb{Z}_m$ és associativa i commutativa perquè ho és a $\mathbb{Z}$.

- El neutre per a la suma és $[0]_m$ i l' invers per a la suma està ben definit com
$$-[a]_m = [-a]_m.$$
La resta està ben definida, aleshores, com la suma de l'invers.
- L'operació producte a $\mathbb{Z}_m$ és associativa i commutativa perquè ho és a $\mathbb{Z}$ i satisfà la propietat distributiva amb la suma.
- El neutre pel producte és $[1]_m$.

Per tot l'anterior, podem afirmar el següent:

> $(\mathbb{Z}_m, +, \cdot)$ és un anell commutatiu amb unitat.

En aquest curs només considerarem la suma i el producte a $\mathbb{Z}_m$ que acabem de definir. Per tant, per simplificar la notació, quan parlem de $\mathbb{Z}_m$ ens referim a l'anell $(\mathbb{Z}_m, +, \cdot)$.

En general, $\mathbb{Z}_m$ no és un cos perquè pot haver-hi elements que no tinguin invers. Per exemple, a $\mathbb{Z}_4$,

$$[2]_4 \cdot [0]_4 = [0]_4,$$
$$[2]_4 \cdot [1]_4 = [2]_4,$$
$$[2]_4 \cdot [2]_4 = [0]_4,$$
$$[2]_4 \cdot [3]_4 = [2]_4.$$

Per tant, no existeix cap classe $[a]_4$ tal que $[2]_4 \cdot [a]_4 = [1]_4$.

Per simplificar la notació, sovint escriurem a en comptes de $[a]_m$.

Exercici 18

Comproveu que a $\mathbb{Z}_2$ es compleix:
- $-a = a$ per tot a,
- $(a+b)^2 = a^2 + b^2$.
- Demostreu per inducció que a $\mathbb{Z}_2$ es compleix $(a_1 + a_2 + \cdots + a_n)^2 = a_1^2 + a_2^2 + \cdots + a_n^2$, per tot n.

Solució (p.42)

Exercici 19

Comproveu que a $\mathbb{Z}_p$, amb p primer, es compleix que
$$(a_1 + a_2 + \cdots + a_n)^p = a_1^p + a_2^p + \cdots + a_n^p,$$
per tot n.

Taules d'operacions

Coneixem les taules de la suma i el producte binaris:

+	0	1
0	0	1
1	1	0

×	0	1
0	0	0
1	0	1

Podem construir les mateixes taules per a qualsevol mòdul.

Vegem, per exemple, les taules de la suma i el producte mòdul 6:

$+$	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

$\times$	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

. . . i les taules de la suma i el producte mòdul 7:

$+$	0	1	2	3	4	5	6
0	0	1	2	3	4	5	6
1	1	2	3	4	5	6	0
2	2	3	4	5	6	0	1
3	3	4	5	6	0	1	2
4	4	5	6	0	1	2	3
5	5	6	0	1	2	3	4
6	6	0	1	2	3	4	5

$\times$	0	1	2	3	4	5	6
0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6
2	0	2	4	6	1	3	5
3	0	3	6	2	5	1	4
4	0	4	1	5	2	6	3
5	0	5	3	1	6	4	2
6	0	6	5	4	3	2	1

Podem fer algunes observacions en aquestes taules:

- Les taules són simètriques. Això és a causa de la commutativitat de les operacions.
- A la taula de la suma, la fila corresponent al 0 és una còpia de la primera fila. Això ens indica que el 0 és el neutre per a la suma.
- A la taula del producte, la fila corresponent a l'1 és una còpia de la primera fila. Això ens indica que l'1 és el neutre pel producte.

Invertibles i divisors de zero

Sigui $(A, +, \cdot)$ un anell amb neutre 0 respecte de $+$.

Si per un element a n'existeix un altre (que anomenem a^{-1}) tal que $a \cdot a^{-1} = 1$, aleshores diem que a^{-1} és l'**invers** de a.

Per exemple, a $\mathbb{Z}_5$, l'invers de 2 és $2^{-1} = 3$, perquè a $\mathbb{Z}_5$, $2 \cdot 3 = 6 = 1$.

Compte: si $a \in \mathbb{Z}$, l'element a^{-1} dins de $\mathbb{Z}_m$ no el podem confondre amb el racional $\frac{1}{a}$.

Invertibles i divisors de zero

Els elements de A que tenen invers es diuen **invertibles**.
Un element $a \in A$, $a \neq 0$ és un **divisor de zero** si existeix $b \in A$, $b \neq 0$ tal que $a \cdot b = b \cdot a = 0$.

Lema 7

Considerem l'anell $\mathbb{Z}_m$ i un element $a \in \mathbb{Z}_m$, $a \neq 0$. Aleshores

1. a és invertible si i només si $\mathrm{mcd}(a, m) = 1$.
2. a és un divisor de zero si i només si $\mathrm{mcd}(a, m) \neq 1$.

Per tant, tot $a \in \mathbb{Z}_m$ és invertible o bé és divisor de zero.

Observem que hem comès un abús de notació al lema, ja que mcd només està definit per parelles d'enters. Però vam veure que si $a_1, a_2 \in [a]_m$, aleshores $\text{mcd}(a_1, m) = \text{mcd}(a_2, m)$ i, per tant, $\text{mcd}(a, m)$ està ben definit.

Demostració. *Pel lema 6, $ax = b \mod m$ té solució si i només si* $\text{mcd}(a, m)$ *divideix b i, en el cas de tenir-ne, el nombre de solucions diferents mòdul m és* $\text{mcd}(a, m)$.

1. *L'element a és invertible si i només si $ax = 1 \mod m$ té solució, que és equivalent al fet que* $\text{mcd}(a, m)$ *divideixi 1 pel lema 6. Com que l'únic divisor positiu de 1 és ell mateix, a serà invertible si i només si* $\text{mcd}(a, m) = 1$.
2. *L'element a és divisor de zero si i només si $ax = 0 \mod m$ té més d'una solució, que és equivalent a* $\text{mcd}(a, m) > 1$ *pel lema 6.*

□

Identitat de Bézout i l'invers d'un element

Si a és invertible a $\mathbb{Z}_m$, aleshores $\text{mcd}(m, a) = 1$.
Per la identitat de Bézout sabem que existiran λ i μ tals que

$$\lambda m + \mu a = 1.$$

Això significa que $\mu a = 1 - \lambda m$ i, per tant,

$$\mu a \equiv 1 \mod m$$

Deduïm, doncs, que $a^{-1} = \mu$.

Teorema 5

$\mathbb{Z}_m$ és un cos si i només si m és primer.

Anomenem $\mathbb{Z}_m^*$ al conjunt d'elements invertibles de $\mathbb{Z}_m$.

Exercici 20

Calculeu $\mathbb{Z}_m^*$ per $1 < m \leq 12$. Solució (p.42)

Funció d'Euler

Ara definim una funció $\phi : \mathbb{N} \to \mathbb{N}$ que s'anomena **funció d'Euler**. Nota (p.49)

Definim, equivalentment,

$$\begin{aligned} \phi(m) &= \#\{a : 0 \leq a < m \text{ i } \text{mcd}(a, m) = 1\} \\ &= \#\mathbb{Z}_m^* \end{aligned}$$

Lema 8

- Si p és primer, aleshores $\phi(p) = p - 1$.
- Si $\text{mcd}(a, b) = 1$, aleshores $\phi(ab) = \phi(a)\phi(b)$.
- Si p és primer, aleshores $\phi(p^k) = p^k - p^{k-1} = p^{k-1}(p-1)$.

El primer punt es pot veure directament de la definició de ϕ. L'últim punt es pot comprovar veient que exactament 1 de cada p enters entre 0 i $p^k - 1$ és no coprimer amb p^k.

Exercici 21

Calculeu

- $\phi(18)$,
- $\phi(27)$,
- $\phi(35)$.

Solució (p.42)

Exercici 22

Comproveu que si la descomposició d'un enter n en producte de primers és $n = p_1^{n_1} \cdots \cdot p_k^{n_k}$, aleshores

$$\phi(n) = p_1^{n_1-1}(p_1 - 1) \cdot p_2^{n_2-1}(p_2 - 1) \cdot \cdots \cdot p_k^{n_k-1}(p_k - 1)$$

Solució (p.43)

Teorema de Fermat i teorema d'Euler

Teorema 6: Teorema de Fermat Nota (p.49)

Si p és primer i $\text{mcd}(a, p) = 1$, aleshores

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

Teorema 7: Teorema d'Euler

Si $\text{mcd}(a, m) = 1$, aleshores

$$a^{\phi(m)} \equiv 1 \mod m.$$

Podeu veure una demostració del teorema d'Euler a l' apèndix (p.48) de la secció.

Exercici 23

Comproveu que el teorema de Fermat és un cas particular del teorema d'Euler.

Els teoremes anteriors són útils per trobar elements inversos.

En efecte, si a és no nul a $\mathbb{Z}_p$, aleshores

$$a^{-1} = a^{p-2} \mod p,$$

i si a és invertible a $\mathbb{Z}_m$, aleshores

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

Exercici 24

1. És $\mathbb{Z}_{27}$ un cos? Per què?
2. Quants elements de $\mathbb{Z}_{27}$ són invertibles?
3. Justifiqueu per què té invers el 8 a $\mathbb{Z}_{27}$.
4. Trobeu l'invers de 8 a $\mathbb{Z}_{27}$ utilitzant la identitat de Bézout.
5. Trobeu l'invers de 8 a $\mathbb{Z}_{27}$ utilitzant el teorema d'Euler.
6. Comproveu que l'element trobat és, en efecte, l'invers.

Solució (p.43)

Ordre i elements primitius

Ordre

L'**ordre** d'un element no nul $a \in \mathbb{Z}_m$ és el mínim exponent $i \neq 0$ tal que $a^i = 1$. El denotem per $\mathbf{ord}_m(a)$.

Lema 9

L'ordre de l'element a de $\mathbb{Z}_m$ existeix si i només si $\mathrm{mcd}(a, m) = 1$.

Demostració. *Si existeix l'ordre de l'element a aleshores existeix l'invers de a, ja que és* $a^{\mathrm{ord}_m(a)-1}$. *Pel lema 7 es dedueix que* $\mathrm{mcd}(a, m) = 1$.
Si $\mathrm{mcd}(a, m) = 1$, *pel teorema d'Euler existeix un exponent positiu tal que a elevat a l'exponent dona* 1. *Per tant, hi haurà un exponent positiu* mínim *tal que a elevat a l'exponent dona* 1. □

Exercici 25

Comproveu si a $\mathbb{Z}_{18}$ les classes de 3 i 7 tenen ordre, fent servir la definició i fent servir la condició anterior.

Solució (p.43)

Exercici 26

Demostreu que si $a \in \mathbb{Z}_m^*$ i a^{-1} és l'invers de a a $\mathbb{Z}_m$, aleshores $\mathrm{ord}_m(a^{-1}) = \mathrm{ord}_m(a)$. Solució (p.44)

Lema 10

Si $a^k = 1$ a $\mathbb{Z}_m$ per un enter positiu k, aleshores l'ordre de a divideix k.

Demostració. *Suposem que la divisió euclidiana de k per* $\mathrm{ord}_m(a)$ *té quocient q i residu r, aleshores* $a^k = (a^{\mathrm{ord}_m(a)})^q a^r$. *Però com que* $a^k = 1$ *i* $a^{\mathrm{ord}_m(a)} = 1$, *aleshores* $a^r = 1$. *Això, tenint en compte que* $0 \leq r < \mathrm{ord}_m(a)$, *només és possible si* $r = 0$, *és a dir, si* $\mathrm{ord}_m(a) \mid k$. □

En conseqüència, tenim el resultat següent:

L'ordre de qualsevol element divideix $\phi(m)$.

Exercici 27

Calculeu l'ordre de tots els elements de $\mathbb{Z}_7$ i comproveu que tots els ordres divideixen $\phi(7)$.
Solució (p.44)

Elements primitius

Un element de $\mathbb{Z}_m$ és **primitiu** si el seu ordre és $\phi(m)$.

No ha d'existir necessàriament un element primitiu. Per exemple, a $\mathbb{Z}_8$ no hi ha elements primitius.

Exercici 28

Comproveu que $\mathbb{Z}_8$ no té elements primitius.
Solució (p.44)

Si existeix un element primitiu, β, aleshores les seves potències cobreixen tot $\mathbb{Z}_m^*$.

$$\mathbb{Z}_m^* = \{1 = \beta^0, \beta, \beta^2, \ldots, \beta^{\phi(m)-1}\}.$$

Lema 11

Suposem que β és un element primitiu de $\mathbb{Z}_m$. L'element β^j amb $1 \le j < \phi(m)$ també és primitiu si i només si $\mathrm{mcd}(j, \phi(m)) = 1$.

Demostració. *Tindrem que* $(\beta^j)^k = \beta^{kj}$ *és igual a* 1 *si i només si* $\mathrm{ord}_m(\beta) \mid kj$*, és a dir, si i només si* $\phi(m) \mid kj$*.*
Llavors, β^j *serà primitiu si i només si* $\phi(m)$ *no divideix cap dels valors* kj *amb* k *entre* 1 *i* $\phi(m) - 1$*.*
Si $\mathrm{mcd}(j, \phi(m)) \neq 1$*, aleshores* $\phi(m)$ *divideix* $\frac{\phi(m)}{\mathrm{mcd}(j,\phi(m))} j$ *que, pel que acabem de veure, suposa que* β^j *no és primitiu.*
Si $\mathrm{mcd}(j, \phi(m)) = 1$*, aleshores* $\phi(m)$ *només pot dividir* kj *si* $\phi(m)$ *divideix* k*, cosa que no és possible si* $k \le \phi(m) - 1$*. Per tant, en aquest cas* β^j *és primitiu.* $\square$

Com a conseqüència tenim el següent:

Si hi ha un element primitiu, aleshores n'hi ha exactament $\phi(\phi(m))$.

Exercici 29

1. Comproveu que $\mathbb{Z}_{18}$ té elements primitius. Solució (p.44)
2. Quants i quins són els elements primitius de $\mathbb{Z}_{18}$? Solució (p.44)

Exponenciació

Lema 12

- Si $a = mq + r$ amb $0 \le r < m$ i $\text{mcd}(a, m) = 1$, aleshores $a^N \equiv r^N \mod m$ per tot $N > 0$.
- Si $N = \phi(m)q + r$ amb $0 \le r < \phi(m)$, aleshores $a^N = a^r \mod m$.

Demostració.

- *Podem provar-ho per inducció. Per $N = 0$ es compleix. Suposem que es compleix $a^i \equiv r^i \mod m$ per tot $i < N$. Aleshores $a^N \equiv a \cdot a^{N-1} \equiv a \cdot r^{N-1} \equiv (mq + r)r^{N-1} \equiv r^N \mod m$.*
- $a^N \equiv a^{\phi(m)q} a^r \equiv (a^{\phi(m)})^q a^r \equiv a^r \mod m$.

□

2.3 Exercicis

Exercici 30

(a) Calculeu l'invers de 16 a $\mathbb{Z}_{29}$ Solució (p.45)

(b) Calculeu l'invers de 258 a $\mathbb{Z}_{2791}$. Solució (p.45)

Exercici 31

1. Expresseu tots els elements no nuls de $\mathbb{Z}_{19}$ com a potències de 2. Solució (p.45)
2. És possible expressar tots els elements no nuls de $\mathbb{Z}_{23}$ com a potències de 2? Solució (p.46)
3. Busqueu un element β de $\mathbb{Z}_{23}$ tal que tot element no nul de $\mathbb{Z}_{23}$ es pugui escriure com a potència de β. Solució (p.46)

Exercici 32

Sigui l'anell $\mathbb{Z}_{18}$

1. És un cos?
2. Quants elements invertibles té i quins són?
3. Quants divisors de zero té?
4. Busqueu un element primitiu.
5. Quants elements primitius té?

Solució (p.46)

Exercici 33

Sigui l'anell $\mathbb{Z}_{27}$

1. És un cos?
2. Quants elements invertibles té i quins són?
3. Quants divisors de zero té?
4. Busqueu un element primitiu.
5. Busqueu un element diferent de $0, 1$ que no sigui primitiu. Quin ordre té?

Solució (p.46)

Exercici 34

Comproveu que si β és un element primitiu de $\mathbb{Z}_m$ i si k és un enter positiu que divideix $\phi(m)$, aleshores

- $\mathrm{ord}_m(\beta^{\frac{\phi(m)}{k}}) = k$,
- $\mathrm{ord}_m(\beta^k) = \frac{\phi(m)}{k}$.

Solució (p.46)

Exercici 35

Calculeu el residu de dividir

- 4187^{3515} entre 3,
- 4187^{3515} entre 5.

Solució (p.47)

Exercici 36

Trobeu les classes a $\mathbb{Z}_{100}$ de

- 6^{41},
- 7^{41},
- 15^{41}.

Solució (p.47)

Exercici 37

- Quin és el darrer dígit de 7^{378}?
- Quines són les dues darreres xifres de 2793^{2792}?

Solució (p.47)

2.4 Solucions

Solució de l'Exercici 17

$a \equiv b \mod m$ és equivalent al fet que $a - b$ és un múltiple de m.

Si $a - b$ és un múltiple de m, aleshores també ho és de d.

Si $a - b$ és un múltiple de d, aleshores $a \equiv b \mod d$.

Torna a l'exercici (p.26)

Solució de l'Exercici 18

- Podem comprovar que $[0]_2 + [0]_2 = [0]_2$ i que $[1]_2 + [1]_2 = [0]_2$. Per tant, l'oposat de qualsevol $a \in \mathbb{Z}_2$ és a.
- Observem que $1^2 = 1$ i $0^2 = 0$. Aleshores $(a+b)^2 = a^2 + 2ab + b^2 \equiv a^2 + b^2 \equiv a + b \mod 2$.
- Sabem que és cert per $n = 2$. Suposem que és cert fins a $n-1$, aleshores $(a_1 + a_2 + \cdots + a_{n-1} + a_n)^2 = ((a_1 + a_2 + \cdots + a_{n-1}) + a_n)^2 = (a_1 + a_2 + \cdots + a_{n-1})^2 + a_n^2 = a_1^2 + a_2^2 + \cdots + a_{n-1}^2 + a_n^2$.

Torna a l'exercici (p.34)

Solució de l'Exercici 20

- $\mathbb{Z}_2^* = \{1\}$
- $\mathbb{Z}_3^* = \{1, 2\}$
- $\mathbb{Z}_4^* = \{1, 3\}$
- $\mathbb{Z}_5^* = \{1, 2, 3, 4\}$
- $\mathbb{Z}_6^* = \{1, 5\}$
- $\mathbb{Z}_7^* = \{1, 2, 3, 4, 5, 6\}$
- $\mathbb{Z}_8^* = \{1, 3, 5, 7\}$
- $\mathbb{Z}_9^* = \{1, 2, 4, 5, 7, 8\}$
- $\mathbb{Z}_{10}^* = \{1, 3, 7, 9\}$
- $\mathbb{Z}_{11}^* = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$
- $\mathbb{Z}_{12}^* = \{1, 5, 7, 11\}$

Torna a l'exercici (p.36)

Solució de l'Exercici 21

- $$\begin{aligned} \phi(18) &= \phi(2 \cdot 9) \\ &= \phi(2)\phi(9) \text{ (propietat 2)} \end{aligned}$$

  $\phi(2) = 1$ (propietat 1)
  $\phi(9) = \phi(3^2) = 3^2 - 3^1 = 9 - 3 = 6$ (propietat 3)

  $$\begin{aligned} &= 1 \cdot 6 \\ &= 6 \end{aligned}$$

- $$\begin{aligned} \phi(27) &= \phi(3^3) \\ &= 3^3 - 3^2 \text{ (propietat 3)} \\ &= 27 - 9 \\ &= 18 \end{aligned}$$

- $$\begin{aligned} \phi(35) &= \phi(5 \cdot 7) \\ &= \phi(5)\phi(7) \text{ (propietat 2)} \\ &= 4 \cdot 6 \text{ (propietat 1)} \\ &= 24 \end{aligned}$$

Torna a l'exercici (p.37)

Solució de l'Exercici 22

En general

$$\begin{aligned}\phi(n) &= \phi(p_1^{n_1}\cdot p_2^{n_2}\cdot\dots\cdot p_k^{n_k})\\ &= \phi(p_1^{n_1})\cdot\phi(p_2^{n_2})\cdot\dots\cdot\phi(p_k^{n_k}) \text{ (propietat 2)}\\ &= (p_1^{n_1-1}(p_1-1))\cdot(p_2^{n_2-1}(p_2-1))\cdot\dots\cdot(p_k^{n_k-1}(p_k-1)) \text{ (propietat 3)}\end{aligned}$$

Torna a l'exercici (p.37)

Solució de l'Exercici 24

1. No, perquè 27 no és primer.
2. $\phi(27) = 27 - 9 = 18$.
3. Perquè $\text{mcd}(8, 27) = 1$.
4. Utilitzem l'algoritme d'Euclides per trobar els coeficients de la identitat de Bézout:

1	0	1	−2	3
0	1	−3	7	−10
		3	2	1
27	8	3	2	1

   Deduïm que $3\cdot 27 + (-10)\cdot 8 = 1$. Reduint mòdul 27 obtenim $(-10)\cdot 8 = 17\cdot 8 = 1$ i, per tant, l'invers de 8 mòdul 27 és 17.

5. Pel teorema d'Euler tenim que $8^{18} = 1 \mod 27$, d'on deduïm que a $\mathbb{Z}_{27}$ l'invers de 8 és 8^{17}. Podem calcular aquesta potència de moltes maneres diferents. En posem una de possible: com que podem reduir els exponents per múltiples de $\phi(27) = 18$, tenim $8^{17} = 2^{3\cdot 17} = 2^{17+17+17} = 2^{17}2^{17}2^{17}$ (perquè $2^{17} = 2^{-1}$, a causa del fet que $2\cdot 2^{17} = 1$) $= 2^{17}2^{-1}2^{-1} = 2^{17-1-1} = 2^{15} = 2^5\cdot 2^5\cdot 2^5 = 32\cdot 32\cdot 32$ (perquè $32 \equiv 5 \mod 27$)
   $= 5\cdot 5\cdot 5 = 125 = 4\cdot 27 + 17 = 17$.
6. Es tracta de comprovar que $8\cdot 17 = 1$ a $\mathbb{Z}_{27}$ i, com en l'apartat anterior, hi ha moltes maneres de fer-ho. En proposem una: $8\cdot 17 = 136 = 27\cdot 5 + 1 = 1$.

Torna a l'exercici (p.38)

Solució de l'Exercici 25

Observem,

$$\begin{aligned}3^1 &= 3\\ 3^2 &= 9\\ 3^3 &= 3\cdot 3^2 = 3\cdot 9 = 27 = 18 + 9 = 9\\ 3^4 &= 3\cdot 3^3 = 3\cdot 9 = 27 = 18+9 = 9\\ &\vdots\end{aligned}$$

$$\begin{aligned}7^1 &= 7\\ 7^2 &= 49 = 18\cdot 2 + 13 = 13\\ 7^3 &= 7\cdot 7^2 = 7\cdot 13 = 91 = 18\cdot 5 + 1 = 1\\ &\vdots\end{aligned}$$

Per tant, no hi ha cap exponent $i > 0$ tal que $3^i = 1$.
Però sí que $7^i = 1$ per $i = 3$.
Per la definició, 7 té ordre però 3 no en té.

Podem comprovar-ho ara amb la condició del mcd. En efecte, $\text{mcd}(3, 18) = 3 \neq 1$, mentre que $\text{mcd}(7, 18) = 1$.

Torna a l'exercici (p.38)

Solució de l'Exercici 26

D'una banda, $(a^{-1})^{\mathrm{ord}_m(a)} = 1$ perquè $(a^{-1})^{\mathrm{ord}_m(a)} = (a^{-1})^{\mathrm{ord}_m(a)} a^{\mathrm{ord}_m(a)} = (a^{-1}a)^{\mathrm{ord}_m(a)} = 1^{\mathrm{ord}_m(a)} = 1$. D'altra banda, si $(a^{-1})^k = 1$, aleshores $a^k = a^k(a^{-1})^k = (aa^{-1})^k = 1$ i, per tant, $k \geq \mathrm{ord}_m(a)$.

Torna a l'exercici (p.38)

Solució de l'Exercici 27

Calculem els ordres de tots els elements de $\mathbb{Z}_7$.

$1^1 = 1$	$2^1 = 2$	$3^1 = 3$	$4^1 = 4$	$5^1 = 5$	$6^1 = 6$
	$2^2 = 4$	$3^2 = 2$	$4^2 = 2$	$5^2 = 4$	$6^2 = 1$
	$2^3 = 1$	$3^3 = 6$	$4^3 = 1$	$5^3 = 6$	
		$3^4 = 4$		$5^4 = 2$	
		$3^5 = 5$		$5^5 = 3$	
		$3^6 = 1$		$5^6 = 1$	
$\mathrm{ord}_7(1) = 1$	$\mathrm{ord}_7(2) = 3$	$\mathrm{ord}_7(3) = 6$	$\mathrm{ord}_7(4) = 3$	$\mathrm{ord}_7(5) = 6$	$\mathrm{ord}_7(6) = 2$

Ara podem observar que tots els ordres són divisors de $\phi(7) = 6$.

Torna a l'exercici (p.39)

Solució de l'Exercici 28

Perquè a sigui un element primitiu de $\mathbb{Z}_8$ ha de tenir ordre. Per tenir ordre ha de ser coprimer amb 8 i, per tant, ha de ser senar. Analitzem les potències de tots els senars:

$1^1 = 1$	$3^1 = 3$	$5^1 = 5$	$7^1 = 7$
	$3^2 = 9 = 1$	$5^2 = 25 = 1$	$7^2 = 49 = 1$
$\mathrm{ord}_8(1) = 1$	$\mathrm{ord}_8(3) = 2$	$\mathrm{ord}_8(5) = 2$	$\mathrm{ord}_8(7) = 2$

A més, per ser primitiu, el seu ordre ha de ser $\phi(8) = 8 - 4 = 4$.

Observem que no n'hi ha cap que tingui ordre 4. Per tant, $\mathbb{Z}_8$ no té elements primitius.

Torna a l'exercici (p.39)

Solució de l'Exercici 29(a)

1. Perquè a sigui un element primitiu de $\mathbb{Z}_{18}$ ha de tenir ordre. Per tenir ordre ha de ser coprimer amb 18 i, per tant, ha de ser senar i no múltiple de 3.

   D'altra banda, els ordres possibles a $\mathbb{Z}_{18}$ seran tots els divisors de $\phi(18) = \phi(9)\phi(2) = 9 - 3 = 6$, és a dir, $1, 2, 3$ o 6.

   Si trobem un element que no tingui ordre $1, 2$, ni 3, aleshores per força tindrà ordre 6 i per força serà primitiu.

   Provem amb $a = 5$. Observem les seves primeres potències:

   $$\begin{aligned} 5^1 &= 5 \\ 5^2 &= 25 = 7 \\ 5^3 &= -1 \end{aligned}$$

   Veiem que l'ordre de 5 no és 1, ni 2, ni 3, aleshores per força es tracta d'un element primitiu.

Solució de l'Exercici 29(b)

2. Ara podem afirmar que, com que existeix un element primitiu, el nombre d'elements primitius serà $\phi(\phi(18)) = \phi(6) = 2$.

   L'altre element primitiu serà 5^j per alguna j entre 2 i 5 amb $\mathrm{mcd}(j, \phi(18)) = 1$ i això només és possible per $j = 5$.

Així doncs, l'altre element primitiu serà $5^5 = 5^2 \cdot 5^3 = -7 = 11$.

Torna a l'exercici (p.39)

Solució de l'Exercici 30(a)

Fem la taula d'Euclides per a 29 i 16.

1	0	1	−1	5	
0	1	−1	2	−9	
		1	1	4	3
29	16	13	3	1	0

Deduïm que

$$5 \cdot 29 + (-9) \cdot 16 = 1$$

i, per tant, $(-9) \cdot 16 \equiv 20 \cdot 16 \equiv 1(29)$.

En conseqüència, l'invers de 16 a $\mathbb{Z}_{29}$ és 20.

Torna a l'exercici (p.40)

Solució de l'Exercici 30(b)

Fem la taula d'Euclides per a 2791 i 258.

1	0	1	−1	5	−11	
0	1	−10	11	−54	119	
		10	1	4	2	23
2791	2587	211	47	23	1	0

Deduïm que

$$(-11) \cdot 2791 + 119 \cdot 258 = 1$$

i, per tant, $119 \cdot 258 \equiv 1(2791)$.

En conseqüència, l'invers de 258 a $\mathbb{Z}_{2791}$ és 119.

Torna a l'exercici (p.40)

Solució de l'Exercici 31(a)

1.
$$\begin{array}{rclrcl}
2^0 & = & 1 & 1 & = & 2^0 \\
2^1 & = & 2 & 2 & = & 2^1 \\
2^2 & = & 4 & 3 & = & 2^{13} \\
2^3 & = & 8 & 4 & = & 2^2 \\
2^4 & = & 16 & 5 & = & 2^{16} \\
2^5 & = & 13 & 6 & = & 2^{14} \\
2^6 & = & 7 & 7 & = & 2^6 \\
2^7 & = & 14 & 8 & = & 2^3 \\
2^8 & = & 9 & 9 & = & 2^8 \\
2^9 & = & 18 & 10 & = & 2^{17} \\
2^{10} & = & 17 & 11 & = & 2^{12} \\
2^{11} & = & 15 & 12 & = & 2^{15} \\
2^{12} & = & 11 & 13 & = & 2^5 \\
2^{13} & = & 3 & 14 & = & 2^7 \\
2^{14} & = & 6 & 15 & = & 2^{11} \\
2^{15} & = & 12 & 16 & = & 2^4 \\
2^{16} & = & 5 & 17 & = & 2^{10} \\
2^{17} & = & 10 & 18 & = & 2^9
\end{array}$$

Solució de l'Exercici 31(b,c)

2. No és possible. En efecte, a $\mathbb{Z}_{23}$,

$$\begin{array}{rcl} 2^0 & = & 1 \\ 2^1 & = & 2 \\ 2^2 & = & 4 \\ 2^3 & = & 8 \\ 2^4 & = & 16 \\ 2^5 & = & 9 \\ 2^6 & = & 18 \\ 2^7 & = & 13 \\ 2^8 & = & 3 \\ 2^9 & = & 6 \\ 2^{10} & = & 12 \\ 2^{11} & = & 1 \\ 2^{12} & = & 2 \\ & \vdots & \end{array}$$

3. Per exemple, 7. Podeu comprovar-ho vosaltres mateixos.

Torna a l'exercici (p.40)

Solució de l'Exercici 32

1. No és un cos.
2. 6 invertibles, que són $1, 5, 7, 11, 13$ i 17.
3. 11.
4. Per exemple, el 5.
5. 2.

Torna a l'exercici (p.40)

Solució de l'Exercici 33

1. No és un cos.
2. $\phi(27) = 3^3 - 3^2 = 18$ invertibles, que són $\{1, 2, 4, 5, 7, 8, 10, 11, 13, 14, 16, 17, 19, 20, 22, 23, 25, 26\}$.
3. 8.
4. Per exemple, el 2.
5. 4, que té ordre 9.

Torna a l'exercici (p.41)

Solució de l'Exercici 34

Els dos resultats són equivalents. Demostrarem el primer, i el segon és anàleg.

Diguem $\gamma = \beta^{\frac{\phi(m)}{k}}$. Per demostrar que l'ordre de γ és k cal fer dues comprovacions:

- Cal veure que $\gamma^k = 1$,
- Cal veure que $\gamma^r \neq 1$ per tot exponent r amb $0 < r < k$.

Vegem el primer punt: $\gamma^k = (\beta^{\frac{\phi(m)}{k}})^k = \beta^{\phi(m)} = 1$.

Per al segon punt, suposem que r és un enter amb $0 < r < k$. Ara, $\gamma^r = (\beta^{\frac{\phi(m)}{k}})^r = \beta^{\frac{r\phi(m)}{k}}$. Com que $\frac{r\phi(m)}{k}$ és un enter (perquè k divideix $\phi(m)$) i és més petit que $\phi(m)$ (perquè $\frac{r}{k} < 1$), aleshores (com que β és primitiu) $\beta^{\frac{r\phi(m)}{k}} \neq 1$. Per tant, $\gamma^r \neq 1$.

Torna a l'exercici (p.41)

Solució de l'Exercici 35

- $4187 \equiv 2(3)$, per tant, $4187^{3515} \equiv 2^{3515}(3)$.
  Ara, com que $2^2 = 1$, deduïm que $2^{3515} \equiv 2(3)$.
- $4187 \equiv 2(5)$, per tant, $4187^{3515} \equiv 2^{3515}(5)$.
  Ara, com que $\mathrm{mcd}(2, 5) = 1$ i, per tant, $2^{\phi(5)} = 2^4 = 1$, deduïm que $2^{3515} \equiv 2^3(5)$.
  Per tant, $4187^{3515} \equiv 3(5)$.

Torna a l'exercici (p.41)

Solució de l'Exercici 36

Calculem primer $\phi(100) = \phi(25)\phi(4) = 20 \cdot 2 = 40$.

Utilitzarem el teorema d'Euler. És a dir, que si $\mathrm{mcd}(a, m) = 1$, aleshores $a^{\phi(m)} \equiv 1(m)$.

- Es pot resoldre de moltes maneres. Per exemple,
  $6^{41} = 2^{41}3^{41} = 2^{41}3 = (2^{10})^4 \cdot 2 \cdot 3 = (24)^4 \cdot 2 \cdot 3 = (76)^2 \cdot 2 \cdot 3 = (-24)^2 \cdot 2 \cdot 3 = 76 \cdot 2 \cdot 3 = 76 \cdot 6 = 456 = 56(100)$.
- $7^{41} = 7$.
- $15^{41} = 3 \cdot 5^{41}$.
  Aquí observem que $5^a \equiv 25(100)$ per tota $a > 1$. Deduïm que $15^{41} = 3 \cdot 25 = 75$.

Torna a l'exercici (p.41)

Solució de l'Exercici 37

Observem que ens estan demanant una quantitat mòdul 10 i una altra quantitat mòdul 100.

D'altra banda, observem primer que $\phi(10) = 4$, mentre que $\phi(100) = 40$, com hem vist abans.

- $7^{378}(10) \equiv 7^2(10) \equiv 9(10)$.
- $2793^{2792}(100) \equiv 93^{392}(100) \equiv 93^{32}(100) \equiv (-7)^{32}(100) \equiv 7^{32}(100)$.
  Arribats a aquest punt podem observar que $7^4 = 2401 \equiv 1(100)$.
  Deduïm que $7^{32} \equiv 1(100)$.
  Per tant, $2793^{2792} \equiv 1(100)$.

Torna a l'exercici (p.41)

2.5 Apèndix 1: Demostració del teorema d'Euler

Demostració. *Suposem que* $\mathbb{Z}_m^* = \{u_1, \ldots, u_{\phi(m)}\}$.
Anomenem $U = u_1 \cdot u_2 \cdot \cdots \cdot u_{\phi(m)}$.
Observem que $U \in \mathbb{Z}_m^*$ *i que el seu invers és*

$$U^{-1} = u_{\phi(m)}^{-1} \cdot u_{\phi(m)-1}^{-1} \cdot \cdots \cdot u_1^{-1}.$$

Ara considerem $a \in \mathbb{Z}_m^*$.
Observem que els elements $au_1, \ldots, au_{\phi(m)}$ *pertanyen tots a* $\mathbb{Z}_m^*$, *per tenir inversos, respectivament,* $u_1^{-1}a^{-1}, \ldots, u_{\phi(m)}^{-1}a^{-1}$.
D'altra banda tots ells són diferents, ja que si $au_i = au_j$, *aleshores multiplicant per* a^{-1} *a les dues bandes de la igualtat veiem que* u_i *hauria de ser igual a* u_j. *Per això,* $\mathbb{Z}_m^* = \{au_1, \ldots, au_{\phi(m)}\}$.
Així doncs, U també el podrem escriure com $au_1 \cdot au_2 \cdot \cdots \cdot au_{\phi(m)} = a^{\phi(m)}U$, *obtenint que* $U = a^{\phi(m)}U$.
Ara, multiplicant per U^{-1} *a les dues bandes de la igualtat obtenim que* $a^{\phi(m)} = 1$ *a* $\mathbb{Z}_m$. □

2.6 Apèndix 2: Repàs d'operacions i estructures algebraiques

Una **operació binària** en un conjunt A és una correspondència del producte cartesià $A \times A = \{(a, b) : a \in A \text{ i } b \in A\}$ en A.

Per exemple, la suma en els naturals la podem entendre com l'aplicació

$$\begin{array}{cccc} + : & (\mathbb{N}, \mathbb{N}) & \to & \mathbb{N} \\ & (a, b) & \mapsto & a + b \end{array}$$

Una operació binària $*$ en un conjunt A pot tenir les següents propietats:

- **Propietat associativa** si $a * (b * c) = (a * b) * c$ per tot $a, b, c \in A$.
- **Existència d'element neutre** si existeix un element de A, que anomenem e_n, tal que $a * e_n = e_n * a = a$ per tot $a \in A$.
- **Existència d'element invers** si per tot element $a \in A$ existeix un element de A, que anomenem e_a, tal que $a * e_a = e_a * e = e_n$.
- **Propietat commutativa** si $a * b = b * a$ per tot $a, b \in A$.

Torna a les propietats aritmètiques de $\mathbb{Z}_m$ (p.33)

Un **grup** és un conjunt A amb una operació associativa amb element neutre i invers. El grup és un **grup commutatiu** si l'operació és commutativa.

Exemples:

- Els enters $\mathbb{Z}$ amb la suma habitual són un grup (commutatiu).
- Els naturals $\mathbb{N}$ amb la suma no són un grup perquè no tots els elements tenen element invers.
- Els enters amb el producte habitual tampoc són grup perquè no sempre existeix l'element invers.

- Considerem el conjunt $\{a, e, i\}$ amb l'operació $*$ donada per la taula

$*$	a	e	i
a	e	i	a
e	i	a	e
i	a	e	i

Observem que l'operació és commutativa per ser la taula simètrica i que té com a element neutre l'element i. L'invers de a per $*$ és e i l'invers de e per $*$ és a. L'invers de i és ell mateix. També es pot comprovar que l'operació és associativa. Per tant el conjunt $\{a, e, i\}$ amb l'operació $*$ és un grup commutatiu.

- Considerem el conjunt $\{a, e, i, o\}$ amb l'operació $+$ donada per la taula

+	*a*	*e*	*i*	*o*
a	*o*	*i*	*e*	*a*
e	*i*	*o*	*a*	*e*
i	*e*	*a*	*o*	*i*
o	*a*	*e*	*i*	*o*

  Observem que l'operació és commutativa per ser la taula simètrica i que té com a element neutre l'element o. Tots els elements es tenen a ells mateixos com al seu propi invers. També es pot comprovar que l'operació és associativa. Per tant, el conjunt $\{a, e, i, o\}$ amb l'operació $+$ és un grup commutatiu.

Una segona operació $**$ en el conjunt A pot tenir la següent propietat respecte de la primera operació $*$.

- **Propietat distributiva** si $a * *(b * c) = (a * *b) * (a * *c)$ per tot $a, b, c \in A$.

Un **anell** és un conjunt A amb dues operacions $\oplus$ i $\otimes$ tal que $\oplus$ li confereix estructura de grup commutatiu i tal que $\otimes$ és associativa i satisfà la proietat distributiva respecte de $\oplus$. Podeu comprovar, com a exercici, que l'element neutre de $\oplus$ multiplicat per qualsevol element de l'anell dona altra vegada el neutre respecte de $\oplus$. Torna a l'anell $\mathbb{Z}_m$ (p.34).

L'anell és **unitari** i **commutatiu** si $\otimes$ té element neutre i satisfà la propietat commutativa, respectivament.

Un **cos** és un anell unitari i commutatiu on $\otimes$ satisfà que tot element diferent del neutre de $\oplus$ té invers. En aquest cas l'invers d'un element respecte de $\oplus$ s'anomena el seu **element oposat**, i es deixa el nom d'**element invers** per a l'invers respecte de $\otimes$. Torna al cos $\mathbb{Z}_p$ (p.36)

Exemples:

- Els enters $\mathbb{Z}$, amb la suma i el producte habituals, són un anell. Però no són un cos perquè no tots els elements tenen element invers.
- Els racionals $\mathbb{Q}$ i els reals $\mathbb{R}$ sí que són cossos.

- El conjunt $\{a, e, i, o\}$ dels exemples anteriors és un cos respecte de l'operació $\oplus = +$ descrita a la segona taula, amb neutre o, i respecte de l'operació $\otimes = *$ descrita a la primera ampliant-la amb el neutre de $+$, que multiplicat per qualsevol element dona o. És a dir

$*$	*a*	*e*	*i*	*o*
a	*e*	*i*	*a*	*o*
e	*i*	*a*	*e*	*o*
i	*a*	*e*	*i*	*o*
o	*o*	*o*	*o*	*o*

  Només queda comprovar que l'operació $*$ és distributiva respecte de $+$, que ho deixem com a exercici.

2.7 Notes històriques

Leonhard Euler (1707-1783) ha estat un dels matemàtics més importants i prolífics. L'estudi de les propietats de la funció d'Euler ha permès descobrir moltes propietats dels nombres enters. Torna a la funció d'Euler (p.36)

Teorema 2.2: Aquest teorema sovint és anomenat teorema "petit" de Fermat. Pierre de Fermat (1601-1665) va contribuir molt a l'aritmètica i és especialment famós per un teorema que va enunciar (sense demostració) que deia que $x^n + y^n = z^n$ no té solució entera per $n > 2$. Aquest teorema (el "gran") no va ser demostrat fins el 1995 per Andrew Wiles. Torna al teorema (p.37)

3 Aritmètica polinomial i cossos finits

3.1 Aritmètica polinomial

Polinomis a $\mathbb{Z}_m$

Anomenem **$\mathbb{Z}_m[x]$** al conjunt de polinomis amb coeficients a $\mathbb{Z}_m$

Exemple.

$$a(x) = 4x^7 + 3x^4 + x + 3 \in \mathbb{Z}_5[x],$$
$$b(x) = 2x^4 + 3 \in \mathbb{Z}_5[x].$$

Els elements de $\mathbb{Z}_m$ s'anomenen les **constants** o els **escalars** de $\mathbb{Z}_m[x]$.

El **grau**, els **coeficients**, el **termes**, etc., es defineixen de manera anàloga als polinomis de $\mathbb{R}[x]$.

Direm que un polinomi és **mònic** si el seu coeficient de grau màxim és 1.

Les sumes a $\mathbb{Z}_m[x]$ es fan coeficient a coeficient segons la suma a $\mathbb{Z}_m$.

Exemple.

$$\begin{aligned} a(x) + b(x) &= (4x^7 + 3x^4 + x + 3) + (2x^4 + 3) \\ &= 4x^7 + (3+2)x^4 + x + (3+3) \\ &= 4x^7 + x + 1. \end{aligned}$$

El producte de polinomis es fa utilitzant la propietat distributiva i el prodcte i la suma dels coeficients segons la suma i el producte a $\mathbb{Z}_m$.

Exemple.

$$\begin{aligned} a(x)\cdot b(x) &= (4x^7 + 3x^4 + x + 3)(2x^4 + 3) \\ &= 4x^7(2x^4+3) + 3x^4(2x^4+3) + x(2x^4+3) + 3(2x^4+3) \\ &= (3x^{11} + 2x^7) + (x^8 + 4x^4) + (2x^5 + 3x) + (x^4 + 4) \\ &= 3x^{11} + x^8 + 2x^7 + 2x^5 + 3x + 4. \end{aligned}$$

Exercici 38

- Doneu un exemple en que $\mathrm{grau}(a(x)b(x)) \neq \mathrm{grau}(a(x)) + \mathrm{grau}(b(x))$.
- Proveu que si m és primer, aleshores $\mathrm{grau}(a(x)b(x)) = \mathrm{grau}(a(x)) + \mathrm{grau}(b(x))$.

Llevat que no s'especifiqui el contrari, **a partir d'ara només considerarem polinomis de $\mathbb{Z}_p[x]$ amb p primer**.

En general emprarem p per denotar un primer.

Divisió de polinomis

Teorema 8: Divisió de polinomis

Donats dos polinomis qualssevol $a(x), b(x) \in \mathbb{Z}_p[x]$ existeixen dos altres polinomis únics $q(x), r(x) \in \mathbb{Z}_p[x]$ tals que

$$a(x) = b(x)q(x) + r(x)$$

amb $0 \leq \text{grau}(r(x)) < \text{grau}(b(x))$.

Dividend, divisor, quocient, residu

Els polinomis $a(x)$ i $b(x)$ són, respectivament, el **dividend** i el **divisor** de la divisió. El polinomi $q(x)$ és el **quocient**. El polinomi $r(x)$ és el **residu**.

Podem dividir de la manera habitual construint el polinomi quocient $q(x)$ dels termes de grau més gran als de grau més petit.

Exemple. *Vegem-ho amb els polinomis anteriors.*

El primer terme de $q(x)$ haurà de ser $2x^3$:

$$
\begin{array}{rrrrrrrrrr|lll}
 & 4x^7 & + & 3x^4 & & & + & x & + & 3 & 2x^4 & + & 3 \\ \cline{11-13}
- & (4x^7 & & & + & x^3) & & & & & 2x^3 & + & \\ \cline{2-6}
 & & & 3x^4 & + & 4x^3 & + & x & + & 3 & & &
\end{array}
$$

i continuem pel terme 4:

$$
\begin{array}{rrrrrrrrrr|lll}
 & 4x^7 & + & 3x^4 & & & + & x & + & 3 & 2x^4 & + & 3 \\ \cline{11-13}
- & (4x^7 & & & + & x^3) & & & & & 2x^3 & + & 4 \\ \cline{2-6}
 & & & 3x^4 & + & 4x^3 & + & x & + & 3 & & & \\
 & & - & (3x^4 & & & & & + & 2) & & & \\ \cline{4-10}
 & & & & & 4x^3 & + & x & + & 1 & & &
\end{array}
$$

En notació anglosaxona és

$$
\begin{array}{rrr|rrrrrrrrrr}
 & & & & 2x^3 & + & & & & & & & \\ \cline{4-13}
2x^4 & + & 3 & & 4x^7 & + & 3x^4 & & & + & x & + & 3 \\
 & & & - & (4x^7 & & & + & x^3) & & & & \\ \cline{4-13}
 & & & & & & 3x^4 & + & 4x^3 & + & x & + & 3
\end{array}
$$

i continuem pel terme 4:

$$
\begin{array}{rrr|rrrrrrrrrr}
 & & & & 2x^3 & + & 4 & & & & & & \\ \cline{4-13}
2x^4 & + & 3 & & 4x^7 & + & 3x^4 & & & + & x & + & 3 \\
 & & & - & (4x^7 & & & + & x^3) & & & & \\ \cline{5-13}
 & & & & & & 3x^4 & + & 4x^3 & + & x & + & 3 \\
 & & & & & - & (3x^4 & & & & & + & 2) \\ \cline{7-13}
 & & & & & & & & 4x^3 & + & x & + & 1
\end{array}
$$

Deduïm que

$$q(x) = 2x^3 + 4,$$
$$r(x) = 4x^3 + x + 1.$$

Observem que el grau de $r(x)$ és més petit que el de $b(x)$ i que $a(x) = b(x)q(x) + r(x)$.

Divisors

Si $r(x) = 0$, aleshores diem que $b(x)$ és un **divisor** de $a(x)$ i que $a(x)$ és un **múltiple** de $b(x)$.

Observem que si $b(x)$ és un divisor de $a(x)$, aleshores per a qualsevol element no nul $k \in \mathbb{Z}_p$, també tenim que $kb(x)$ és un divisor de $a(x)$. Diem que $kb(x)$ és un **múltiple escalar** de $b(x)$.

Algoritme d'Euclides i identitat de Bézout

El màxim comú divisor, l'algoritme d'Euclides i la identitat de Bézout per a polinomis es poden definir de forma anàloga a com ho hem fet per als enters.

Ara, quan diem el màxim dels divisors comuns, ens referim al de màxim grau.

Si p és primer, tot parell de polinomis no nuls de $\mathbb{Z}_p[x]$ tindrà un mcd mònic i aquest és únic. Si diem "*el* mcd" ens estarem referint a aquest.

Exemple. *Volem calcular a $\mathbb{Z}_5[x]$ el màxim comú divisor i els coeficients de la identitat de Bézout corresponent als polinomis $a = x^5 + x + 1$ i $b = x^3 + x^2$. Fem les divisions successives:*

$$\begin{array}{rrrrrl|l}
 x^5 & & & & +x+1 & & x^3+x^2 \\ \cline{7-7}
 -(x^5 & +\ x^4 & & & &) & x^2+4x+1 \\ \cline{1-6}
 & 4x^4 & & & +x+1 & & \\
 & -(4x^4 & +\ 4x^3 & & &) & \\ \cline{2-6}
 & & x^3 & & +x+1 & & \\
 & & -(x^3 & +\ x^2 & &) & \\ \cline{3-6}
 & & & 4x^2 & +x+1 & &
\end{array}$$

$$\begin{array}{rrrl|l}
 x^3 & +\ x^2 & & & 4x^2+x+1 \\ \cline{5-5}
 -(x^3 & +\ 4x^2+4x & &) & 4x+3 \\ \cline{1-4}
 & 2x^2+\ x & & & \\
 & -(2x^2+3x+3) & & & \\ \cline{2-4}
 & & 3x+2 & &
\end{array}$$

$$\begin{array}{rl|l}
 4x^2+x+1 & & 3x+2 \\ \cline{3-3}
 -(4x^2+x &) & 3x \\ \cline{1-2}
 1 & &
\end{array}$$

$$
\begin{array}{r|l}
3x + 2 & 1 \\ \cline{2-2}
-(3x \qquad) & 3x+2 \\ \cline{1-1}
2 & \\
-(2) & \\ \cline{1-1}
0 &
\end{array}
$$

I completem la taula:

λ	1	0	1	$x+2$	$2x^2+4x+1$	
μ	0	1	$4x^2+x+4$	$4x^3+4x^2+x+4$	$3x^4+3x^3+x^2+4x+4$	
quocients			x^2+4x+1	$4x+3$	$3x$	$3x+2$
residus	x^5+x+1	x^3+x^2	$4x^2+x+1$	$3x+2$	1	0

Deduïm que el màxim comú divisor és 1 *i que els coeficients de la identitat de Bézout són* $2x^2+4x+1$ *i* $3x^4+3x^3+x^2+4x+4$.

Per tant, la identitat de Bézout queda de la forma

$$(2x^2+4x+1)(x^5+x+1)+(3x^4+3x^3+x^2+4x+4)(x^3+x^2)=1.$$

Arrels de polinomis

Lema 13: Arrels

Donat un polinomi $f(x) \in \mathbb{Z}_p[x]$ i $a \in \mathbb{Z}_p$, són equivalents:

- $x-a$ divideix $f(x)$,
- $f(a)=0$.

En aquest cas, diem que a és una **arrel** de $f(x)$.

Demostració. *Si* $x-a$ *divideix* $f(x)$, *aleshores existeix* $q(x)$ *tal que* $f(x)=(x-a)q(x)$, *i en aquest cas és clar que* $f(a)=0$.
Suposem ara que $f(a)=0$. *Dividim* $f(x)$ *entre* $(x-a)$ *i obtindrem un quocient* $q(x)$ *i un residu* r *de grau més petit que* 1 *(i, per tant, constant) tal que* $f(x)=(x-a)q(x)+r$. *Si ara utilitzem que* $f(a)=0$, *i ho substituïm a la igualtat anterior obtenim* $f(a)=0+r=0$ *i, per tant,* $r=0$.
Això vol dir que $f(x)=(x-a)q(x)$. □

Exercici 39

És $x-3$ un divisor de $x^5+2x^3+3x^2+1$ a $\mathbb{Z}_7[x]$? I a $\mathbb{Z}_5[x]$? I a $\mathbb{Z}_3[x]$? I a $\mathbb{Z}_2[x]$?
Solució (p.67)

Exercici 40

Demostreu que un polinomi de $\mathbb{Z}_2[x]$,

- és divisible per x si i només si no té terme constant;
- és divisible per $x+1$ si i només si té un nombre parell de termes.

Solució (p.67)

Exercici 41: Mètode per trobar les arrels d'un polinomi de grau dos a $\mathbb{Z}_p$, en cas de p primer senar.

1. Per què podem afirmar que 2 és un element invertible de $\mathbb{Z}_p$?
2. En general, qui és l'element 2^{-1}, invers de 2 a $\mathbb{Z}_p$, en funció de p?
3. Considerem la taula dels quadrats de tots els elements de $\mathbb{Z}_p$. Per exemple, la taula dels quadrats de $\mathbb{Z}_5$ seria:

a	a^2
0	0
1	1
2	4
3	4
4	1

Doneu la taula dels quadrats de $\mathbb{Z}_7$.

4. Si $a \in \mathbb{Z}_p$, aleshores definim el **conjunt d'arrels quadrades** $\sqrt{a}^{\mathbb{Z}_p}$ com el conjunt de tots els elements $b \in \mathbb{Z}_p$ tals que $b^2 = a$. Així, per exemple, els conjunts d'arrels quadrades de tots els elements de $\mathbb{Z}_5$ són els següents:

$$\begin{array}{rcl} \sqrt{0}^{\mathbb{Z}_5} & = & \{0\} \\ \sqrt{1}^{\mathbb{Z}_5} & = & \{1,4\} \\ \sqrt{2}^{\mathbb{Z}_5} & = & \emptyset = \{\} \\ \sqrt{3}^{\mathbb{Z}_5} & = & \emptyset = \{\} \\ \sqrt{4}^{\mathbb{Z}_5} & = & \{2,3\} \end{array}$$

Doneu els conjunts d'arrels quadrades de tots els elements de $\mathbb{Z}_7$.

5. Si $b, c \in \mathbb{Z}_p$ són tals que $\sqrt{b^2-4c}^{\mathbb{Z}_p}$ té un o més valors diferents, aleshores les arrels de x^2+bx+c són

$$(-b+\sqrt{b^2-4c}^{\mathbb{Z}_p})\frac{p+1}{2} \mod p$$

o, dit d'altra manera, són els valors $(-b+y)\frac{p+1}{2} \mod p$ on y agafa tots els valors de $\sqrt{b^2-4c}^{\mathbb{Z}_p}$.

Per exemple, les arrels de $x^2+3x+2 \in \mathbb{Z}_5[x]$ són

$$\begin{aligned} (-b+\sqrt{b^2-4c}^{\mathbb{Z}_p})\frac{p+1}{2} \mod 5 &= (-3+\sqrt{4-3}^{\mathbb{Z}_p})\frac{5+1}{2} \mod 5 \\ &= (2+\sqrt{1}^{\mathbb{Z}_p})3 \mod 5 \\ &= 1+3\{1,4\} \mod 5 \\ &= \begin{cases} 1+3\cdot 1 \mod 5 = 4 \\ 1+3\cdot 4 \mod 5 = 3 \end{cases} \end{aligned}$$

Comproveu que 4 i 3 són, en efecte, arrels de $x^2+3x+2 \in \mathbb{Z}_5[x]$.

6. A $\mathbb{Z}_7[x]$ trobeu les arrels dels següents polinomis:
   - x^2+5x+1,
   - x^2+6,
   - x^2+5x+4.
7. Comproveu les arrels obtingudes en l'apartat anterior.

Solució (p.68)

Lema 14

El nombre d'arrels d'un polinomi $f(x) \in \mathbb{Z}_p[x]$ és com a molt el seu grau.

Polinomis irreductibles

Polinomis irreductibles

Un polinomi és **irreductible** si els seus únics divisors són 1 i ell mateix i tots els seus múltiples escalars possibles.

Observem que tots els escalars no nuls i tots els polinomis de grau 1 són irreductibles.

Si un polinomi de grau més gran que 1 és irreductible, aleshores no té arrels.

Perquè, si tingués una arrel a, aleshores tindria un factor de la forma $x - a$.

Exemple. *El polinomi $f(x) = x^2 + x + 1$ és irreductible a $\mathbb{Z}_2[x]$ i no té arrels. En efecte, $f(0) = 1 \neq 0$ i $f(1) = 3 = 1 \neq 0$.*

El recíproc no és cert.

Exemple. *A $\mathbb{Z}_2[x]$, el polinomi $g(x) = x^4 + x^2 + 1$ no té arrels perquè $g(0) = 1 \neq 0$ i $g(1) = 3 = 1 \neq 0$. Però, en canvi, $(x^2+x+1)(x^2+x+1) = x^4+x^3+x^2+x^3+x^2+x+x^2+x+1 = x^4+2x^3+3x^2+2x+1 = x^4+x^2+1 = g(x)$, és a dir, $g(x)$ no és irreductible.*

Exemple. *Considerem el polinomi*

$$f(x) = x^4 + x^3 + 2x^2 + 2x + 1 \in \mathbb{Z}_3[x].$$

Comproveu que no té arrels.

I, tanmateix, $f(x)$ no és irreductible perquè

$$f(x) = (x^2 + 2x + 2)^2.$$

Exercici 42

Demostreu que, si un polinomi té grau 2 o 3, aleshores el polinomi és irreductible si i només si no té arrels.

Solució (p.68)

Exercici 43

Trobeu tots els polinomis irreductibles de grau més petit o igual que 4 de $\mathbb{Z}_2[x]$.

Solució (p.69)

Exercici 44

Considerem els polinomis de $\mathbb{Z}_2[x]$

$$\begin{aligned} f &= x^5 + x^2 + 1, \\ g &= x^2 + x + 1. \end{aligned}$$

1. Quins són el quocient i el residu de dividir f entre g?
2. Demostreu que f i g són irreductibles a $\mathbb{Z}_2[x]$.

Solució (p.69)

Exercici 45

1. Quants polinomis mònics hi ha a $\mathbb{Z}_3[x]$ de grau 2?
2. Quins són els polinomis irreductibles mònics de $\mathbb{Z}_3[x]$ de grau 2?

Solució (p.70)

Exercici 46

1. Considerem el conjunt P de polinomis amb coeficients a $\mathbb{Z}_3$ que tenen exactament un monomi de grau senar i coeficient 1 i la resta de monomis de grau parell. Poseu-ne un exemple.
2. Demostreu que un polinomi $p \in P$ que sigui irreductible ha de complir:
   (a) La suma dels seus coeficients no és múltiple de 3.
   (b) La suma dels seus coeficients no és congruent amb 2 mòdul 3.
3. Doneu una altra condició que ha de complir un polinomi de P que sigui irreductible.

Solució (p.70)

Factorització de polinomis

Factorització

Tot polinomi es pot descompondre en producte de polinomis irreductibles.

Aquí la descomposició és única llevat del producte per escalars.

Exemple. *Per exemple, a* $\mathbb{Z}_5[x]$

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

Però també

$$2x^2 + 3 = (2x+2)(x+4).$$

I també podem separar amb una constant i un producte de polinomis irreductibles mònics:

$$2x^2 + 3 = 2(x+1)(x+4).$$

Factorització

Si p és primer, tot polinomi de $\mathbb{Z}_p[x]$ es pot descompondre de manera única en el producte d'una constant per un producte de polinomis irreductibles mònics.

Aquí és important que p sigui primer. Per exemple, a $\mathbb{Z}_4[x]$, el polinomi $2x+3$ no es pot escriure com una constant per un polinomi mònic perquè 2 no té invers a $\mathbb{Z}_4$.

De la mateixa manera, a $\mathbb{Z}_8$, el polinomi x^2+7 admet dues descomposicions diferents: $x^2+7 = (x+1)(x+7) = (x+3)(x+5)$.

La demostració de la unicitat de la factorització en irreductibles és equivalent a la vista pel cas dels enters. En el cas dels enters, a partir de la Identitat de Bézout hem deduït que, si p és primer i $p \mid ab$, aleshores $p \mid a$ o $p \mid b$. D'aquí se segueix la demostració de la factorització en primers.

En el cas de polinomis podem demostrar, també a partir de la identitat de Bézout, que si $c(x)$ és irreductible i $c(x) \mid a(x)b(x)$, aleshores $c(x) \mid a(x)$ o $c(x) \mid b(x)$. I ara aquest resultat el podem utilitzar per demostrar la unicitat de la factorització en irreductibles.

Exercici 47

Factoritzeu completament el polinomi $2x^4+4x^2+3x+1$ a $\mathbb{Z}_5[x]$.
Solució (p.70)

3.2 Congruències de polinomis i anells quocient $\mathbb{Z}_p/f(x)$

Congruències de polinomis

Definició

Si $r(x)$ és el residu de dividir $a(x)$ per $m(x)$, aleshores diem que $r(x)$ és la **reducció de $a(x)$ mòdul $m(x)$**. Escriurem

$$a(x) = r(x) \mod m(x).$$

Exemple. *Considerem els polinomis del principi de la secció,* $a(x) = 4x^7+3x^4+x+3$ *i* $b(x) = 2x^4+3 \in \mathbb{Z}_5$.

En fer la divisió euclidiana *de* $a(x)$ *entre* $b(x)$ *hem vist que el seu quocient i residu són, respectivament,* $q(x) = 2x^3+4$ *i* $r(x) = 4x^3+x+1$.

En aquest cas, diem que la reducció de $4x^7+3x^4+x+3$ *mòdul* $2x^4+3$ *és* $4x^3+x+1$ *o que*

$$4x^7+3x^4+x+3 = 4x^3+x+1 \mod 2x^4+3$$

Congruències

Donats tres polinomis $a(x), b(x), f(x) \in \mathbb{Z}_p[x]$, diem que $a(x)$ i $b(x)$ són **congruents** mòdul $f(x)$ si, equivalentment,

- els residus de dividir $a(x)$ i $b(x)$ entre $f(x)$ coincideixen,
- la diferència $b(x)-a(x)$ és un múltiple de $f(x)$.

Escrivim

$$a(x) \equiv b(x) \mod f(x)$$

Exercici 48

Comproveu que, efectivament, les dues condicions de la definició són equivalents. Vegeu el resultat anàleg de les congruències d'enters.

Anells quocient $\mathbb{Z}_p/f(x)$

Com en el cas dels enters, la relació de congruència és una relació d'equivalència i per això les classes de congruència queden ben definides.

$\mathbb{Z}_p/f(x)$

Anomenem $\mathbb{Z}_p/f(x)$ al conjunt de classes de congruència mòdul $f(x)$.

Si $\text{grau}(r(x)) < \text{grau}(f(x))$, $[r(x)]_f$ representa la classe de tots els polinomis que dividits entre $f(x)$ tenen residu $r(x)$.

Per extensió, escriurem $[a(x)]_f = [r(x)]_f$ si $a(x) = q(x)f(x) + r(x)$ amb $\text{grau}(r(x)) < \text{grau}(f(x))$.

En particular, tindrem que $[a(x)]_f = [a(x) + k(x)f(x)]_f$ per a qualsevol polinomi $k(x) \in \mathbb{Z}_p[x]$.

Exemple. *Considerem l'anell $\mathbb{Z}_3[x]$ i el polinomi*

$$f(x) = x^2 + 2x + 2 \in \mathbb{Z}_3[x].$$

Si dividim un polinomi de $\mathbb{Z}_3[x]$ entre $f(x)$, quin pot ser el residu?

Haurà de ser un polinomi de grau més petit que 2 i amb coeficients dins de $\mathbb{Z}_3$.

Només hi ha un nombre finit de possibilitats:

$$\begin{array}{ccc} 0 & 1 & 2 \\ x & x+1 & x+2 \\ 2x & 2x+1 & 2x+2 \end{array}$$

Això ens està dient que només hi ha 9 classes de congruència mòdul $f(x)$ i que $\mathbb{Z}_3[x]/f(x)$ té 9 elements:

$$\mathbb{Z}_3[x]/f(x) = \{[0]_f, [1]_f, [2]_f, [x]_f, [x+1]_f, [x+2]_f, [2x]_f, [2x+1]_f, [2x+2]_f\}$$

Exercici 49

Seguint el mateix procediment, llisteu totes les classes de congruència de $\mathbb{Z}_2[x]/x^3 + x + 1$.
Solució (p.71)

Deduïm el següent:

L'anell $\mathbb{Z}_p[x]/f(x)$ està format per $p^{\text{grau}(f)}$ classes d'equivalència.

Exercici 50

1. Quants elements tindrà $\mathbb{Z}_2[x]/x^3 + x + 1$?
2. Quants elements tindrà $\mathbb{Z}_3[x]/x^3 + x + 1$?

Solució (p.71)

Aritmètica dels anells quocient $\mathbb{Z}_p/f(x)$

Dins de $\mathbb{Z}_p[x]/f(x)$ tenim dues operacions ben definides

$$[r_1(x)]_f + [r_2(x)]_f = [r_1(x) + r_2(x)]_f,$$

$$[r_1(x)]_f \cdot [r_2(x)]_f = [r_1(x) \cdot r_2(x)]_f.$$

Aquestes operacions doten $\mathbb{Z}_p/f(x)$ de l'estructura d'anell.

Exemple. *Hem vist que per $f(x) = x^2 + 2x + 2$,*

$$\mathbb{Z}_3[x]/f(x) = \{[0]_f, [1]_f, [2]_f, [x]_f, [x+1]_f, [x+2]_f, [2x]_f, [2x+1]_f, [2x+2]_f\}$$

Podem operar amb les classes d'equivalència fent reduccions mòdul 3 i reduccions mòdul f. Per exemple,

$$\begin{aligned} [2x+1]_f + [x+1]_f &= [3x+2]_f \\ &= [2]_f \end{aligned}$$

o bé

$$\begin{aligned} [2x+1]_f \cdot [x+1]_f &= [2x^2+3x+1]_f \\ &= [2x^2+1]_f \\ &= [2x^2+1+f(x)]_f \\ &= [2x^2+1+(x^2+2x+2)]_f \\ &= [3x^2+2x+3]_f \\ &= [2x]_f \end{aligned}$$

3.3 Cossos finits

Elements invertibles

Exemple. *Tornem a l'exemple anterior*

$$\mathbb{Z}_3[x]/x^2 + 2x + 2 = \{[0]_f, [1]_f, [2]_f, [x]_f, [x+1]_f, [x+2]_f, [2x]_f, [2x+1]_f, [2x+2]_f\}.$$

Volem saber si la classe $[x+1]_f$ té invers a $\mathbb{Z}_3[x]/f(x)$, és a dir, si hi ha alguna classe que multiplicada per $[x+1]_f$ doni $[1]_f$.

Opció 1: *Podem provar-ho per cerca exhaustiva.*

$$\begin{array}{rcllllr} [1]_f \cdot [x+1]_f &=& [x+1]_f & & & & \neq [1]_f \\ [2]_f \cdot [x+1]_f &=& [2x+2]_f & & & & \neq [1]_f \\ [x]_f \cdot [x+1]_f &=& [x^2+x]_f & = [x^2+x+2f]_f & = [x^2+x+2(x^2+2x+2)]_f & = [2x+1] & \neq [1]_f \\ [x+1]_f \cdot [x+1]_f &=& [x^2+2x+1]_f & = [x^2+2x+1+2f]_f & = [x^2+2x+1+2(x^2+2x+2)]_f & = [2]_f & \neq [1]_f \\ [x+2]_f \cdot [x+1]_f &=& [x^2+2]_f & = [x^2+2+2f]_f & = [x^2+2+2(x^2+2x+2)]_f & = [x]_f & \neq [1]_f \\ [2x]_f \cdot [x+1]_f &=& [2x^2+2x]_f & = [2x^2+2x+f]_f & = [2x^2+2x+(x^2+2x+2)]_f & = [x+2] & \neq [1]_f \\ [2x+1]_f \cdot [x+1]_f &=& [2x^2+1]_f & = [2x^2+1+f]_f & = [2x^2+1+(x^2+2x+2)]_f & = [2x]_f & \neq [1]_f \\ [2x+2]_f \cdot [x+1]_f &=& [2x^2+x+2]_f & = [2x^2+x+2+f]_f & = [2x^2+x+2+(x^2+2x+2)]_f & & = [1]_f \end{array}$$

Trobem, doncs, que $([x+1]_f)^{-1} = [2x+2]_f$.

Opció 2:

Podem utilitzar la identitat de Bézout de $x+1$ i x^2+2x+2.

En aquest cas, la taula de l'algoritme d'Euclides és

1	0	1	
0	1	$2x+2$	
		$x+1$	
x^2+2x+2	$x+1$	1	0

Per tant, la identitat de Bézout és

$$1\cdot(x^2+2x+2)+(2x+2)\cdot(x+1)=1.$$

Si reduïm mòdul $f(x)$ a les dues bandes de la identitat obtenim que

$$[2x+2]_f\cdot[x+1]_f=[1]_f,$$

deduint de nou que $([x+1]_f)^{-1}=[2x+2]_f$.

Identitat de Bézout i l'invers d'un element

En general, si $\mathrm{mcd}(f(x),a(x))=1$, aleshores, per la identitat de Bézout, existiran polinomis $\lambda(x)$ i $\mu(x)$ tals que

$$\lambda(x)f(x)+\mu(x)a(x)=1$$

Això significa que $\mu(x)a(x)=1-\lambda(x)f(x)$ i, per tant,

$$\mu(x)a(x)\equiv 1 \mod f(x).$$

Deduïm, doncs, que $[a(x)]_f^{-1}=[\mu(x)]_f$.

Exercici 51

1. Calculeu a $\mathbb{Z}_3[x]$ el màxim comú divisor del polinomi $a=x^2+2x+2$ i el polinomi $b=2x+1$ i expresseu-lo com a combinació lineal de a i b.
2. Podem deduir si $2x+1$ és invertible a $\mathbb{Z}_3[x]/x^2+2x+2$? En cas afirmatiu calculeu-ne l'invers.
3. Podem deduir si $x+2$ és invertible a $\mathbb{Z}_3[x]/x^2+2x+2$? En cas afirmatiu calculeu-ne invers.
4. Comproveu que tots els inversos que heu trobat són, en efecte, inversos.

Solució (p.71)

Construcció de cossos finits

Ara ens volem centrar a veure quins dels anells de la forma $\mathbb{Z}_p[x]/f(x)$ són cossos.

Exercici 52

1. Calculeu les taules de la suma i del producte a $\mathbb{Z}_2[x]/x^2+x+1$.
2. Calculeu les taules de la suma i del producte a $\mathbb{Z}_2[x]/x^2+1$.
3. Calculeu la taula del producte a $\mathbb{Z}_3[x]/x^2+1$.
4. Raoneu si $\mathbb{Z}_2[x]/x^2+x+1$, $\mathbb{Z}_2[x]/x^2+1$, o $\mathbb{Z}_3[x]/x^2+1$ són cossos.

Solució (p.71)

Observem que si $f(x)$ és irreductible, aleshores és coprimer amb qualsevol polinomi que no sigui un múltiple seu i, per tant, qualsevol classe diferent de zero (la classe del zero correspon als múltiples de $f(x)$) és invertible. Per això podem afirmar el següent:

Si m és un primer i si $f(x)$ és irreductible a $\mathbb{Z}_m[x]$, aleshores $\mathbb{Z}_m[x]/f(x)$ és un cos.

Per contra, si m no és primer, els divisors de m no seran invertibles a $\mathbb{Z}_m[x]$ i, si m és primer, però $f(x)$ no és irreductible, els seus divisors no seran invertibles a $\mathbb{Z}_m[x]/f(x)$.

Teorema 9

$\mathbb{Z}_m[x]/f(x)$ és un cos si i només si m és primer i $f(x)$ és irreductible a $\mathbb{Z}_m[x]$.

Si $\mathbb{Z}_p[x]/f(x)$ és cos l'anomenem $\mathbb{F}_{p^n}$, on $n = \text{grau}(f(x))$.

Exercici 53

Utilitzeu l'Exercici 46 per donar un polinomi que generi $\mathbb{F}_{27}$. Solució (p.72)

Ordre i elements primitius

Teorema 10

Per a qualsevol $\beta \in \mathbb{F}_{p^n}^*$, es té $\beta^{p^n-1} = 1$.

Exercici 54

Demostreu el teorema anterior. Podeu emprar els mateixos arguments que en la demostració del teorema d'Euler.

Ordre

L'**ordre** de $\beta \in \mathbb{F}_{p^n} \setminus \{0\}$ és el mínim exponent $i \neq 0$ tal que $\beta^i = 1$. El denotem per $\mathbf{ord}_{\mathbb{F}_{p^n}}(a)$

Pel teorema anterior, si $\mathbb{F}_{p^n}$ és un cos finit, tot element no nul de $\mathbb{F}_{p^n}$ tindrà un ordre.

Exercici 55

Demostreu que si $\beta^k = 1$ per un enter positiu k, aleshores l'ordre de β divideix k. Vegeu el resultat anàleg per l'ordre dels elements de $\mathbb{Z}_m$.

Com a conseqüència del resultat de l'exercici i del teorema 10 tenim el resultat següent.

L'ordre d'un element no nul de $\mathbb{F}_{p^n}$ sempre divideix $p^n - 1$.

Exercici 56

Demostreu que, a $\mathbb{Z}_p[x]/f(x)$, si la classe $[x]_f$ és diferent de zero, aleshores té ordre més gran o igual que el grau de $f(x)$. Solució (p.72)

Elements primitius

Diem que $\beta \in \mathbb{F}_{p^n}$ és un **element primitiu** si el seu ordre és $p^n - 1$.

Si β és primitiu, aleshores

$$\mathbb{F}_{p^n} = \{0, 1, \beta, \ldots, \beta^{p^n-2}\}.$$

Polinomis primitius

Diem que $f(x)$ és **primitiu** si la classe $[x]_f$ és un element primitiu de $\mathbb{Z}_p[x]/f(x)$.

Exemple. *Considerem, per exemple, el cos $\mathbb{F}_{16} = \mathbb{Z}_2[x]/x^4 + x^3 + 1$. Anomenem α a la classe $[x]_f$ on $f(x) = x^4 + x^3 + 1$. En particular, tindrem $f(\alpha) = 0$. Per tant, $\alpha^4 = -\alpha^3 - 1 = \alpha^3 + 1$. La resta de potències de α seran:*

$$\begin{array}{rcl}
\alpha^0 & = & 1 \\
\alpha^1 & = & \alpha \\
\alpha^2 & = & \alpha^2 \\
\alpha^3 & = & \alpha^3 \\
\alpha^4 & = & \alpha^3 + 1 \\
\alpha^5 & = & \alpha\alpha^4 = \alpha(\alpha^3 + 1) = \alpha^4 + \alpha = \alpha^3 + \alpha + 1 \\
\alpha^6 & = & \alpha\alpha^5 = \alpha(\alpha^3 + \alpha + 1) = \alpha^4 + \alpha^2 + \alpha = \alpha^3 + \alpha^2 + \alpha + 1 \\
\alpha^7 & = & \alpha\alpha^6 = \alpha(\alpha^3 + \alpha^2 + \alpha + 1) = \alpha^4 + \alpha^3 + \alpha^2 + \alpha = \alpha^3 + 1 + \alpha^3 + \alpha^2 + \alpha \\
 & = & 2\alpha^3 + \alpha^2 + \alpha + 1 = \alpha^2 + \alpha + 1 \\
\alpha^8 & = & \alpha^3 + \alpha^2 + \alpha \\
\alpha^9 & = & \alpha^2 + 1 \\
\alpha^{10} & = & \alpha^3 + \alpha \\
\alpha^{11} & = & \alpha^3 + \alpha^2 + 1 \\
\alpha^{12} & = & \alpha + 1 \\
\alpha^{13} & = & \alpha^2 + \alpha \\
\alpha^{14} & = & \alpha^3 + \alpha^2 \\
\alpha^{15} & = & 1
\end{array}$$

Això ens permet veure que α és primitiu i $f(x)$ també.

Representació d'elements

Suposem que tenim un cos finit $\mathbb{Z}_p/(f(x))$ i que $d = \text{grau}(f(x))$.

Anomenem α a la classe de congruència mòdul $f(x)$ de l'element x.
En particular tindrem que $f(\alpha) = 0$.
Qualsevol element de $\mathbb{Z}_p/(f(x))$ es podrà expressar com un polinomi en α de grau més petit que d.
És el que anomenem **notació polinomial**.

D'altra banda, suposem que β és un element primitiu. Qualsevol element no nul es podrà expressar també com una potència de β amb un exponent més petit que $p^d - 1$.
És el que anomenem **notació exponencial** o **notació potencial**.

Finalment, podem representar els elements de $\mathbb{Z}_p/(f(x))$ per un vector de d coordenades $(a_0, \ldots, a_{d-1})$ on a_i és el coeficient de grau i de la notació polinomial.
És el que anomenem **notació vectorial**.

Exemple. *En l'exemple anterior,*
α^{11} *(notació exponencial)* $= 1 + \alpha^2 + \alpha^3$ *(notació polinomial)* $= (1, 0, 1, 1)$ *(notació vectorial).*

La notació polinomial i la notació vectorial ens aniran molt bé per fer sumes i restes, mentre que la notació exponencial ens anirà molt bé per poder fer multiplicacions i divisions. Per això ens serà convenient poder fer servir totes les notacions a la vegada i per això emprarem les **taules d'equivalència** entre les diferents notacions.

Continuant l'exemple anterior,

pot.	pol.	vect.
α^0	1	(1000)
α^1	α	(0100)
α^2	α^2	(0010)
α^3	α^3	(0001)
α^4	$\alpha^3 + 1$	(1001)
α^5	$\alpha^3 + \alpha + 1$	(1101)
α^6	$\alpha^3 + \alpha^2 + \alpha + 1$	(1111)
α^7	$\alpha^2 + \alpha + 1$	(1110)
α^8	$\alpha^3 + \alpha^2 + \alpha$	(0111)
α^9	$\alpha^2 + 1$	(1010)
α^{10}	$\alpha^3 + \alpha$	(0101)
α^{11}	$\alpha^3 + \alpha^2 + 1$	(1011)
α^{12}	$\alpha + 1$	(1100)
α^{13}	$\alpha^2 + \alpha$	(0110)
α^{14}	$\alpha^3 + \alpha^2$	(0011)

Resum

$\boldsymbol{\mathbb{Z}_m}$	$\boldsymbol{\mathbb{Z}_p[x]/f(x)}$ (amb p primer)
Divisió euclidiana a $\mathbb{Z}$: Donats $a, b \in \mathbb{Z}$ existeixen $q, r \in \mathbb{Z}$ tals que $a = bq + r$ amb $0 \leq r < b$.	Divisió euclidiana a $\mathbb{Z}_p[x]$: Donats $a(x), b(x) \in \mathbb{Z}_p[x]$ existeixen $q(x), r(x) \in \mathbb{Z}_p[x]$ tals que $a(x) = b(x)q(x) + r(x)$ amb $0 \leq \text{grau}(r(x)) < \text{grau}(b(x))$.
Fer congruències mòdul m és quedar-nos amb el residu de dividir per m $\Rightarrow$ obtenim enters $< m$.	Fer congruències mòdul $f(x)$ és quedar-nos amb el residu de dividir per $f(x)$ $\Rightarrow$ obtenim polinomis de grau $< \text{grau}(f(x))$.
$\mathbb{Z}_m = \{0, 1, \ldots, m-1\}$ amb les operacions reduïdes mòdul m.	$\mathbb{Z}_p[x]/f(x) = \{a_0 + a_1x + \cdots + a_{n-1}x^{n-1}$ amb $a_0, \ldots, a_{n-1} \in \mathbb{Z}_p\}$ amb les operacions reduïdes mòdul p i mòdul $f(x)$, on $n = \text{grau } f(x)$.
$\mathbb{Z}_m$ té m elements.	$\mathbb{Z}_p[x]/f(x)$ té p^n elements.
	Diem que la classe de x és un generador de $\mathbb{Z}_p[x]/f(x)$.
$a \in \mathbb{Z}_m$ és invertible si i només si $\text{mcd}(a, m) = 1$. L'invers es troba per la identitat de Bézout: $\lambda a + \mu m = 1 \Rightarrow \lambda a = 1 \Rightarrow a^{-1} = \lambda$. Anomenem $\mathbb{Z}_m^*$ als invertibles de $\mathbb{Z}_m$.	$a(x) \in \mathbb{Z}_p[x]/f(x)$ és invertible si i només si $\text{mcd}(a(x), f(x))$ és constant. L'invers es troba per la identitat de Bézout: $\lambda(x)a(x) + \mu(x)f(x) = 1 \Rightarrow \lambda(x)a(x) = 1 \Rightarrow (a(x))^{-1} = \lambda(x)$. Anomenem $(\mathbb{Z}_p[x]/f(x))^*$ als invertibles de $\mathbb{Z}_p[x]/f(x)$.
Funció d'Euler: $\phi(m) = \#\{a : 1 \leq a < m, \text{mcd}(a, m) = 1\}$ • $\phi(p) = p - 1$ si p és primer, • $\phi(p^k) = p^k - p^{k-1}$ si p és primer, • $\phi(ab) = \phi(a)\phi(b)$ si $\text{mcd}(a, b) = 1$. Teorema d'Euler: $a^{\phi(m)} \equiv 1 \mod m$ si $\text{mcd}(a, m) = 1$.	
$\mathbb{Z}_m$ és cos si i només si m és primer. Si p és primer $\mathbb{Z}_p$ també l'anomenem $\mathbb{F}_p$.	$\mathbb{Z}_p[x]/f(x)$ és cos si i només si $f(x)$ és irreductible. Si $\mathbb{Z}_p[x]/f(x)$ és cos l'anomenem $\mathbb{F}_{p^n}$.
L'ordre de $a \in \mathbb{Z}_m$ és el mínim exponent $i \neq 0$ tal que $a^i \equiv 1 \mod m$.	L'ordre de $\beta \in \mathbb{F}_{p^n}$ és el mínim exponent $i \neq 0$ tal que $\beta^i = 1$.
L'ordre sempre és un divisor de $\phi(m)$.	L'ordre sempre és un divisor de $p^n - 1$.
Diem que $a \in \mathbb{Z}_m$ és primitiu si el seu ordre és $\phi(m)$.	Diem que $\beta \in \mathbb{F}_{q^n}$ és primitiu si el seu ordre és $p^n - 1$.
	Si β és primitiu, aleshores $\mathbb{F}_{p^n} = \{0, 1, \beta, \ldots, \beta^{p^n-2}\}$. Diem que $f(x)$ és primitiu si la classe de x és un element primitiu de $\mathbb{Z}_p[x]/f(x)$.

3.4 Exercicis

Exercici 57

1. Per quins polinomis $f(x)$ de $\mathbb{Z}_2[x]$ el quocient $\mathbb{Z}_2[x]/f(x)$ és un cos de 4 elements?
2. Doneu-ne un element primitiu i la taula d'equivalències potencial-vectorial-polinomial.
3. Doneu també una taula per a la suma i una taula per al producte.

Solució (p.72)

Exercici 58

Considerem $\mathbb{Z}_3[x]/x^2+x+2$

1. Demostreu que és un cos.
2. Quants elements té?
3. És $\alpha = [x]$ un element primitiu? Per què?
4. Doneu-ne una taula d'equivalències amb les notacions potencial, polinomial i vectorial.
5. Calculeu $\alpha^2\left(\frac{\alpha^{20}-\alpha^5+\alpha}{\alpha^3-\alpha}\right)$.

Solució (p.73)

Exercici 59

Considerem els següents polinomis de $\mathbb{Z}_3[x]$.

- $f(x) = x^3+x^2+2$,
- $g(x) = x^3+2x+1$,
- $h(x) = x^3+2x^2+2$.

Sabem que

- $x^{11} \mod f(x) = x+1$,
- $x^{11} \mod g(x) = x^2+x+2$,
- $x^{11} \mod h(x) = 2x^2+x+1$.

1. Quins d'aquests polinomis són irreductibles?
2. Quins dels polinomis irreductibles són primitius?
3. Per quins polinomis, en fer quocient a $\mathbb{Z}_3[x]$, s'obté un cos? De quants elements?
4. Per quins dels polinomis anteriors que, en fer quocient, ens donen un cos, podem expressar qualsevol element del cos com a potència de la classe de x en el quocient?

Solució (p.74)

Exercici 60

Considerem $\mathbb{Z}_3[x]/x^2+1$

(a) Demostreu que és un cos.

(b) Quants elements té?

(c) Anomenem α l'element del cos que correspon a la classe de x mòdul x^2+1. Quin és l'ordre de α?

(d) És $\alpha = [x]$ un element primitiu? Per què?

(e) Trobeu un element primitiu β.

(f) Escriviu α com una potència de β.

(g) Doneu una taula d'equivalències amb les notacions potencial amb potències de β, polinomial amb polinomis en α i vectorial.

(h) Calculeu $\beta^{15}\left(\frac{\beta^2-\beta^3}{\beta^6+\beta}\right)$.

Solució (p.75)

Exercici 61

Considerem el cos finit $\mathbb{F}_8 = \mathbb{Z}_2[x]/x^3 + x + 1$. Anomenem α a la classe de x.

1. Doneu la taula d'equivalències de les notacions exponencial i vectorial.
2. Doneu els oposats i els inversos dels elements de $\mathbb{F}_8$.
3. Doneu la taula de les sumes i la taula de les restes de $\mathbb{F}_8$.
4. Doneu la taula de les multiplicacions i la taula de les divisions de $\mathbb{F}_8$.
5. Calculeu $\frac{x^5+(\alpha+1)x^4+(\alpha^2+\alpha+1)x^3+\alpha^2x^2+\alpha x+\alpha^2+1}{x^2+\alpha^2x+\alpha}$.

Solució (p.76)

Exercici 62

Considerem el cos finit $\mathbb{F}_9 = \mathbb{Z}_3[x]/x^2 + 2x + 2$. Anomenem α a la classe de x.

1. Doneu la taula d'equivalències de les notacions exponencial i vectorial.
2. Doneu els oposats i els inversos dels elements de $\mathbb{F}_9$.
3. Doneu la taula de les sumes i la taula de les restes de $\mathbb{F}_9$.
4. Doneu la taula de les multiplicacions i la taula de les divisions de $\mathbb{F}_9$.
5. Calculeu $\frac{x^8-1}{x^4+\alpha^6x^3+x^2+\alpha^3x+\alpha^2}$.

Solució (p.77)

Exercici 63

(a) Justifiqueu si són irreductibles els següents polinomis a $\mathbb{Z}_2[x]$:

   i. $x^4 + 1$

   ii. $x^4 + x + 1$

   iii. $x^4 + x^2 + 1$

   iv. $x^4 + x^3 + x^2 + x + 1$

(b) Escriviu cadascun dels polinomis de l'apartat (a) com a producte de polinomis irreductibles.

(c) Doneu el màxim comú divisor de $x^4 + 1$ i $x^4 + x^2 + 1$.

(d) Podeu expressar el màxim comú divisor de $x^4 + 1$ i $x^4 + x^2 + 1$ com a combinació lineal dels mateixos polinomis? Doneu-ne els coeficients i feu la comprovació.

(e) Quines de les següents estructures són un cos i, en cas de ser-ho, quants elements tenen?

   i. $\mathbb{Z}_2[x]/x^4 + 1$

   ii. $\mathbb{Z}_2[x]/x^4 + x + 1$

   iii. $\mathbb{Z}_2[x]/x^4 + x^2 + 1$

   iv. $\mathbb{Z}_2[x]/x^4 + x^3 + x^2 + x + 1$

(f) En quins dels casos en què tenim un cos, si anomenem α a la classe de x, tenim que α és un element primitiu?

(g) Doneu una taula exponencial-polinòmica-vectorial per un cas en què α sigui primitiu. Els apartats que segueixen els referirem al mateix cas (la mateixa α i la mateixa taula).

(h) Quins són els ordres possibles dels elements del cos?

(i) Per a cadascun dels ordres possibles, doneu un element del cos amb aquell ordre.

Solució (p.78)

3.5 Solucions

Solució de l'Exercici 39

Si avaluem el polinomi $x^5 + 2x^3 + 3x^2 + 1$ a $x = 3$ ens dona $243 + 2 \cdot 27 + 3 \cdot 9 + 1 = 243 + 54 + 27 + 1 = 325$.

Com que $325 \equiv 3 \mod 7$, deduïm que 3 no és una arrel de $x^5 + 2x^3 + 3x^2 + 1$ a $\mathbb{Z}_7[x]$.

Com que $325 \equiv 0 \mod 5$, deduïm que 3 és una arrel de $x^5 + 2x^3 + 3x^2 + 1$ a $\mathbb{Z}_5[x]$.

Com que $325 \equiv 1 \mod 3$, deduïm que 3 no és una arrel de $x^5 + 2x^3 + 3x^2 + 1$ a $\mathbb{Z}_3[x]$.

Com que $325 \equiv 1 \mod 2$, deduïm que 3 no és una arrel de $x^5 + 2x^3 + 3x^2 + 1$ a $\mathbb{Z}_2[x]$.

Torna a l'exercici (p.53)

Solució de l'Exercici 40

Sabem que un polinomi $f(x) \in \mathbb{Z}_2[x]$ és divisible per x si i només si 0 és una arrel. I 0 és una arrel si i només si $f(0) = 0$. Com que $f(0)$ és exactament el terme constant, deduïm que $f(x)$ és divisible per x si i només si el seu terme constant és 0.

Sabem que un polinomi $f(x) \in \mathbb{Z}_2[x]$ és divisible per $x + 1$ si i només si 1 és una arrel. I 1 és una arrel si i només si $f(1) = 0$. Com que $f(1)$ és exactament el nombre de termes de $f(x)$, deduïm que $f(x)$ és divisible per $x+1$ si i només si el seu nombre de termes és parell.

Torna a l'exercici (p.53)

Solució de l'Exercici 41

1. 2 és invertible si p és senar perquè en aquest cas $\mathrm{mcd}(2,p)=1$.
2. L'element $p+1$ és parell i l'invers de 2 serà l'enter $\frac{p+1}{2}$ ja que $2\cdot\frac{p+1}{2}=p+1=1$ a $\mathbb{Z}_p$.
3.

a	a^2
0	0
1	1
2	4
3	2
4	2
5	4
6	1

4.

$$\begin{array}{|lcl|}\hline \sqrt{0}^{\mathbb{Z}_7} & = & \{0\} \\ \sqrt{1}^{\mathbb{Z}_7} & = & \{1,6\} \\ \sqrt{2}^{\mathbb{Z}_7} & = & \{3,4\} \\ \sqrt{3}^{\mathbb{Z}_7} & = & \varnothing=\{\} \\ \sqrt{4}^{\mathbb{Z}_7} & = & \{2,5\} \\ \hline\end{array}$$

5. Si substituïm x per 4 a $x^2+3x+2\in\mathbb{Z}_5[x]$ ens dona $4^2+3\cdot4+2=16+12+2=30=0$.
   Si substituïm x per 3 a $x^2+3x+2\in\mathbb{Z}_5[x]$ ens dona $3^2+3\cdot3+2=9+9+2=20=0$.
6.
   - Per x^2+5x+1 tenim $b=5, c=1$ i les arrels seran $(2+y)4 \mod 7$ on y agafa tots els valors de $\sqrt{0}^{\mathbb{Z}_7}=\{0\}$, és a dir, hi ha una única arrel en aquest cas, que és 1.
   - Per x^2+6 tenim $b=0, c=6$ i les arrels seran $(x)4 \mod 7$ on x agafa tots els valors de $\sqrt{4}^{\mathbb{Z}_7}=\{2,5\}$, és a dir, les arrels en aquest cas són 1 i 6.
   - Per x^2+5x+4 tenim $b=5, c=4$ i les arrels seran $(2+x)4 \mod 7$ on x agafa tots els valors de $\sqrt{25-16}^{\mathbb{Z}_7}=\sqrt{2}^{\mathbb{Z}_7}=\{3,4\}$, és a dir, les arrels en aquest cas són 6 i 3.
7.
   - Si substituïm x per 1 a $x^2+5x+1\in\mathbb{Z}_5[x]$ ens dona $1+5+1=0$.
   - Si substituïm x per 1 i $6=-1$ a $x^2+6\in\mathbb{Z}_5[x]$ ens dona $1+6=0$.
   - Si substituïm x per 3 a $x^2+5x+4\in\mathbb{Z}_5[x]$ ens dona $3^2+5\cdot3+4=2+1+4=0$. Si substituïm x per 6 a $x^2+5x+4\in\mathbb{Z}_5[x]$ ens dona $6^2+5\cdot6+4=1+2+4=0$.

Torna a l'exercici (p.54)

Solució de l'Exercici 42

Suposem que un polinomi $f(x)$ té grau 2 o 3 i que es pot descompondre en el producte següent:

$$f(x)=g(x)h(x),$$

amb $g(x)$ i $h(x)$ no constants. Les úniques opcions per als graus de $g(x)$ i $h(x)$ són:

Si $\mathrm{grau}(f)=2$

$\mathrm{grau}(g)$	$\mathrm{grau}(h)$
1	1

Si $\mathrm{grau}(f)=3$

$\mathrm{grau}(g)$	$\mathrm{grau}(h)$
2	1
1	2

En qualsevol cas, algun dels factors ha de ser de grau 1 i, per tant, de la forma $x - a$. En aquest cas a serà una arrel.

Torna a l'exercici (p.55)

Solució de l'Exercici 43

Analitzem per graus.

Grau 0: 1 és l'únic polinomi de grau 0 i és irreductible.

Grau 1: x i $x + 1$ són els únics polinomis de grau 1 i són irreductibles.

A partir de grau 2, observem que, pel lema 13,

- un polinomi és divisible per x si i només si no té terme constant,
- un polinomi és divisible per $x + 1$ si i només si té un nombre parell de coeficients.

Ara, per l'Exercici 42, pels casos de grau 2 i grau 3, aquestes condicions seran suficients per determinar els irreductibles. Així podem continuar:

Grau 2: $x^2 + x + 1$.

Grau 3: $x^3 + x^2 + 1$, $x^3 + x + 1$.

Per grau 4, suposem que $f(x)$ té grau 4 i es pot descompondre com

$$f(x) = g(x)h(x),$$

amb $g(x)$ i $h(x)$ no constants. Els graus de $g(x)$ i $h(x)$ poden ser:

grau(g)	grau(h)
3	1
2	2
1	3

En els casos primer i tercer tindríem una arrel, situació que podem descartar imposant que hi hagi terme constant i un nombre senar de termes no nuls.

El segon cas només es podria donar si algun dels factors té arrels (descartables amb les dues condicions anteriors) o bé si $g(x)$ i $h(x)$ són irreductibles de grau 2, és a dir, $g(x) = x^2 + x + 1$ i $h(x) = x^2 + x + 1$. En aquest cas, $f(x)$ seria $x^4 + x^2 + 1$. Així, podem concloure:

Grau 4: $x^4 + x^3 + 1$, $x^4 + x + 1$, $x^4 + x^3 + x^2 + x + 1$. Torna a l'exercici (p.55)

Solució de l'Exercici 44

1. Fem la divisió de polinomis

$$\begin{array}{rcccccl|l}
 & x^5 & & & +x^2 & +1 & & x^2+x+1 \\ \cline{8-8}
-(& x^5 & +x^4 & +x^3 & & &) & x^3+x^2 \\ \cline{1-7}
 & & x^4 & +x^3 & +x^2 & +1 & & \\
 & -(& x^4 & +x^3 & +x^2 & &) & \\ \cline{2-7}
 & & & & & 1 & &
\end{array}$$

   Obtenim $q = x^3 + x^2$, $r = 1$. Podem comprovar que, en efecte, $(x^2 + x + 1)(x^3 + x^2) + 1 = x^5 + x^4 + x^4 + x^3 + x^3 + x^2 + 1 = x^5 + x^2 + 1$.

2. El polinomi g és irreductible perquè té grau 2 i no té arrels. Com que el polinomi f té grau 5, per veure que és irreductible hem de veure que no té factors irreductibles de grau 1 (ho sabem perquè no té arrels) ni factors irreductibles de grau 2. Això darrer ho sabem perquè l'únic polinomi irreductible de grau 2 és $x^2 + x + 1 = g$ i, del primer apartat, deduïm que g no divideix f.

Torna a l'exercici (p.56)

Solució de l'Exercici 45

1. Hi ha 9 polinomis mònics de grau 2 a $\mathbb{Z}_3[x]$, ja que són tots els polinomis de la forma $x^2 + ax + b$ amb a i b variant cadascun en els tres valors de $\mathbb{Z}_3$.
2. El polinomi $x^2 + ax + b$, per ser irreductible, com que té grau 2, no ha de tenir arrels. Perquè 0 no sigui arrel, cal que $0^2 + 0a + b \neq 0$. Això implica $b = 1$ o $b = 2$. Perquè 1 no sigui arrel, cal que $1 + a + b \neq 0$. Perquè 2 no sigui arrel, cal que $4 + 2a + b \neq 0$. Això ens dona tres opcions:
   - $b = 1$, $a = 0$
   - $b = 2$, $a = 1$
   - $b = 2$, $a = 2$

   que corresponen als tres polinomis
   - $x^2 + 1$
   - $x^2 + x + 2$
   - $x^2 + 2x + 2$

Torna a l'exercici (p.56)

Solució de l'Exercici 46

1. $x^3 + x^2 + 2 \in P$,
   o bé
   $2x^{12} + x^8 + x^7 + 2x^6 + 2x^4 + 1 \in P$.
2. (a) La suma dels coeficients de p és $p(1)$. Si $p(1)$ és un múltiple de 3 aleshores s'anul·la a $\mathbb{Z}_3$ i 1 és una arrel de p. Per tant, p no és irreductible.

   (b) Tenim que $2^2 = 4 = 1$ a $\mathbb{Z}_3$. Per tant, $2^r = \begin{cases} 1 \text{ si } r \text{ és parell} \\ 2 \text{ si } r \text{ és senar} \end{cases}$

   Tenim que $p(2)$ és la suma de coeficients més 1 i, per tant, $p(2)$ no s'anul·la a $\mathbb{Z}_3$ si i només si la suma de coeficients és congruent amb 2 mòdul 3.
3. El coeficient constant, com que és $p(0)$, no ha de ser nul.

Torna a l'exercici (p.56)

Solució de l'Exercici 47

Observem que el polinomi $2x^4 + 4x^2 + 3x + 1$ té arrels 1 i 2. Per tant, és divisible per $(x+4)(x+3) = x^2 + 2x + 2$.

Dividim $2x^4 + 4x^2 + 3x + 1$ entre $x^2 + 2x + 2$.

$$
\begin{array}{rrrrrr|l}
 & 2x^4 & & +4x^2 & +3x & +1 & x^2+2x+2 \\
\cline{7-7}
-(& 2x^4 & +4x^3 & +4x^2 & &) & 2x^2+x+3 \\
\cline{1-6}
 & & x^3 & & +3x & +1 & \\
 & -(& x^3 & +2x^2 & +2x &) & \\
\cline{2-6}
 & & & 3x^2 & +x & +1 & \\
 & & -(& 3x^2 & +x & +1) & \\
\cline{3-6}
 & & & & & 0 &
\end{array}
$$

Ens dona $2x^2 + x + 3 = 2(x^2 + 3x + 4)$.

Com que $x^2 + 3x + 4$ té grau 2 i no té arrels, sabem que és irreductible.

Per tant, la factorització completa serà

$$2x^4 + 4x^2 + 3x + 1 = 2(x^2 + 3x + 4)(x + 3)(x + 4).$$

Torna a l'exercici (p.57)

Solució de l'Exercici 49

$\mathbb{Z}_2[x]/x^3 + x + 1 = \{[0], [1], [x], [x + 1], [x^2], [x^2 + 1], [x^2 + x], [x^2 + x + 1]\}$. Torna a l'exercici (p.58)

Solució de l'Exercici 50

1. $\mathbb{Z}_2[x]/x^3 + x + 1$ tindrà $2^3 = 8$ elements.
2. $\mathbb{Z}_3[x]/x^3 + x + 1$ tindrà $3^3 = 27$ elements.

Torna a l'exercici (p.58)

Solució de l'Exercici 51

1.

$$\begin{array}{rl|l} & x^2+2x+2 & 2x+1 \\ \cline{3-3} -(& x^2+2x \quad\ ) & 2x \\ \cline{2-2} & \qquad\quad 2 & \end{array}$$

1	0	1	
0	1	x	
		$2x$	$x+2$
x^2+2x+2	$2x+1$	2	0

Deduïm que $(x^2 + 2x + 2) + x(2x + 1) = 2$.

2. $2x + 1$ és invertible perquè és coprimer amb $x^2 + 2x + 2$. De la igualtat $(x^2 + 2x + 2) + x(2x + 1) = 2$ deduïm que $2(x^2 + 2x + 2) + 2x(2x + 1) = 1$. En conseqüència, l'invers de $(2x + 1)$ és $2x$.

3. Observem que $x + 2 = 2(2x + 1)$. Com que $(2x + 1)(2x) = 1$, també $(2(2x + 1))(2(2x)) = 1$, és a dir, $(x + 2)x = 1$. Per tant, l'invers de $x + 2$ és x.

4.
   - $(2x + 1)(2x) = 4x^2 + 2x = x^2 + 2x = x^2 + 2x - (x^2 + 2x + 2) = -2 = 1 \mod x^2 + 2x + 2$.
   - $(x + 2)(x) = x^2 + 2x = x^2 + 2x - (x^2 + 2x + 2) = -2 = 1 \mod x^2 + 2x + 2$.

Torna a l'exercici (p.60)

Solució de l'Exercici 52

1. A $\mathbb{Z}_2[x]/x^2 + x + 1$:

$+$	$[0]$	$[1]$	$[x]$	$[x+1]$
$[0]$	$[0]$	$[1]$	$[x]$	$[x+1]$
$[1]$	$[1]$	$[0]$	$[x+1]$	$[x]$
$[x]$	$[x]$	$[x+1]$	$[0]$	$[1]$
$[x+1]$	$[x+1]$	$[x]$	$[1]$	$[0]$

$\times$	$[0]$	$[1]$	$[x]$	$[x+1]$
$[0]$	$[0]$	$[0]$	$[0]$	$[0]$
$[1]$	$[0]$	$[1]$	$[x]$	$[x+1]$
$[x]$	$[0]$	$[x]$	$[x+1]$	$[1]$
$[x+1]$	$[0]$	$[x+1]$	$[1]$	$[x]$

2. A $\mathbb{Z}_2[x]/x^2 + 1$:

+	[0]	[1]	[x]	[$x+1$]
[0]	[0]	[1]	[x]	[$x+1$]
[1]	[1]	[0]	[$x+1$]	[x]
[x]	[x]	[$x+1$]	[0]	[1]
[$x+1$]	[$x+1$]	[x]	[1]	[0]

×	[0]	[1]	[x]	[$x+1$]
[0]	[0]	[0]	[0]	[0]
[1]	[0]	[1]	[x]	[$x+1$]
[x]	[0]	[x]	[1]	[$x+1$]
[$x+1$]	[0]	[$x+1$]	[$x+1$]	[0]

3. A $\mathbb{Z}_3[x]/x^2+1$:

×	[0]	[1]	[2]	[x]	[$x+1$]	[$x+2$]	[$2x$]	[$2x+1$]	[$2x+2$]
[0]	[0]	[0]	[0]	[0]	[0]	[0]	[0]	[0]	[0]
[1]	[0]	[1]	[2]	[x]	[$x+1$]	[$x+2$]	[$2x$]	[$2x+1$]	[$2x+2$]
[2]	[0]	[2]	[1]	[$2x$]	[$2x+2$]	[$2x+1$]	[x]	[$x+2$]	[$x+1$]
[x]	[0]	[x]	[$2x$]	[2]	[$x+2$]	[$2x+2$]	[1]	[$x+1$]	[$2x+1$]
[$x+1$]	[0]	[$x+1$]	[$2x+2$]	[$x+2$]	[$2x$]	[1]	[$2x+1$]	[2]	[x]
[$x+2$]	[0]	[$x+2$]	[$2x+1$]	[$2x+2$]	[1]	[x]	[$x+1$]	[$2x$]	[2]
[$2x$]	[0]	[$2x$]	[x]	[1]	[$2x+1$]	[$x+1$]	[2]	[$2x+2$]	[$x+2$]
[$2x+1$]	[0]	[$2x+1$]	[$x+2$]	[$x+1$]	[2]	[$2x$]	[$2x+2$]	[x]	[1]
[$2x+2$]	[0]	[$2x+2$]	[$x+1$]	[$2x+1$]	[x]	[2]	[$x+2$]	[1]	[$2x$]

4. Podem observar que, en el primer cas i en el tercer cas, en la taula del producte hi ha el valor [1] en totes les files i en totes les columnes, excepte en les que corresponen a [0]. Això significa que qualsevol valor no nul de l'anell en té un altre de manera que el producte dels dos és [1]. Per tant, qualsevol valor no nul de l'anell té invers i això fa que l'anell sigui un cos.

   En el segon cas, el valor $[x+1]$ no té invers perquè no hi ha cap valor que multiplicat per ell doni [1]. Per això el segon cas no es tracta d'un cos.

Torna a l'exercici (p.61)

Solució de l'Exercici 53

El polinomi buscat ha de ser irreductible i de grau 3.

Podem agafar x^3+2x^2+1 o bé x^3+x^2+2.

Torna a l'exercici (p.61)

Solució de l'Exercici 56

Si l'ordre de la classe $[x]_f$ és k, aleshores tenim $x^k \equiv 1 \mod f(x)$ i, per tant, $x^k - 1$ és un múltiple de $f(x)$.

Això implica que k ha de ser més gran o igual que el grau de $f(x)$. Torna a l'exercici (p.62)

Solució de l'Exercici 57

1. Perquè $\mathbb{Z}_2[x]/f(x)$ sigui un cos de 4 elements, cal que $f(x)$ sigui irreductible i que el grau de $f(x)$ sigui 2. Els polinomis de grau 2 són
   - x^2
   - x^2+1
   - x^2+x

- $x^2 + x + 1$

Cap dels tres primers polinomis és irreductible a $\mathbb{Z}_2[x]$.

En efecte, $x^2 = x \cdot x$, $x^2 + 1 = (x+1) \cdot (x+1)$ i $x^2 + x = x(x+1)$.

El quart és irreductible, ja que és de grau 2 i no té arrels ($0^2 + 0 + 1 \neq 0$ i $1^2 + 1 + 1 \neq 0$).

Agafem, doncs, $x^2 + x + 1$.

Comprovem que la classe de x és un element primitiu.

Anomenem $\alpha = [x]$.

Tenim $\alpha^2 = \alpha^2 - (\alpha^2 + \alpha + 1) = -\alpha - 1 = \alpha + 1 \neq 1$ i, per tant, és un element primitiu.

La taula d'equivalències potencial-vectorial-polinomial és la següent:

pot.	*vec.*	*pol.*
0	$(0,0)$	0
α^0	$(1,0)$	1
α	$(0,1)$	α
α^2	$(1,1)$	$1+\alpha$

Les taules de la suma i del producte són

$+$	0	1	α	α^2
0	0	1	α	α^2
1	1	0	α^2	α
α	α	α^2	0	1
α^2	α^2	α	1	0

$\times$	0	1	α	α^2
0	0	0	0	0
1	0	1	α	α^2
α	0	α	α^2	1
α^2	0	α^2	1	α

Hem utilitzat, entre d'altres,

$\alpha^2 + 1 = (\alpha+1) + 1 = \alpha + 2 = \alpha$

$\alpha^2 + \alpha = (\alpha+1) + \alpha = 2\alpha + 1 = 1$

$\alpha \cdot \alpha^2 = \alpha(\alpha+1) = \alpha^2 + \alpha = (\alpha+1) + \alpha = 2\alpha + 1 = 1$

$\alpha^2 \cdot \alpha^2 = (\alpha+1)(\alpha+1) = \alpha^2 + \alpha + \alpha + 1 = \alpha^2 + 2\alpha + 1 = \qquad \alpha^2 + 1 = (\alpha+1) + 1 = \alpha + 2 = \alpha$

Torna a l'exercici (p.64)

Solució de l'Exercici 58

1. Veiem que 3 és primer i després cal veure si $x^2 + x + 2$ és irreductible i ho és perquè té grau 2 i no té arrels.

   En efecte,

$$\begin{aligned} f(0) &= 2 \neq 0 \\ f(1) &= 1 \neq 0 \\ f(2) &= 2 \neq 0 \end{aligned}$$

2. $3^2 = 9$.

3. Els únics ordres possibles dels elements de $\mathbb{Z}_3[x]/x^2 + x + 2$ són els divisors de $9 - 1 = 8$, és a dir, $\{1, 2, 4, 8\}$.

   Però α^1 i α^2 són $\neq 1$ i $\alpha^4 = (\alpha^2)^2 = (2\alpha+1)^2 = 4\alpha^2 + 4\alpha + 1 = \alpha^2 + \alpha + 1 = 2\alpha + 1 + \alpha + 1 = 2 \neq 1$.

   Per tant, l'ordre de α no és $1, 2$ ni 4 i ha de ser 8.

4. Utilitzarem que $\alpha^2 = 2\alpha + 1$. Així,

$$\begin{aligned}
\alpha^3 &= \alpha\alpha^2 = \alpha(2\alpha+1) = 2\alpha^2+\alpha = 2(2\alpha+1)+\alpha = 2\alpha+2\\
\alpha^4 &= \alpha\alpha^3 = \alpha(2\alpha+2) = 2\alpha^2+2\alpha = 2(2\alpha+1)+2\alpha = 2\\
\alpha^5 &= \alpha\alpha^4 = \alpha(2) = 2\alpha\\
\alpha^6 &= \alpha\alpha^5 = \alpha(2\alpha) = 2\alpha^2 = 2(2\alpha+1) = \alpha+2\\
\alpha^7 &= \alpha\alpha^6 = \alpha(\alpha+2) = \alpha^2+2\alpha = (2\alpha+1)+2\alpha = \alpha+1\\
\alpha^8 &= \alpha\alpha^7 = \alpha(\alpha+1) = \alpha^2+\alpha = (2\alpha+1)+\alpha = 1
\end{aligned}$$

I obtenim la taula

$pot.$	$pol.$	$vect.$
0	0	$(0,0)$
α	α	$(0,1)$
α^2	$2\alpha+1$	$(1,2)$
α^3	$2\alpha+2$	$(2,2)$
α^4	2	$(2,0)$
α^5	2α	$(0,2)$
α^6	$\alpha+2$	$(2,1)$
α^7	$\alpha+1$	$(1,1)$
α^8	1	$(1,0)$

5.

$$\begin{aligned}
\alpha^2\left(\frac{\alpha^{20}-\alpha^5+\alpha}{\alpha^3-\alpha}\right) &= \alpha^2\left(\frac{\alpha^4-\alpha^5+\alpha}{\alpha^3-\alpha}\right)\\
&= \alpha^2\left(\frac{2-2\alpha+\alpha}{2\alpha+2-\alpha}\right)\\
&= \alpha^2\left(\frac{2+2\alpha}{\alpha+2}\right)\\
&= \alpha^2\left(\frac{\alpha^3}{\alpha^6}\right)\\
&= \frac{\alpha^5}{\alpha^6}\\
&= \frac{\alpha^{13}}{\alpha^6}\\
&= \alpha^7.
\end{aligned}$$

Torna a l'exercici (p.65)

Solució de l'Exercici 59

1. Com que són polinomis de grau 3, n'hi ha prou de veure si tenen arrels.
   - $f(x) = x^3 + x^2 + 2$ no té arrels, ja que $f(0) = 2 \neq 0$, $f(1) = 1 \neq 0$ i $f(2) = 2 \neq 0$. Per tant, és irreductible.
   - $g(x) = x^3 + 2x + 1$ no té arrels, ja que $g(0) = 1 \neq 0$, $g(1) = 1 \neq 0$ i $g(2) = 1 \neq 0$. Per tant, és irreductible.
   - $h(x) = x^3 + 2x^2 + 2$ és reductible, ja que $h(0) = 2 \neq 0$, $h(1) = 2 \neq 0$, però $h(2) = 0$. Per tant, $h(x)$ és divisible per $x - 2$.

2. Perquè un polinomi $a(x) \in \mathbb{Z}_p[x]$ sigui primitiu, cal que sigui irreductible i que la classe de x dins de $\mathbb{Z}_p/(a(x))$ sigui un element primitiu, és a dir, tingui ordre $p^{\text{grau}(a)} - 1$.

En el nostre cas, caldrà que l'ordre de la classe de x sigui 26.

Si el grau de $a(x)$ és 3, els ordres de tots els elements de $\mathbb{Z}_3/(a(x))$ seran divisors de 26. Per tant, només podran ser $1, 2, 13$ o 26.

En els casos de f i g, la classe de x no tindrà ordre 1, ni 2, ja que

$$\begin{array}{rl} x \not\equiv 1 \mod f & (\text{perquè } x-1 \text{ no pot ser un múltiple de } x^3+\ldots) \\ x^2 \not\equiv 1 \mod f & (\text{perquè } x^2-1 \text{ no pot ser un múltiple de } x^3+\ldots) \\ x \not\equiv 1 \mod g & (\text{perquè } x-1 \text{ no pot ser un múltiple de } x^3+\ldots) \\ x^2 \not\equiv 1 \mod g & (\text{perquè } x^2-1 \text{ no pot ser un múltiple de } x^3+\ldots). \end{array}$$

Per tant, l'ordre només pot ser 13 o 26. Per això mirarem si $x^{13} \equiv 1 \mod f$ o $x^{13} \equiv 1 \mod g$.

$$\begin{aligned} x^{13} &\equiv x^2x^{11} \mod f \\ &\equiv x^2(x+1) \mod f \\ &\equiv x^3+x^2 \mod f \\ &\equiv f+1 \mod f \\ &\equiv 1 \mod f \end{aligned}$$

$$\begin{aligned} x^{13} &\equiv x^2x^{11} \mod g \\ &\equiv x^2(x^2+x+2) \mod g \\ &\equiv x(x^3+x^2+2x) \mod g \\ &\equiv x(g(x)+2+x^2) \mod g \\ &\equiv x^3+2x \mod g \\ &\equiv g(x)+2 \mod g \\ &\equiv 2 \mod g \\ &\not\equiv 1 \mod g \end{aligned}$$

Observem que, pel cas de $f(x)$, la classe de x té ordre 13 i, per tant, $f(x)$ no és primitiu. En canvi, pel cas de $g(x)$, la classe de x no té ordre 13 i, per tant, ha de tenir ordre 26. Deduïm que $g(x)$ és primitiu.

3. $f(x)$ i $g(x)$. El cos tindrà $3^3 = 27$ elements.
4. $g(x)$.

Torna a l'exercici (p.65)

Solució de l'Exercici 60

(a) És un cos perquè, d'una banda, 3 és primer i, d'altra banda, x^2+1 té grau 2 i no té arrels i, per tant, és irreductible a $\mathbb{Z}_3[x]$.

(b) $3^2 = 9$.

(c) $\alpha^1 \neq 1$, $\alpha^2 = 2 \neq 1$, $\alpha^3 = 2\alpha \neq 1$, $\alpha^4 = (\alpha^2)^2 = 2^2 = 1$. Per tant, l'ordre de α és 4.

(d) No ho és perquè per ser primitiu hauria de tenir ordre $9-1 = 8$.

(e) Els únics ordres possibles són els divisors de 8 i, per tant, β és primitiu si i només si $\beta^4 \neq 1$. Agafem $\beta = \alpha+1$ i veiem que és un element primitiu. En efecte, si $\beta = \alpha+1$, aleshores $\beta^2 = (\alpha+1)^2 = \alpha^2+2\alpha+1$. Ara $\beta^4 = (\beta^2)^2$ serà

$$\begin{aligned} (\alpha^2+2\alpha+1)^2 &= \alpha^2(\alpha^2+2\alpha+1)+2\alpha(\alpha^2+2\alpha+1)+(\alpha^2+2\alpha+1) \\ &= (\alpha^4+2\alpha^3+\alpha^2)+(2\alpha^3+4\alpha^2+2\alpha)+(\alpha^2+2\alpha+1) \\ &= \alpha^4+4\alpha^3+6\alpha^2+4\alpha+1 \\ &= \alpha^4+\alpha^3+\alpha+1 \\ &= (1)+(2\alpha)+\alpha+1 \\ &= 3\alpha+2 \\ &= 2 \neq 1 \end{aligned}$$

Haguéssim pogut agafar $\beta = \alpha+2$, $\beta = 2\alpha+1$, $\beta = 2\alpha+2$ i també ens haurien donat elements primitius.

(f) Ho podem fer a partir de la taula de l'apartat següent i obtenim $\alpha = \beta^6$. Si en lloc d'agafar $\beta = \alpha + 1$ haguéssim agafat $\beta = 2\alpha + 2$, seria el mateix. Si haguéssim agafat $\beta = \alpha + 2$ o bé $\beta = 2\alpha + 1$, aleshores tindríem $\alpha = \beta^2$.

(g) Depenent de quina β haguem agafat, tindrem alguna de les següents taules:

pot.	pol.	vect.
0	0	$(0,0)$
β	$\alpha+1$	$(1,1)$
β^2	2α	$(0,2)$
β^3	$2\alpha+1$	$(1,2)$
β^4	2	$(2,0)$
β^5	$2\alpha+2$	$(2,2)$
β^6	α	$(0,1)$
β^7	$\alpha+2$	$(2,1)$
β^8	1	$(1,0)$

pot.	pol.	vect.
0	0	$(0,0)$
β	$\alpha+2$	$(2,1)$
β^2	α	$(0,1)$
β^3	$2\alpha+2$	$(2,2)$
β^4	2	$(2,0)$
β^5	$2\alpha+1$	$(1,2)$
β^6	2α	$(0,2)$
β^7	$\alpha+1$	$(1,1)$
β^8	1	$(1,0)$

pot.	pol.	vect.
0	0	$(0,0)$
β	$2\alpha+1$	$(1,2)$
β^2	α	$(0,1)$
β^3	$\alpha+1$	$(1,1)$
β^4	2	$(2,0)$
β^5	$\alpha+2$	$(2,1)$
β^6	2α	$(0,2)$
β^7	$2\alpha+2$	$(2,2)$
β^8	1	$(1,0)$

pot.	pol.	vect.
0	0	$(0,0)$
β	$2\alpha+2$	$(2,2)$
β^2	2α	$(0,2)$
β^3	$\alpha+2$	$(2,1)$
β^4	2	$(2,0)$
β^5	$\alpha+1$	$(1,1)$
β^6	α	$(0,1)$
β^7	$2\alpha+1$	$(1,2)$
β^8	1	$(1,0)$

(h) En tots els casos dona 1. Vegem-ho en el cas $\beta = \alpha + 1$: $\beta^{15}\left(\frac{\beta^2-\beta^3}{\beta^6+\beta}\right) = \beta^{-1}\left(\frac{\beta^2-\beta^3}{\beta^6+\beta}\right) = \frac{\beta-\beta^2}{\beta^6+\beta} = \frac{1-\beta}{\beta^5+1} = \frac{2\alpha}{2\alpha} = 1$.

Torna a l'exercici (p.65)

Solució de l'Exercici 61

1.

pot.	*vec.*
0	000
α^0	100
α^1	010
α^2	001
α^3	110
α^4	011
α^5	111
α^6	101

2.

a	$-a$
0	0
1	1
α	α
α^2	α^2
α^3	α^3
α^4	α^4
α^5	α^5
α^6	α^6

a	a^{-1}
1	1
α	α^6
α^2	α^5
α^3	α^4
α^4	α^3
α^5	α^2
α^6	α

3.

$+$	1	α	α^2	α^3	α^4	α^5	α^6
1	0	α^3	α^6	α	α^5	α^4	α^2
α	α^3	0	α^4	1	α^2	α^6	α^5
α^2	α^6	α^4	0	α^5	α	α^3	1
α^3	α	1	α^5	0	α^6	α^2	α^4
α^4	α^5	α^2	α	α^6	0	1	α^3
α^5	α^4	α^6	α^3	α^2	1	0	α
α^6	α^2	α^5	1	α^4	α^3	α	0

$-$	1	α	α^2	α^3	α^4	α^5	α^6
1	0	α^3	α^6	α	α^5	α^4	α^2
α	α^3	0	α^4	1	α^2	α^6	α^5
α^2	α^6	α^4	0	α^5	α	α^3	1
α^3	α	1	α^5	0	α^6	α^2	α^4
α^4	α^5	α^2	α	α^6	0	1	α^3
α^5	α^4	α^6	α^3	α^2	1	0	α
α^6	α^2	α^5	1	α^4	α^3	α	0

4.

$\cdot$	1	α	α^2	α^3	α^4	α^5	α^6
1	1	α	α^2	α^3	α^4	α^5	α^6
α	α	α^2	α^3	α^4	α^5	α^6	1
α^2	α^2	α^3	α^4	α^5	α^6	1	α
α^3	α^3	α^4	α^5	α^6	1	α	α^2
α^4	α^4	α^5	α^6	1	α	α^2	α^3
α^5	α^5	α^6	1	α	α^2	α^3	α^4
α^6	α^6	1	α	α^2	α^3	α^4	α^5

/	1	α	α^2	α^3	α^4	α^5	α^6
1	1	α^6	α^5	α^4	α^3	α^2	α
α	α	1	α^6	α^5	α^4	α^3	α^2
α^2	α^2	α	1	α^6	α^5	α^4	α^3
α^3	α^3	α^2	α	1	α^6	α^5	α^4
α^4	α^4	α^3	α^2	α	1	α^6	α^5
α^5	α^5	α^4	α^3	α^2	α	1	α^6
α^6	α^6	α^5	α^4	α^3	α^2	α	1

5. Per la taula d'equivalències observem que

$$x^5+(\alpha+1)x^4+(\alpha^2+\alpha+1)x^3+\alpha^2x^2+\alpha x+\alpha^2+1 = x^5+\alpha^3x^4+\alpha^5x^3+\alpha^2x^2+\alpha x+\alpha^6.$$

Fem la divisió:

$$\begin{array}{rl}
x^5+\alpha^3x^4+\alpha^5x^3+\alpha^2x^2+\alpha x+\alpha^6 & \big|\ x^2+\alpha^2x+\alpha \\
-(x^5+\alpha^2x^4+\alpha x^3) & \quad x^3+\alpha^5x^2+\alpha^2x+\alpha^5 \\
\hline
\alpha^5x^4+\alpha^6x^3+\alpha^2x^2+\alpha x+\alpha^6 & \\
-(\alpha^5x^4+x^3+\alpha^6x^2) & \\
\hline
\alpha^2x^3+x^2+\alpha x+\alpha^6 & \\
-(\alpha^2x^3+\alpha^4x^2+\alpha^3x) & \\
\hline
\alpha^5x^2+x+\alpha^6 & \\
-(\alpha^5x^2+x+\alpha^6) & \\
\hline
0 &
\end{array}$$

Per tant, $\frac{x^5+(\alpha+1)x^4+(\alpha^2+\alpha+1)x^3+\alpha^2x^2+\alpha x+\alpha^2+1}{x^2+\alpha^2x+\alpha} = x^3+\alpha^5x^2+\alpha^2x+\alpha^5$.

Torna a l'exercici (p.66)

Solució de l'Exercici 62

1.

pot.	*vec.*
0	00
α^0	10
α^1	01
α^2	11
α^3	12
α^4	20
α^5	02
α^6	22
α^7	21

2.

a	$-a$
0	0
1	α^4
α	α^5
α^2	α^6
α^3	α^7
α^4	1
α^5	α
α^6	α^2
α^7	α^3

a	a^{-1}
1	1
α	α^7
α^2	α^6
α^3	α^5
α^4	α^4
α^5	α^3
α^6	α^2
α^7	α

3.

$+$	1	α	α^2	α^3	α^4	α^5	α^6	α^7
1	α^4	α^2	α^7	α^6	0	α^3	α^5	α
α	α^2	α^5	α^3	1	α^7	0	α^4	α^6
α^2	α^7	α^3	α^6	α^4	α	1	0	α^5
α^3	α^6	1	α^4	α^7	α^5	α^2	α	0
α^4	0	α^7	α	α^5	1	α^6	α^3	α^2
α^5	α^3	0	1	α^2	α^6	α	α^7	α^4
α^6	α^5	α^4	0	α	α^3	α^7	α^2	1
α^7	α	α^6	α^5	0	α^2	α^4	1	α^3

$-$	1	α	α^2	α^3	α^4	α^5	α^6	α^7
1	0	α^3	α^5	α	α^4	α^2	α^7	α^6
α	α^7	0	α^4	α^6	α^2	α^5	α^3	1
α^2	α	1	0	α^5	α^7	α^3	α^6	α^4
α^3	α^5	α^2	α	0	α^6	1	α^4	α^7
α^4	1	α^6	α^3	α^2	0	α^7	α	α^5
α^5	α^6	α	α^7	α^4	α^3	0	1	α^2
α^6	α^3	α^7	α^2	1	α^5	α^4	0	α
α^7	α^2	α^4	1	α^3	α	α^6	α^5	0

4.

$\cdot$	1	α	α^2	α^3	α^4	α^5	α^6	α^7
1	1	α	α^2	α^3	α^4	α^5	α^6	α^7
α	α	α^2	α^3	α^4	α^5	α^6	α^7	1
α^2	α^2	α^3	α^4	α^5	α^6	α^7	1	α
α^3	α^3	α^4	α^5	α^6	α^7	1	α	α^2
α^4	α^4	α^5	α^6	α^7	1	α	α^2	α^3
α^5	α^5	α^6	α^7	1	α	α^2	α^3	α^4
α^6	α^6	α^7	1	α	α^2	α^3	α^4	α^5
α^7	α^7	1	α	α^2	α^3	α^4	α^5	α^6

$/$	1	α	α^2	α^3	α^4	α^5	α^6	α^7
1	1	α^7	α^6	α^5	α^4	α^3	α^2	α
α	α	1	α^7	α^6	α^5	α^4	α^3	α^2
α^2	α^2	α	1	α^7	α^6	α^5	α^4	α^3
α^3	α^3	α^2	α	1	α^7	α^6	α^5	α^4
α^4	α^4	α^3	α^2	α	1	α^7	α^6	α^5
α^5	α^5	α^4	α^3	α^2	α	1	α^7	α^6
α^6	α^6	α^5	α^4	α^3	α^2	α	1	α^7
α^7	α^7	α^6	α^5	α^4	α^3	α^2	α	1

5.

$$
\begin{array}{rl|l}
 & x^8 \qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad + \alpha^4 & x^4+\alpha^6x^3+x^2+\alpha^3x+\alpha^2 \\ \cline{3-3}
 & -(x^8+\alpha^6x^7+x^6+\alpha^3x^5+\alpha^2x^4) & x^4+\alpha^2x^3+x^2+\alpha^7x+\alpha^2 \\ \cline{2-2}
 & \alpha^2x^7+\alpha^4x^6+\alpha^7x^5+\alpha^6x^4 \qquad\qquad + \alpha^4 & \\
 & -(\alpha^2x^7+x^6+\alpha^2x^5+\alpha^5x^4+\alpha^4x^3) & \\ \cline{2-2}
 & x^6+x^5+\alpha^4x^4+x^3 \qquad\qquad + \alpha^4 & \\
 & -(x^6+\alpha^6x^5+x^4+\alpha^3x^3+\alpha^2x^2) & \\ \cline{2-2}
 & \alpha^7x^5+x^4+\alpha x^3+\alpha^6x^2 \qquad + \alpha^4 & \\
 & -(\alpha^7x^5+\alpha^5x^4+\alpha^7x^3+\alpha^2x^2+\alpha x) & \\ \cline{2-2}
 & \alpha^2x^4+x^3+\alpha^2x^2+\alpha^5x+\alpha^4 & \\
 & -(\alpha^2x^4+x^3+\alpha^2x^2+\alpha^5x+\alpha^4) & \\ \cline{2-2}
 & 0 &
\end{array}
$$

Per tant, $\frac{x^8-1}{x^4+\alpha^6x^3+x^2+\alpha^3x+\alpha^2} = x^4+\alpha^2x^3+x^2+\alpha^7x+\alpha^2$.

Torna a l'exercici (p.66)

Solució de l'Exercici 63

(a)
- i. El primer polinomi s'anul·la en 1 i, per tant, és reductible.
- ii. El segon polinomi no té arrels. Per ser reductible hauria de ser el quadrat de l'únic polinomi reductible de grau 2, és a dir, hauria de ser $(x^2+x+1)^2 = x^4+x^2+1$, però veiem que no ho és. Per tant, és irreductible.
- iii. El tercer polinomi acabem de veure que és $(x^2+x+1)^2 = x^4+x^2+1$, per això és reductible.

iv. El quart polinomi és irreductible pel mateix argument que el segon.

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

(c) 1, perquè no tenen factors irreductibles no constants en comú.

(d) Utilitzem l'algoritme d'Euclides.

1	0	1	x^2
0	1	-1	x^2+1
		1	x^2
x^4+x^2+1	x^4+1	x^2	1

Obtenim que $(x^2)(x^4+x^2+1)+(x^2+1)(x^4+1)=1$.

Comprovem el resultat: $(x^2)(x^4+x^2+1)+(x^2+1)(x^4+1)=(x^6+x^4+x^2)+(x^6+x^2)+(x^4+1)=1$.

(e) La segona i la quarta. Tenen $2^4=16$ elements.

(f) Sabem que els únics ordres possibles de α són els divisors de 15, és a dir, $1, 3, 5, 15$. Perquè α sigui primitiu cal que el seu ordre sigui màxim, és a dir, 15.

En el segon cas, α té ordre 15, ja que $1, 3$ són més petits que el grau del polinomi generador i $\alpha^5 = \alpha\alpha^4=\alpha(\alpha+1)=\alpha^2+\alpha\neq 1$. Per tant, α és primitiu.

En el quart cas, $\alpha^5=\alpha(\alpha^3+\alpha^2+\alpha+1)=\alpha^4+\alpha^3+\alpha^2+\alpha=\alpha^3+\alpha^2+\alpha+1+\alpha^3+\alpha^2+\alpha=1$. Per tant, α té ordre $5<15$ i no és primitiu.

(g)

exp.	pol.	vect.
α^0	1	1000
α^1	α	0100
α^2	α^2	0010
α^3	α^3	0001
α^4	$\alpha+1$	0011
α^5	$\alpha^2+\alpha$	0110
α^6	$\alpha^3+\alpha^2$	0011
α^7	$\alpha^3+\alpha+1$	1101
α^8	α^2+1	1010
α^9	$\alpha^3+\alpha$	0101
α^{10}	$\alpha^2+\alpha+1$	1110
α^{11}	$\alpha^3+\alpha^2+\alpha$	0111
α^{12}	$\alpha^3+\alpha^2+\alpha+1$	1111
α^{13}	$\alpha^3+\alpha^2+1$	1011
α^{14}	α^3+1	1001

(h) Tots els divisors de $16-1=15$, que són $1, 3, 5, 15$.

(i) 1 té ordre 1, $\alpha^5=\alpha^2+\alpha$ té ordre 3, α^3 té ordre 5 i α té ordre 15.

Torna a l'exercici (p.67)

4 Teoria de codis: codis lineals

4.1 Motivació

Suposem que en una comunicació amb molt de soroll ambiental s'han de comunicar una de les paraules

CERT o **FALS**.

Si el receptor rep la paraula

CART,

quina paraula deduiríeu que s'ha enviat?

CERT →**CART**.

En aquest cas podem dir que s'ha produït **un error**.

Suposem que s'han esborrat algunes lletres i hem rebut

??LS.

Què es deu haver enviat?

FALS →**??LS**

En aquest cas podem dir que s'han produït **dos esborralls**.

I si rebem

CALT,

podem deduir què s'ha enviat?

La teoria de codis gira al voltant d'aquesta problemàtica.

El conjunt

$$\{CERT, FALS\}$$

seria un codi que permetria transmetre dues paraules.

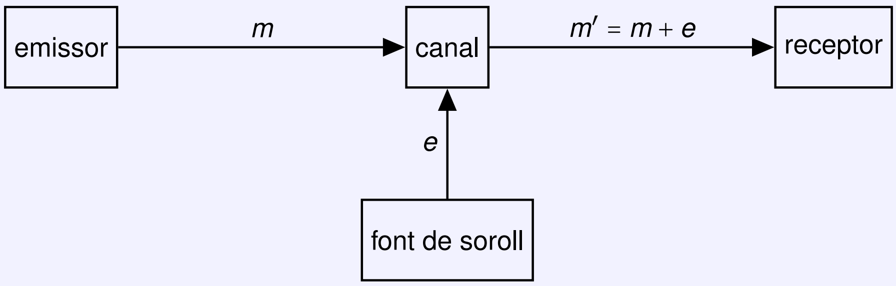
Podríem corregir un sol error en cada paraula i fins a tres esborralls.

Veurem exemples més grans, però, sobretot, dotats d'estructures més potents.

Aquestes estructures ens permetran transmetre qualsevol seqüència de missatges a través d'un procés de codificació i ens permetran predir quants errors i quants esborralls es poden produir, de manera que es puguin corregir i, finalment, ens donaran eines per corregir i per tornar a descodificar i obtenir així la informació original.

Model de comunicació

En general, per abordar el problema de l'exemple, es pot considerar el model de la figura. Un **emissor** envia un missatge m a un **receptor** a través d'un **canal** de comunicació en el qual hi ha cert **soroll**. El receptor rep $m' = m + e$, on e és soroll.



m: missatge enviat, m': missatge rebut, e: soroll

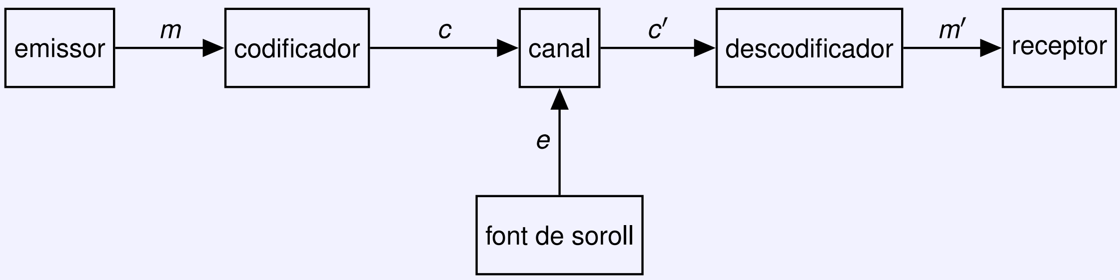
Perquè la comunicació sigui satisfactòria, el que volem és que el receptor pugui conèixer m.

A l'exemple anterior, la informació que s'enviava era binària: cert o fals. De fet, era suficient enviar un bit: 1 (cert) o 0 (fals). Però si només s'envia el bit d'informació, si hi ha soroll, el missatge es pot perdre completament.

És per això que les llengües han evolucionat buscant un **codi** que intenta reduir els problemes ocasionats pel soroll ambiental, per comunicar-nos millor.

A les comunicacions digitals tenim el mateix problema. Aquest problema s'aborda formalment a la **teoria de codis**.

Per minimitzar els problemes causats pel soroll, s'incorporen mecanismes de **codificació** i **descodificació**. Ara, el que s'envia a través del canal és el missatge codificat.



m: missatge enviat, c: codificació del missatge, c': codificació rebuda, m': missatge obtingut, e: soroll

Afegint mecanismes de codificació, el que buscarem serà que la comunicació sigui

- **fiable**: Que el receptor obtingui $m' = m$ amb *alta* probabilitat,
- **eficient**: Que la proporció entre la llargada de c i de m sigui *petita*.

El que ens cal és trobar un compromís entre aquestes dues propietats. Això es pot veure al següent exemple.

Exemple. *Suposem que el missatge és un bit b. Si volem una comunicació molt fiable, podem utilitzar un* ***codi*** *de r-**repetició**: repetim r vegades el bit b.*

Amb un codi de 3-repetició, tindríem $c = bbb$. És a dir, si $b = 0$, $c = 000$, i si $b = 1$, $c = 111$. Es descodificarà pel criteri de la majoria:

- *Si el receptor rep $c' = 000, 100, 010,$ o 001, dirà que $m' = 0$.*
- *Si el receptor rep $c' = 111, 011, 101,$ o 110, dirà que $m' = 1$.*

Això es pot estendre a qualsevol r imparell. Com més gran sigui r, més ***fiable*** *serà. Però, com més gran* *sigui r, menor **eficiència** tindrem.*

En aquest curs veurem codis que permeten un millor compromís entre fiabilitat i eficiència.

4.2 Codis lineals

Definició

Un **codi lineal** C de **longitud** n sobre un alfabet $\mathbb{F}_q$ és un subespai vectorial de $\mathbb{F}_q^n$.

Exercici 64

Dins de $\mathbb{F}_2^3$ considerem el conjunt de paraules

$$C = \{(000), (111), (101), (010)\}.$$

Demostreu que C és un codi lineal.
Solució (p.97)

Si $q = 2$, aleshores diem que el codi és **binari**, mentre que si $q = 3$, aleshores diem que el codi és **ternari**.

Exercici 65

Com és el codi $C = \{(000), (111), (101), (010)\}$ de l'exercici anterior?
Solució (p.98)

La **dimensió** k del codi és la dimensió del subespai.

Exercici 66

Quina seria la dimensió del codi
$C = \{(000), (111), (101), (010)\} \subseteq \mathbb{F}_2^3$? Solució (p.98)

La **taxa de transmissió és** $\frac{k}{n}$. La **codimensió** és $n - k$.

Exercici 67

Quines serien la taxa de transmissió i la codimensió del codi $C = \{(000), (111), (101), (010)\} \subseteq \mathbb{F}_2^3$?
Solució (p.98)

Matriu generadora i codificació

▸ ***Matriu generadora arbitrària***

Si un codi C és un subespai vectorial de dimensió k, aleshores té una base formada per k vectors.

Podem col·locar els k vectors d'una base de C un damunt de l'altre en forma de matriu. Obtenim el que anomenem una matriu generadora.

> Diem que una matriu G de k files i n columnes és una **matriu generadora** del codi lineal C si les seves files són una base de C.

La matriu generadora no és única. Es poden intercanviar files, per exemple.

> **Exercici 68**
>
> Doneu una matriu generadora del codi
> $C = \{(000), (111), (101), (010)\} \subseteq \mathbb{F}_2^3$.
> Solució (p.98)

> Per **codificar** una paraula de k símbols de $\mathbb{F}_q$, la multipliquem per la matriu generadora.

Exemple. *Podem representar els elements de $\mathbb{Z}_7$ de la següent manera:*

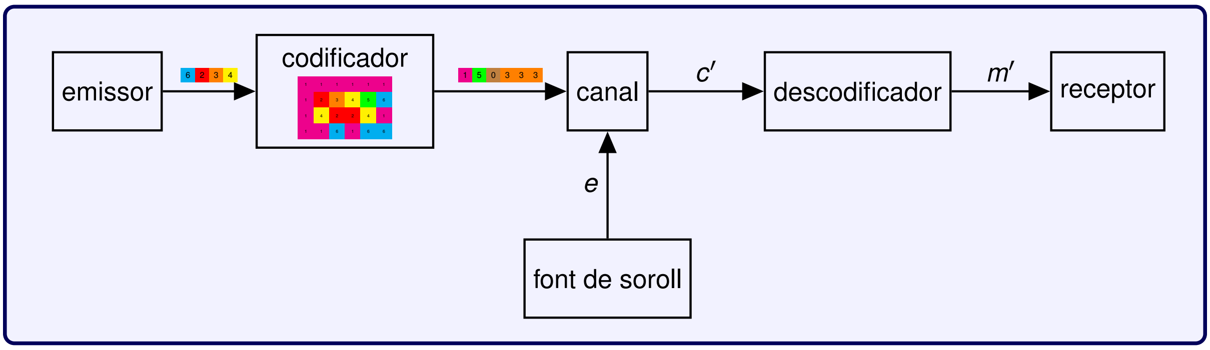
$$\mathbb{Z}_7 = \{ \boxed{0} \ , \ \boxed{1} \ , \ \boxed{2} \ , \ \boxed{3} \ , \ \boxed{4} \ , \ \boxed{5} \ , \ \boxed{6} \}$$

Considerem el codi generat per la matriu

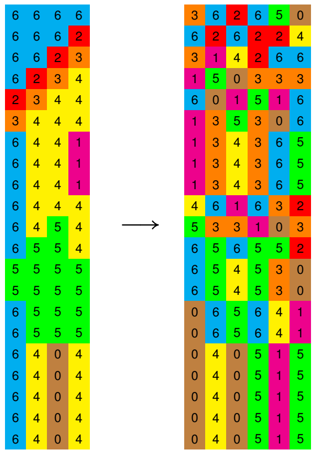
$$G = \begin{array}{|c|c|c|c|c|c|} \hline 1 & 1 & 1 & 1 & 1 & 1 \\ \hline 1 & 2 & 3 & 4 & 5 & 6 \\ \hline 1 & 4 & 2 & 2 & 4 & 1 \\ \hline 1 & 1 & 6 & 1 & 6 & 6 \\ \hline \end{array}$$

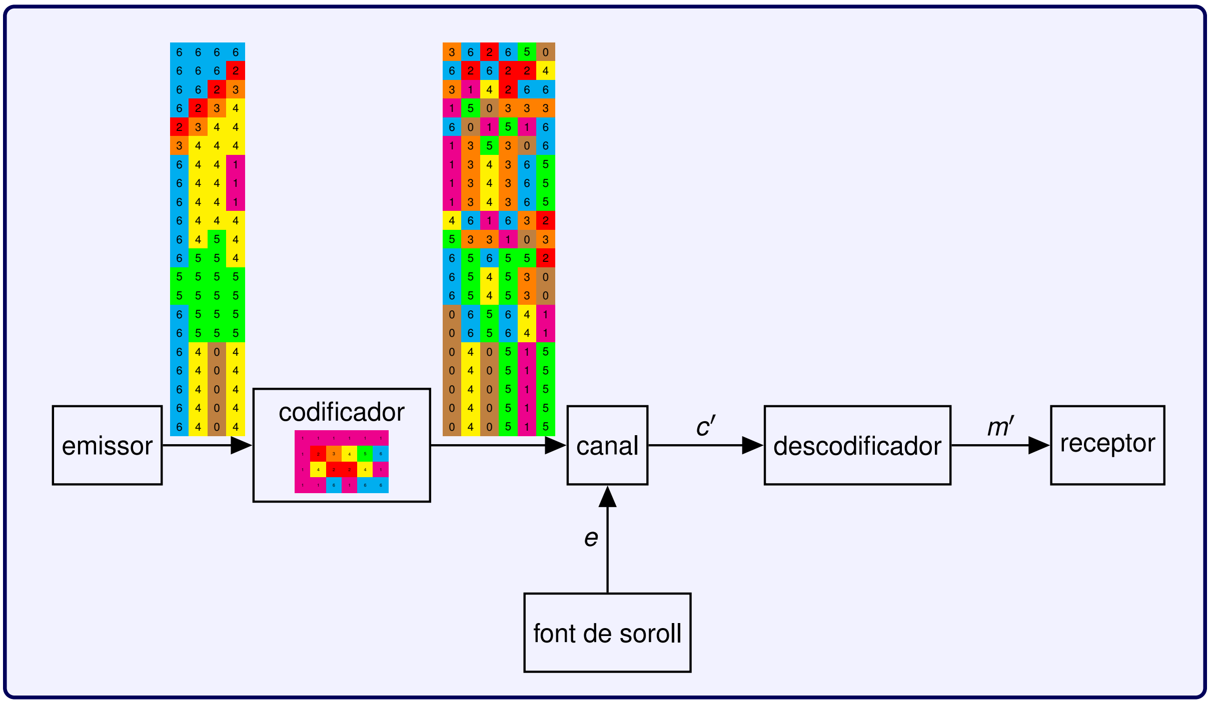
Per codificar una paraula com $\begin{array}{|c|c|c|c|} \hline 6 & 2 & 3 & 4 \\ \hline \end{array}$ *amb la matriu G, la multipliquem per G.*

$$\begin{array}{|c|c|c|c|} \hline 6 & 2 & 3 & 4 \\ \hline \end{array} \cdot \begin{array}{|c|c|c|c|c|c|} \hline 1 & 1 & 1 & 1 & 1 & 1 \\ \hline 1 & 2 & 3 & 4 & 5 & 6 \\ \hline 1 & 4 & 2 & 2 & 4 & 1 \\ \hline 1 & 1 & 6 & 1 & 6 & 6 \\ \hline \end{array} = \begin{array}{|c|c|c|c|c|c|} \hline 1 & 5 & 0 & 3 & 3 & 3 \\ \hline \end{array}$$



Suposem que ara volem codificar la imatge següent. Codificarem cadascuna de les seves files.





Exercici 69

Comproveu que les paraules del codi $C = \{(000), (111), (101), (010)\} \subseteq \mathbb{F}_2^3$ són totes les codificacions possibles amb la matriu

$$G = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}.$$

Solució (p.98)

▸ ***Matriu generadora sistemàtica***

Diem que una matriu generadora és **sistemàtica** en les primeres posicions (o en les darreres) si conté la identitat en les primeres posicions (o en les darreres).

En codificar utilitzant una matriu generadora sistemàtica, la informació es repeteix en aquelles posicions on la matriu és sistemàtica.

Vegeu més sobre l'existència de matrius sistemàtiques (p.105)

Exemple. *Recordem l'exemple de codi sobre $\mathbb{Z}_7$.*

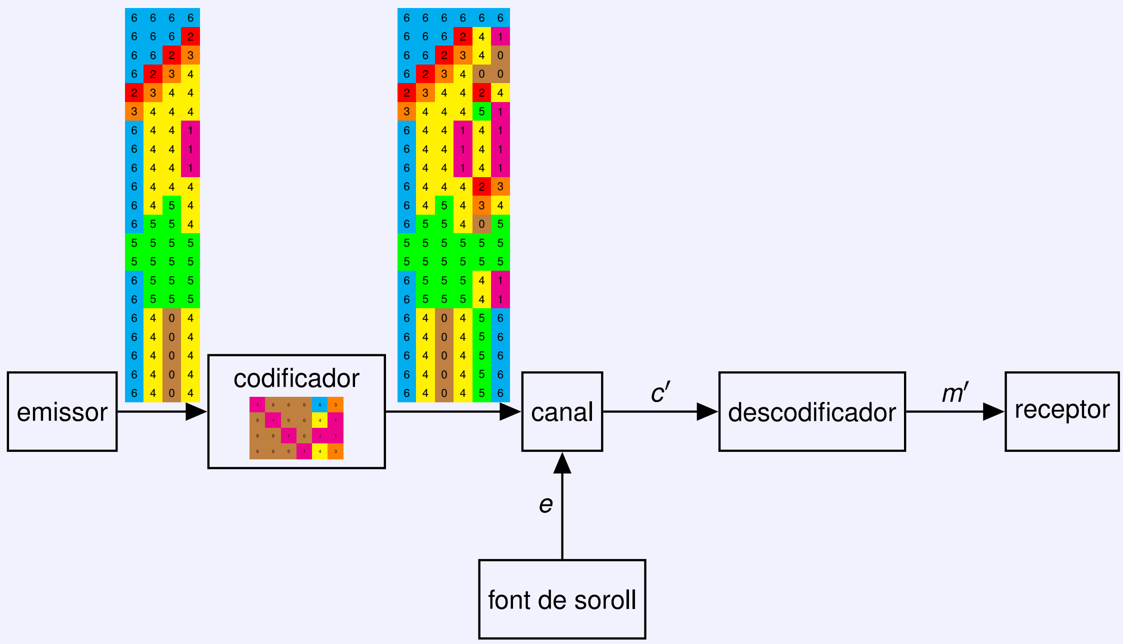
Una alternativa per codificar és fer servir la següent matriu sistemàtica equivalent a G:

$$G_s = \begin{array}{|cccccc|} 1 & 0 & 0 & 0 & 6 & 3 \\ 0 & 1 & 0 & 0 & 4 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 4 & 3 \end{array}$$

Així, codificar una paraula com $\begin{array}{|cccc|} 6 & 2 & 3 & 4 \end{array}$ *serà*

$$\begin{array}{|cccc|} 6 & 2 & 3 & 4 \end{array} \cdot \begin{array}{|cccccc|} 1 & 0 & 0 & 0 & 6 & 3 \\ 0 & 1 & 0 & 0 & 4 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 4 & 3 \end{array} = \begin{array}{|cccccc|} 6 & 2 & 3 & 4 & 0 & 0 \end{array}$$

Ara, en codificar la imatge, què observem?



Més endavant utilitzarem aquest exemple per a la detecció d'errors (p.91) i per a la error correction (p.94).

Exercici 70

Considerem un codi ternari amb matriu generadora

$$\begin{pmatrix} 2 & 2 & 0 & 2 & 1 & 1 \\ 2 & 0 & 1 & 1 & 2 & 2 \\ 1 & 2 & 0 & 2 & 1 & 0 \end{pmatrix}$$

Codifiqueu sistemàticament a l'esquerra la informació

- $(1, 0, 2)$
- $(2, 2, 1)$

Solució (p.98)

Codificació en símbols i en dígits

En un cos finit de p^m elements distingim

- **dígits**: són els elements de $\mathbb{Z}_p$,
- **símbols**: són els elements de $\mathbb{F}_{p^m}$.

Cada símbol es pot representar amb m dígits mitjançant la notació vectorial.

Els dígits de $\mathbb{Z}_2$ també s'anomenen **bits**. Els dígits de $\mathbb{Z}_3$ també s'anomenen **trits**.

Exemple. *Suposem que volem utilitzar un codi sobre $\mathbb{F}_9 = \mathbb{Z}_3/x^2 + 2x + 2$. Si diem α a la classe de x, tenim la taula d'equivalències següent:*

exp.	*vect.*
0	00
α^0	10
α^1	01
α^2	11
α^3	12
α^4	20
α^5	02
α^6	22
α^7	21

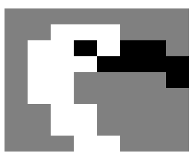
↑ ↑

símbols ***parelles de dígits***

Considerem el codi que té matriu generadora

$$\begin{pmatrix} \alpha^2 & \alpha^3 & 1 & \alpha^6 & 1 & 0 & 0 & 0 \\ \alpha^4 & 1 & \alpha^4 & \alpha^4 & 0 & 1 & 0 & 0 \\ \alpha^2 & \alpha^5 & \alpha^4 & \alpha^3 & 0 & 0 & 1 & 0 \\ \alpha & \alpha^6 & \alpha^4 & \alpha^6 & 0 & 0 & 0 & 1 \end{pmatrix}$$

i suposem que volem codificar la imatge digital següent:



La representem amb dígits de $\mathbb{F}_3 = \mathbb{Z}_3$.

$$\begin{matrix} 1&1&1&1&1&1&1&1\\ 1&1&2&2&2&1&1&1\\ 1&2&2&0&2&0&0&1\\ 1&2&2&2&0&0&0&0\\ 1&2&2&1&1&1&1&0\\ 1&2&2&1&1&1&1&1\\ 1&1&2&2&1&1&1&1\\ 1&1&2&2&1&1&1&1\\ 1&1&1&2&2&1&1&1 \end{matrix}$$

I agrupem cada $m = 2$ dígits per formar un símbol, mitjançant la taula d'equivalències anterior.

$$\begin{matrix} 1&1\\1&1\\1&2\\1&2\\1&2\\1&2\\1&1\\1&1\\1&1 \end{matrix} \quad \begin{matrix} 1&1\\2&2\\2&0\\2&2\\2&1\\2&1\\2&2\\2&2\\1&2 \end{matrix} \quad \begin{matrix} 1&1\\2&1\\2&0\\0&0\\1&1\\1&1\\1&1\\1&1\\2&1 \end{matrix} \quad \begin{matrix} 1&1\\1&1\\0&1\\0&0\\1&0\\1&1\\1&1\\1&1\\1&1 \end{matrix} \quad \leftrightarrow \quad \begin{pmatrix} \alpha^2&\alpha^2&\alpha^2&\alpha^2\\ \alpha^2&\alpha^6&\alpha^7&\alpha^2\\ \alpha^3&\alpha^4&\alpha^4&\alpha\\ \alpha^3&\alpha^6&0&0\\ \alpha^3&\alpha^7&\alpha^2&1\\ \alpha^3&\alpha^7&\alpha^2&\alpha^2\\ \alpha^2&\alpha^6&\alpha^2&\alpha^2\\ \alpha^2&\alpha^3&\alpha^7&\alpha^2 \end{pmatrix}$$

Ara ja podem multiplicar cada fila per la matriu generadora

$$\begin{pmatrix} \alpha^2&\alpha^2&\alpha^2&\alpha^2\\ \alpha^2&\alpha^6&\alpha^7&\alpha^2\\ \alpha^3&\alpha^4&\alpha^4&\alpha\\ \alpha^3&\alpha^6&0&0\\ \alpha^3&\alpha^7&\alpha^2&1\\ \alpha^3&\alpha^7&\alpha^2&\alpha^2\\ \alpha^2&\alpha^6&\alpha^2&\alpha^2\\ \alpha^2&\alpha^3&\alpha^7&\alpha^2 \end{pmatrix} \begin{pmatrix} \alpha^2&\alpha^3&1&\alpha^6&1&0&0&0\\ \alpha^4&1&\alpha^4&\alpha^4&0&1&0&0\\ \alpha^2&\alpha^5&\alpha^4&\alpha^3&0&0&1&0\\ \alpha&\alpha^6&\alpha^4&\alpha^6&0&0&0&1 \end{pmatrix} = \begin{pmatrix} \alpha^2&\alpha^2&\alpha^2&\alpha^2&\alpha^2&\alpha^2&\alpha^2&\alpha^2\\ \alpha^2&\alpha^7&\alpha^4&\alpha^3&\alpha^2&\alpha^6&\alpha^7&\alpha^2\\ \alpha^3&\alpha&\alpha&\alpha^4&\alpha^3&\alpha^4&\alpha^4&\alpha\\ 1&\alpha^2&\alpha^4&\alpha^3&\alpha^3&\alpha^6&0&0\\ \alpha^5&\alpha^4&0&\alpha&\alpha^3&\alpha^7&\alpha^2&1\\ 1&\alpha^2&\alpha^5&\alpha^6&\alpha^3&\alpha^7&\alpha^2&\alpha^2\\ 0&\alpha^6&0&0&\alpha^2&\alpha^6&\alpha^2&\alpha^2\\ \alpha^7&\alpha^2&0&\alpha^6&\alpha^2&\alpha^3&\alpha^7&\alpha^2 \end{pmatrix}$$

I ara podem tornar a convertir cada símbol en la parella de dígits que li correspon i obtenim la imatge codificada.

$$\begin{pmatrix} \alpha^2&\alpha^2&\alpha^2&\alpha^2&\alpha^2&\alpha^2&\alpha^2&\alpha^2\\ \alpha^2&\alpha^7&\alpha^4&\alpha^3&\alpha^2&\alpha^6&\alpha^7&\alpha^2\\ \alpha^3&\alpha&\alpha&\alpha^4&\alpha^3&\alpha^4&\alpha^4&\alpha\\ 1&\alpha^2&\alpha^4&\alpha^3&\alpha^3&\alpha^6&0&0\\ \alpha^5&\alpha^4&0&\alpha&\alpha^3&\alpha^7&\alpha^2&1\\ 1&\alpha^2&\alpha^5&\alpha^6&\alpha^3&\alpha^7&\alpha^2&\alpha^2\\ 0&\alpha^6&0&0&\alpha^2&\alpha^6&\alpha^2&\alpha^2\\ \alpha^7&\alpha^2&0&\alpha^6&\alpha^2&\alpha^3&\alpha^7&\alpha^2 \end{pmatrix} \to \begin{matrix} 1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1\\ 1&1&2&1&2&0&1&2&1&1&2&2&2&1&1&1\\ 1&2&0&1&0&1&2&0&1&2&2&0&2&0&0&1\\ 1&0&1&1&2&0&1&2&1&2&2&2&0&0&0&0\\ 0&2&2&0&0&0&0&1&1&2&2&1&1&1&1&0\\ 1&0&1&1&0&2&2&2&1&2&2&1&1&1&1&1\\ 0&0&2&2&0&0&0&0&1&1&2&2&1&1&1&1\\ 0&0&2&2&0&0&0&0&1&1&2&2&1&1&1&1\\ 2&1&1&1&0&0&2&2&1&1&1&2&2&1&1&1 \end{matrix}$$

Codi dual i matriu de control

El **codi dual** (o ortogonal) de C és

$$C^{\perp} = \{v \in \mathbb{F}_q^n : v \cdot c = 0 \text{ per a tot } c \in C\}.$$

El codi dual d'un codi és, per tant, el complement ortogonal (p.106) del codi.

És un codi lineal de la mateixa longitud que C i de dimensió $n - k$.

Es pot definir a partir d'un sistema d'equacions lineals amb matriu de coeficients G.

Exemple. *El codi ternari amb matriu generadora*

$$\begin{pmatrix} 2 & 2 & 0 & 2 & 1 & 1 \\ 2 & 0 & 1 & 1 & 2 & 2 \\ 1 & 2 & 0 & 2 & 1 & 0 \end{pmatrix}$$

té com a codi dual el conjunt de vectors $(x_1, \ldots, x_6)$ *que són solucions de*

$$\begin{array}{cccccccc} 2x_1 & +2x_2 & & +2x_4 & +x_5 & +x_6 & = 0 \\ 2x_1 & & +x_3 & +x_4 & +2x_5 & +2x_6 & = 0 \\ x_1 & +2x_2 & & +2x_4 & +x_5 & & = 0 \end{array}$$

Una matriu H generadora de $C^{\perp}$ es diu que és una **matriu de control** de C.

Equivalentment, una matriu de control de C és una matriu tal que el codi C es pot redefinir com

$$C = \{c \in \mathbb{F}_q^n : c \cdot h = 0 \text{ per a tota fila } h \text{ de } H\}.$$

Si una matriu generadora és de la forma

$$G = (I|P),$$

aleshores una matriu de control és

$$H = (-P^T|I).$$

I si una matriu generadora és de la forma

$$G = (P|I),$$

aleshores una matriu de control és

$$H = (I| - P^T).$$

Anàlogament, si una matriu de control és $H = (I|P)$, aleshores una matriu generadora és $G = (-P^T|I)$ i, si una matriu de control és $H = (P|I)$, aleshores una matriu generadora és $G = (I| - P^T)$.

Vegeu una justificació de l'àlgebra lineal (p.105)

Exercici 71

Considerem el codi ternari de l'Exercici 70 amb matriu generadora

$$\begin{pmatrix} 2 & 2 & 0 & 2 & 1 & 1 \\ 2 & 0 & 1 & 1 & 2 & 2 \\ 1 & 2 & 0 & 2 & 1 & 0 \end{pmatrix}$$

Doneu-ne una matriu de control.

Solució (p.99)

Exercici 72

Considerem el codi $C = \{(000), (111), (101), (010)\} \subseteq \mathbb{F}_2^3$.

1. Doneu una matriu de control de C.
2. Comproveu que totes les paraules del codi, quan les multipliquem per la matriu de control, donen 0.
3. Doneu el codi dual $C^{\perp}$.
4. Comproveu que les paraules del codi dual, quan les multipliquem per la matriu G, donen 0.

Solució (p.99)

4.3 Detecció i correcció d'errors

Distància de Hamming i pes

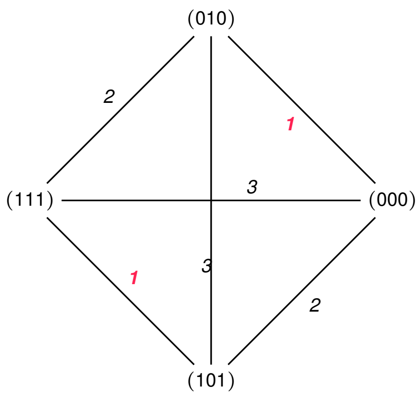
La **distància de Hamming** entre dues paraules de la mateixa longitud és el nombre de posicions on difereixen.
Anomenem $d_H(u, v)$ a la distància de Hamming entre les paraules u i v.

Exemple.

$$\begin{aligned} d_H(CERT, CART) &= 1 \\ d_H(FALS, CART) &= 3 \\ d_H(CERT, CALT) &= 2 \\ d_H(FALS, CALT) &= 2 \end{aligned}$$

En un codi ens interessarà considerar la distància de Hamming entre cada parella de paraules i determinar la mínima d'aquestes distàncies.

Exemple. *Les distàncies entre les paraules del codi* $C = \{(000), (111), (101), (010)\}$ *són les següents:*



El **pes** d'una paraula és el nombre de posicions no nul·les.
Anomenem $w(u)$ al pes de u.

Exemple. *Els pesos de les paraules del codi anterior són:*

$$\begin{aligned} w(000) &= 0 \\ w(010) &= 1 \\ w(101) &= 2 \\ w(111) &= 3 \end{aligned}$$

Si $u, v \in \mathbb{F}_q^n$ i diem $\vec{0}$ al vector nul de $\mathbb{F}_q^n$, aleshores,

- $d(u, \vec{0}) = w(u)$,
- $d(u, v) = d(u - v, \vec{0}) = w(u - v)$.

Distància mínima i capacitat correctora

La **distància mínima** d'un codi lineal C es pot definir indistintament com

- La mínima distància de Hamming entre dues paraules de C.
- El mínim pes de les paraules no nul·les de C.
- El mínim nombre de columnes linealment dependents de H.

Exemple. *Volem determinar la distància mínima del codi C de $\mathbb{Z}_5^5$ que té matriu de control*

$$H = \begin{pmatrix} 3 & 1 & 3 & 2 & 1 \\ 4 & 1 & 0 & 4 & 1 \\ 3 & 2 & 2 & 0 & 3 \end{pmatrix}.$$

- *Perquè d fos 1 caldria que hi hagués una columna linealment dependent a H. Una sola columna és linealment dependent si i només si és nul·la. Com que no hi ha cap columna nul·la descartem $d = 1$.*
- *Perquè d fos 2 caldria que hi hagués dues columnes linealment dependents a H. Dues columnes són linealment dependents si una és un múltiple de l'altra. Com que això no es dona per cap parella de columnes, descartem $d = 2$.*
- *Perquè d fos 3 caldria que hi hagués tres columnes linealment dependents a H. Tres columnes són linealment dependents si una és una combinació lineal de les altres dues. Observem, per exemple, que la tercera columna és la suma de la segona i la quarta. Deduïm que $d = 3$.*

La **fita de Singleton** estableix que, en un codi de longitud n i distància mínima d, la dimensió k satisfà

$$k \leq n - d + 1.$$

Exercici 73

Considerem el codi $C = \{(000), (111), (101), (010)\} \subseteq \mathbb{F}_2^3$.

1. Quina és la seva distància mínima?

2. Verifiqueu la fita de Singleton pel codi C.

Solució (p.100)

Utilitzant un codi de distància mínima d, es podran

- detectar $d - 1$ errors,

- corregir $d-1$ esborralls,
- corregir $\lfloor \frac{d-1}{2} \rfloor$ errors.

La **capacitat correctora** d'un codi de distància mínima d és

$$\left\lfloor \frac{d-1}{2} \right\rfloor$$

Detecció d'errors

Suposem que rebem una paraula u i volem verificar si és del codi ($u \in C$) o, en cas contrari, **detectar** que conté **errors** ($u \notin C$).

Anomenem **síndrome** de u respecte d'una matriu de control H de C al resultat del producte $H \cdot u$.

Observem que la síndrome depèn de la matriu de control emprada.

Una paraula c és de C si i només si la seva síndrome és zero.

Tot i que la síndrome depèn de la matriu de control emprada, si per a alguna matriu de control H es compleix $H \cdot u = 0$, aleshores es complirà per a totes les matrius de control.

Si la síndrome de u és nul·la, deduïm que $u \in C$.
Si no, aleshores **detectem error**.

Exemple. *A $\mathbb{Z}_5$ considerem el codi C que té matriu de control*

$$\begin{pmatrix} 3 & 1 & 3 & 2 & 1 \\ 4 & 1 & 0 & 4 & 1 \\ 3 & 2 & 2 & 0 & 3 \end{pmatrix}$$

Volem detectar si en les paraules (11111) *i* (01234) *hi ha errors.*

Multipliquem les paraules per la matriu H.

$$\begin{pmatrix} 3 & 1 & 3 & 2 & 1 \\ 4 & 1 & 0 & 4 & 1 \\ 3 & 2 & 2 & 0 & 3 \end{pmatrix} \begin{pmatrix} 1 \\ 1 \\ 1 \\ 1 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix} \Longrightarrow \textit{paraula de C}$$

$$\begin{pmatrix} 3 & 1 & 3 & 2 & 1 \\ 4 & 1 & 0 & 4 & 1 \\ 3 & 2 & 2 & 0 & 3 \end{pmatrix} \begin{pmatrix} 0 \\ 1 \\ 2 \\ 3 \\ 4 \end{pmatrix} = \begin{pmatrix} 2 \\ 2 \\ 3 \end{pmatrix} \neq \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix} \Longrightarrow \textit{error detectat}$$

Exemple. *Una martriu de control del codi que havíem vist és*

$$H = \begin{matrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 4 & 2 & 2 & 4 & 1 \end{matrix}$$

Suposem que se'ns embruta la imatge codificada:

$$
\begin{matrix}
6&6&6&6&6&6\\
6&6&6&2&4&1\\
6&6&2&3&4&0\\
6&2&3&4&0&0\\
2&3&4&4&2&4\\
3&4&4&4&5&1\\
6&4&4&1&4&1\\
6&4&4&1&4&1\\
6&4&4&1&4&1\\
6&4&4&4&2&3\\
6&4&5&4&3&4\\
6&5&5&4&0&5\\
5&5&5&5&5&5\\
5&5&5&5&5&5\\
6&5&5&5&4&1\\
6&5&5&5&4&1\\
6&4&0&4&5&6\\
6&4&0&4&5&6\\
6&4&0&4&5&6\\
6&4&0&4&5&6\\
6&4&0&4&5&6
\end{matrix}
\quad\rightarrow\quad
\begin{matrix}
6&6&6&6&6&6\\
6&6&6&2&4&1\\
6&6&2&3&4&0\\
6&2&3&4&0&0\\
2&3&4&4&2&4\\
3&4&4&4&5&1\\
6&4&4&1&4&1\\
6&4&4&1&4&1\\
6&4&4&1&4&1\\
2&4&4&4&2&3\\
6&2&5&4&3&4\\
6&5&2&4&0&5\\
5&5&5&5&5&5\\
5&5&5&5&5&5\\
6&5&5&5&4&1\\
6&5&5&5&4&1\\
6&4&0&4&5&6\\
6&4&0&4&5&6\\
6&4&0&4&5&6\\
6&4&0&4&5&6\\
6&4&0&4&5&6
\end{matrix}
$$

Per identificar on s'han produït els errors, multiplicarem cada fila per H^T (transposem H, ja que uH^T és una transposició de Hu).

$$
\begin{matrix}
6&6&6&6&6&6\\
6&6&6&2&4&1\\
6&6&2&3&4&0\\
6&2&3&4&0&0\\
2&3&4&4&2&4\\
3&4&4&4&5&1\\
6&4&4&1&4&1\\
6&4&4&1&4&1\\
6&4&4&1&4&1\\
2&4&4&4&2&3\\
6&2&5&4&3&4\\
6&5&2&4&0&5\\
5&5&5&5&5&5\\
5&5&5&5&5&5\\
6&5&5&5&4&1\\
6&5&5&5&4&1\\
6&4&0&4&5&6\\
6&4&0&4&5&6\\
6&4&0&4&5&6\\
6&4&0&4&5&6\\
6&4&0&4&5&6
\end{matrix}
\quad
\begin{matrix}
1&1\\
2&4\\
3&2\\
4&2\\
5&4\\
6&1
\end{matrix}
\quad\longrightarrow\quad
\begin{matrix}
0&0\\
0&0\\
0&0\\
0&0\\
0&0\\
0&0\\
0&0\\
0&0\\
0&0\\
3&3\\
3&6\\
5&1\\
0&0\\
0&0\\
0&0\\
0&0\\
0&0\\
0&0\\
0&0\\
0&0\\
0&0
\end{matrix}
$$

Allà on el resultat és diferent de zero és on hi ha errors.

Exercici 74

1. Doneu justificadament un polinomi en x que generi $\mathbb{F}_4$.
2. Doneu una taula exponencial-vectorial de $\mathbb{F}_4$.
3. Anomenem α a la classe de x dins de $\mathbb{F}_4$. Considerem el codi C amb matriu generadora

$$G = \begin{pmatrix} 1 & \alpha & \alpha & 1 \\ 0 & \alpha^2 & 0 & \alpha^2 \end{pmatrix}.$$

   Codifiqueu la cadena de bits 011001001111 i doneu el resultat també en bits.
4. Doneu una matriu de control del codi.
5. Quina és la distància mínima del codi C?
6. Quants errors es poden corregir en cada paraula rebuda? I quants esborralls? Quants errors es poden detectar?
7. Detecteu si hi ha errors en la cadena codificada de bits

$$0111110100110010000000000.$$

Solució (p.100)

Correcció d'esborralls

Suposem que rebem una paraula on s'han esborrat alguns dels símbols i s'han convertit en **esborralls**.

Considerant els esborralls com a incògnites, a partir de

$$H \cdot u = 0$$

obtenim un sitema lineal d'equacions.
Si el nombre d'esborralls és com a màxim $d-1$, aleshores el sistema és compatible i determinat.
La substitució de les incògnites per la solució del sistema ens dona la **correcció d'esborralls**.

Exemple. *A $\mathbb{Z}_5$ considerem el codi C que té matriu de control*

$$\begin{pmatrix} 3 & 1 & 3 & 2 & 1 \\ 4 & 1 & 0 & 4 & 1 \\ 3 & 2 & 2 & 0 & 3 \end{pmatrix}$$

Volem corregir els esborralls de la paraula $(324??)$ *i donar-ne la paraula corregida.*

Substiuïm els esborralls per incògnites: $(324xy)$ *i resolem el sistema*

$$\begin{pmatrix} 3 & 1 & 3 & 2 & 1 \\ 4 & 1 & 0 & 4 & 1 \\ 3 & 2 & 2 & 0 & 3 \end{pmatrix} \begin{pmatrix} 3 \\ 2 \\ 4 \\ x \\ y \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}$$

equivalent a

$$\begin{array}{rcll} 3+2x+y & = & 0 & \qquad\qquad \Longrightarrow \; 2x+1=0 \; \Longrightarrow \; x=2 \\ 4+4x+y & = & 0 & \\ 1+3y & = & 0 & \Longrightarrow \; y=3 \end{array}$$

que té solució $x = 2$ i $y = 3$. Per tant, la paraula corregida és (32423).

Exercici 75

1. Comproveu que el polinomi $x^2 + 2x + 2$ és irreductible i primitiu a $\mathbb{Z}_3[x]$.
2. Doneu una taula exponencial-vectorial de $\mathbb{Z}_3[x]/x^2 + 2x + 2$, utilitzant $\alpha = [x]$.
3. Considerem el codi C amb matriu generadora
$$G = \begin{pmatrix} 1 & \alpha & \alpha^2 & \alpha^3 \\ 0 & \alpha^4 & 0 & 1 \end{pmatrix}.$$
Codifiqueu la cadena de trits 01211022. Doneu el resultat també com a cadena de trits.
4. Doneu una matriu de control del codi.
5. Quina és la distància mínima de C?
6. Quants errors es poden corregir en cada paraula rebuda? I quants esborralls? Quants errors es poden detectar?
7. Corregiu els esborralls de la cadena de trits 0112??22. Doneu el resultat en trits.

Solució (p.101)

Correcció d'errors

Ara suposem que s'ha enviat una paraula de codi $c \in C$, que eventualment s'han produït errors i s'ha convertit en u.

Anomenem $e = u - c$. Suposarem que s'han produït pocs errors i que, per tant, e és nul gairebé en totes les coordenades excepte en unes poques.

Diem que c és la **paraula codi**, u és la **paraula rebuda** i e és el **vector d'errors**.

Si $e = (0, \dots, 0, e_{i_1}, 0, \dots, 0, e_{i_2}, 0, \dots, 0, \dots, e_{i_t})$ amb $e_{i_1}, e_{i_2}, \dots, e_{i_t} \neq 0$, aleshores diem que $i_1, i_2, \dots, i_t$ són les **posicions d'error**, mentre que $e_{i_1}, \dots, e_{i_t}$ són els **valors dels errors**.

Per corregir errors utilitzarem que la **síndrome** de la paraula rebuda satisfà
$$H \cdot u = H \cdot e$$

Anomenarem $s = H \cdot u$.

Per corregir 1 **error:**

Si només es produeix un error, aleshores

- $e = (0, \dots, 0, e_i, 0, \dots, 0)$,
- $s = H \cdot u = h_i e_i$, on h_i és la columna i-èssima de H.

Aleshores

- buscant quina columna de H és un múltiple de s, tindrem la **posició d'error**,
- buscant l'únic valor e_i tal que $s = h_i e_i$, tindrem el **valor de l'error**.

Exemple. *Continuem amb el codi que havíem vist.*

$$\begin{pmatrix}
6&6&6&6&6&6\\
6&6&6&2&4&1\\
6&6&2&3&4&0\\
6&2&3&4&0&0\\
2&3&4&4&2&4\\
3&4&4&4&5&1\\
6&4&4&1&4&1\\
6&4&4&1&4&1\\
6&4&4&1&4&1\\
2&4&4&4&2&3\\
6&2&5&4&3&4\\
6&5&2&4&0&5\\
5&5&5&5&5&5\\
5&5&5&5&5&5\\
6&5&5&5&4&1\\
6&5&5&5&4&1\\
6&4&0&4&5&6\\
6&4&0&4&5&6\\
6&4&0&4&5&6\\
6&4&0&4&5&6\\
6&4&0&4&5&6
\end{pmatrix}
\rightarrow
\begin{pmatrix}
0&0\\0&0\\0&0\\0&0\\0&0\\0&0\\0&0\\0&0\\0&0\\3&3\\3&6\\5&1\\0&0\\0&0\\0&0\\0&0\\0&0\\0&0\\0&0\\0&0\\0&0
\end{pmatrix}$$

Havíem calculat les síndromes.

Per trobar el valor dels errors, vegem que les síndromes són múltiples de columnes de H:

$$\begin{pmatrix}
0&0\\0&0\\0&0\\0&0\\0&0\\0&0\\0&0\\0&0\\0&0\\3&3\\3&6\\5&1\\0&0\\0&0\\0&0\\0&0\\0&0\\0&0\\0&0\\0&0\\0&0
\end{pmatrix}
\rightarrow
\begin{array}{l}
\begin{pmatrix}3&3\end{pmatrix} = \begin{pmatrix}3&0&0&0&0&0\end{pmatrix}\begin{pmatrix}1&1\\2&4\\3&2\\4&2\\5&4\\6&1\end{pmatrix}\\[2ex]
\begin{pmatrix}3&6\end{pmatrix} = \begin{pmatrix}0&5&0&0&0&0\end{pmatrix}\begin{pmatrix}1&1\\2&4\\3&2\\4&2\\5&4\\6&1\end{pmatrix}\\[2ex]
\begin{pmatrix}5&1\end{pmatrix} = \begin{pmatrix}0&0&4&0&0&0\end{pmatrix}\begin{pmatrix}1&1\\2&4\\3&2\\4&2\\5&4\\6&1\end{pmatrix}
\end{array}$$

Deduïm que les paraules d'error són $\begin{pmatrix}3&0&0&0&0&0\end{pmatrix}$ $\begin{pmatrix}0&5&0&0&0&0\end{pmatrix}$ $\begin{pmatrix}0&0&4&0&0&0\end{pmatrix}$

Restem les paraules d'error de les paraules rebudes

$$\begin{pmatrix}
6&6&6&6&6&6\\
6&6&6&2&4&1\\
6&6&2&3&4&0\\
6&2&3&4&0&0\\
2&3&4&4&2&4\\
3&4&4&4&5&1\\
6&4&4&1&4&1\\
6&4&4&1&4&1\\
6&4&4&1&4&1\\
2&4&4&4&2&3\\
6&2&5&4&3&4\\
6&5&2&4&0&5\\
5&5&5&5&5&5\\
5&5&5&5&5&5\\
6&5&5&5&4&1\\
6&5&5&5&4&1\\
6&4&0&4&5&6\\
6&4&0&4&5&6\\
6&4&0&4&5&6\\
6&4&0&4&5&6\\
6&4&0&4&5&6
\end{pmatrix}
-
\begin{pmatrix}
0&0&0&0&0&0\\
0&0&0&0&0&0\\
0&0&0&0&0&0\\
0&0&0&0&0&0\\
0&0&0&0&0&0\\
0&0&0&0&0&0\\
0&0&0&0&0&0\\
0&0&0&0&0&0\\
0&0&0&0&0&0\\
3&0&0&0&0&0\\
0&5&0&0&0&0\\
0&0&4&0&0&0\\
0&0&0&0&0&0\\
0&0&0&0&0&0\\
0&0&0&0&0&0\\
0&0&0&0&0&0\\
0&0&0&0&0&0\\
0&0&0&0&0&0\\
0&0&0&0&0&0\\
0&0&0&0&0&0\\
0&0&0&0&0&0
\end{pmatrix}
=
\begin{pmatrix}
6&6&6&6&6&6\\
6&6&6&2&4&1\\
6&6&2&3&4&0\\
6&2&3&4&0&0\\
2&3&4&4&2&4\\
3&4&4&4&5&1\\
6&4&4&1&4&1\\
6&4&4&1&4&1\\
6&4&4&1&4&1\\
6&4&4&4&2&3\\
6&4&5&4&3&4\\
6&5&5&4&0&5\\
5&5&5&5&5&5\\
5&5&5&5&5&5\\
6&5&5&5&4&1\\
6&5&5&5&4&1\\
6&4&0&4&5&6\\
6&4&0&4&5&6\\
6&4&0&4&5&6\\
6&4&0&4&5&6\\
6&4&0&4&5&6
\end{pmatrix}
\rightarrow
\begin{pmatrix}
6&6&6&6\\
6&6&6&2\\
6&6&2&3\\
6&2&3&4\\
2&3&4&4\\
3&4&4&4\\
6&4&4&1\\
6&4&4&1\\
6&4&4&1\\
6&4&4&4\\
6&4&5&4\\
6&5&5&4\\
5&5&5&5\\
5&5&5&5\\
6&5&5&5\\
6&5&5&5\\
6&4&0&4\\
6&4&0&4\\
6&4&0&4\\
6&4&0&4\\
6&4&0&4
\end{pmatrix}$$

I descodifiquem per la part sistemàtica.

Exercici 76

Utilitzem el codi dels Exercicis 70 i 71.
Useu la síndrome per descodificar el vector rebut 212121.
Solució (p.102)

Cas general:

La descodificació per **màxima versemblança** consisteix a descodificar u per $u - e'$, on e' és un vector de $\mathbb{F}_q^n$ amb mínim pes d'entre els que tenen la mateixa síndrome que u.

Per fer-ho busquem una combinació lineal mínima de columnes de H que sigui igual a la síndrome. És a dir, si la representació d'H en columnes és $(h_1, h_2, \dots, h_n)$, busquem una combinació $\alpha_{i_1} h_{i_1} + \cdots + \alpha_{i_r} h_{i_r}$ que utilitzi el mínim possible de columnes d'H i que sigui igual a la síndrome $H \cdot u$. Aleshores prenem $e' = (0, \dots, 0, \alpha_{i_1}^{(i_1}, 0, \dots 0, \alpha_{i_r}^{(i_r}, 0, \dots, 0)$.

La descodificació és única si el nombre d'errors és, com a màxim, la capacitat correctora.

Exemple. *Codi de repetició 3:*

1. *Quan rebem la seqüència* 001*, sabem que hi ha hagut algun error. Podríem pensar que la paraula era* 000 *i s'ha produït l'error* 001*, o que la paraula era* 111 *i l'error ha estat el* 110.
2. *La probabilitat d'error del canal p_c ens informa de la probabilitat que un bit canviï en ser transmès per un canal determinat.*
3. *La probabilitat que l'error sigui* 001 *és $(1 - p_c)^2 p_c$, mentre que la probabilitat que l'error sigui* 110 *és $(1 - p_c)p_c^2$.*
4. *Si $p_c = 0.01$, $(1 - p_c)^2 p_c = 0.0098$, i $(1 - p_c)p_c^2 = 0.000099$.*
5. *Si $p_c < 1/2$, el primer cas és més probable que el segon.*

Sota el principi de màxima versemblança, sempre assumirem que la paraula enviada ha estat la que correspon al cas més probable.

Exercici 77

Utilitzem el codi dels Exercicis 70 i 71.
Useu la síndrome per corregir els vectors rebuts

1. 120102, Solució (p.103)
2. 222222. Solució (p.103)

Exercici 78

Considerem el codi C definit sobre $\mathbb{F}_5$ format per les solucions del sistema

$$\begin{aligned} x_1 + 3x_2 + 2x_4 + 4x_5 &= 0 \\ x_2 + 3x_3 + x_4 + x_5 &= 0 \end{aligned}$$

1. Quina és la seva dimensió?
2. Quina és la seva distància mínima?
3. Corregiu el missatge 1132321231.

Solució (p.103)

Exercici 79

Sigui C el codi sobre $\mathbb{F}_2$ amb matriu generadora

$$\begin{pmatrix} 1 & 1 & 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 & 0 & 1 \end{pmatrix}$$

1. Calculeu una matriu de control de C.
2. Quins són els paràmetres d'aquest codi?
3. Quants errors corregeix?
4. Calculeu la síndrome de $v = (00111101)$.
5. Corregiu v.
6. Si hem emprat G per codificar, quina era la paraula transmesa?
7. Quin era el missatge enviat?

Solució (p.103)

Procés de codificació-descodificació

$$s \in \mathbb{F}_p^{k\cdot m} \xrightarrow{\text{dígits a símbols}} \underset{(q = p^m)}{i \in \mathbb{F}_q^k} \xrightarrow{\text{codificació}} \underset{(c = i \cdot G)}{c \in C} \xrightarrow{\text{possible pertorbació}} \underset{(y = c + e)}{y \in \mathbb{F}_q^n} \xrightarrow{\text{correcció d'errors}} c' \in C \xrightarrow{\text{descodificació}} i' \in \mathbb{F}_q^k \xrightarrow{\text{símbols a dígits}} s' \in \mathbb{F}_p^{k\cdot m}$$

(i' obtingut de les posicions sistemàtiques si G és sistemàtica)

$$\ell \in \mathbb{F}_p^{k\cdot m} \rightarrow \underset{(q = p^m)}{i \in \mathbb{F}_q^k} \xrightarrow{\text{codificar}} \underset{(c = i \cdot G)}{c \in C} \rightarrow \underset{(u = c + e)}{u \in \mathbb{F}_q^n} \xrightarrow{\text{descodificar}} c' \in C \rightarrow i' \in \mathbb{F}_q^k \rightarrow \ell' \in \mathbb{F}_p^{k\cdot m}$$

(i' obtingut de les posicions sistemàtiques si G és sistemàtica)

4.4 Solucions

Solució de l'Exercici 64

Com que C és un subespai de $\mathbb{F}_2^3$, els escalars són únicament 0 i 1. Així els vectors de C multiplicats per escalars són o bé el vector nul o bé els mateixos vectors.

Queda comprovar que les sumes de dos vectors de C són vectors de C. I, en efecte,

$$\begin{array}{ccccccc}
(000) & + & (000) & = & (000) & \in & C \\
(000) & + & (111) & = & (111) & \in & C \\
(000) & + & (101) & = & (101) & \in & C \\
(000) & + & (010) & = & (010) & \in & C \\
(111) & + & (111) & = & (000) & \in & C \\
(111) & + & (101) & = & (010) & \in & C \\
(111) & + & (010) & = & (101) & \in & C \\
(101) & + & (101) & = & (000) & \in & C \\
(101) & + & (010) & = & (111) & \in & C \\
(010) & + & (010) & = & (000) & \in & C
\end{array}$$

Torna a l'exercici (p.82)

Solució de l'Exercici 65

Es tracta d'un codi binari.

Torna a l'exercici (p.82)

Solució de l'Exercici 66

$k = 2$

Torna a l'exercici (p.82)

Solució de l'Exercici 67

$\frac{k}{n} = 0.666$, $n - k = 1$

Torna a l'exercici (p.82)

Solució de l'Exercici 68

Per exemple,

$$G = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix},$$

però també $\begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 1 & 1 \\ 1 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 1 \end{pmatrix} \dots$

Torna a l'exercici (p.83)

Solució de l'Exercici 69

Vegem com la matriu G genera tot C:

$$\begin{array}{ll}
\begin{pmatrix} 0 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix} & = \begin{pmatrix} 0 & 0 & 0 \end{pmatrix} \\
\begin{pmatrix} 1 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix} & = \begin{pmatrix} 1 & 1 & 1 \end{pmatrix} \\
\begin{pmatrix} 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix} & = \begin{pmatrix} 1 & 0 & 1 \end{pmatrix} \\
\begin{pmatrix} 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix} & = \begin{pmatrix} 0 & 1 & 0 \end{pmatrix}
\end{array}$$

Torna a l'exercici (p.84)

Solució de l'Exercici 70

Busquem la matriu equivalent sistemàtica per l'esquerra:

$$\begin{pmatrix} 2 & 2 & 0 & 2 & 1 & 1 \\ 2 & 0 & 1 & 1 & 2 & 2 \\ 1 & 2 & 0 & 2 & 1 & 0 \end{pmatrix} \sim_{\substack{f_1' = 2f_1 \\ f_2' = 2f_1 + f_2 \\ f_3' = f_1 + f_3}} \begin{pmatrix} 1 & 1 & 0 & 1 & 2 & 2 \\ 0 & 1 & 1 & 2 & 1 & 1 \\ 0 & 1 & 0 & 1 & 2 & 1 \end{pmatrix} \sim_{\substack{f_1' = f_1 + 2f_2 \\ f_3' = 2f_2 + f_3}} \begin{pmatrix} 1 & 0 & 2 & 2 & 1 & 1 \\ 0 & 1 & 1 & 2 & 1 & 1 \\ 0 & 0 & 2 & 2 & 1 & 0 \end{pmatrix} \sim_{\substack{f_1' = f_1 + 2f_3 \\ f_2' = f_2 + f_3 \\ f_3' = 2f_3}}$$

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 2 & 1 \\ 0 & 0 & 1 & 1 & 2 & 0 \end{pmatrix}$$

La codificació demanada és

$$\begin{pmatrix} 1 & 0 & 2 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 2 & 1 \\ 0 & 0 & 1 & 1 & 2 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 2 & 2 & 1 & 1 \end{pmatrix}$$

$$\begin{pmatrix} 2 & 2 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 2 & 1 \\ 0 & 0 & 1 & 1 & 2 & 0 \end{pmatrix} = \begin{pmatrix} 2 & 2 & 1 & 0 & 0 & 1 \end{pmatrix}$$

Torna a l'exercici (p.86)

Solució de l'Exercici 71

En la resolució de l'Exercici 70 (p.98) hem vist que la matriu generadora donada és equivalent a la matriu sistemàtica

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 2 & 1 \\ 0 & 0 & 1 & 1 & 2 & 0 \end{pmatrix}$$

que és de la forma $(I|P)$ amb

$$I = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \text{ i } P = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 2 & 1 \\ 1 & 2 & 0 \end{pmatrix}$$

Ara tindrem $P^T = \begin{pmatrix} 0 & 1 & 1 \\ 0 & 2 & 2 \\ 1 & 1 & 0 \end{pmatrix}$ i $-P^T = \begin{pmatrix} 0 & 2 & 2 \\ 0 & 1 & 1 \\ 2 & 2 & 0 \end{pmatrix}$

Una matriu de control serà, doncs,

$$H = \begin{pmatrix} 0 & 2 & 2 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 \\ 2 & 2 & 0 & 0 & 0 & 1 \end{pmatrix}$$

Torna a l'exercici (p.88)

Solució de l'Exercici 72

1. Com que la matriu generadora

   $$G = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}$$

   té la forma $(I|P)$, podem construir H com $(-P^T|I)$.

   En aquest cas $P = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$, per tant, $P^T = \begin{pmatrix} 1 & 0 \end{pmatrix}$, que és igual a $-P^T$. Ens queda

   $$H = (101).$$

2. Podem comprovar que totes les paraules de C, quan les multipliquem per H, ens donen 0. En efecte,
$$\begin{pmatrix} 1 & 0 & 1 \end{pmatrix}\begin{pmatrix} 0\\0\\0 \end{pmatrix} = 0, \quad \begin{pmatrix} 1 & 0 & 1 \end{pmatrix}\begin{pmatrix} 1\\1\\1 \end{pmatrix} = 0,$$
$$\begin{pmatrix} 1 & 0 & 1 \end{pmatrix}\begin{pmatrix} 1\\0\\1 \end{pmatrix} = 0, \quad \begin{pmatrix} 1 & 0 & 1 \end{pmatrix}\begin{pmatrix} 0\\1\\0 \end{pmatrix} = 0.$$

3. El codi dual és el que està generat per H. En el nostre cas és $\{0H, 1H\} = \{(000), (101)\}$.

4. $$\begin{pmatrix} 1 & 0 & 1\\ 0 & 1 & 0 \end{pmatrix}\begin{pmatrix} 0\\0\\0 \end{pmatrix} = \begin{pmatrix} 0\\0 \end{pmatrix},$$
$$\begin{pmatrix} 1 & 0 & 1\\ 0 & 1 & 0 \end{pmatrix}\begin{pmatrix} 1\\0\\1 \end{pmatrix} = \begin{pmatrix} 0\\0 \end{pmatrix}.$$

Torna a l'exercici (p.89)

Solució de l'Exercici 73

1. La distància mínima és $d = 1$. Es pot veure de tres maneres diferents:
   - per la matriu de control, que en l'exercici anterior havíem vist que era (101) i, per tant, té una columna linealment dependent;
   - perquè hi ha una paraula de pes 1;
   - perquè podem trobar dues paraules a distància 1.

2. Pel codi C tenim paràmetres $n = 3$, $k = 2$, $d = 1$. La fita de Singleton estableix $k \leq n - d + 1$, que en el cas de C correspon a
$$2 \leq 3 - 1 + 1 = 3.$$

Torna a l'exercici (p.90)

Solució de l'Exercici 74

1. Els polinomis irreductibles de grau 2 de $\mathbb{Z}_2[x]$ seran aquells que no s'anul·lin a 0 (coef. constant 1) ni a 1 (nombre senar de termes no nuls). L'únic polinomi amb aquestes característiques és $x^2 + x + 1$.

2.

0	00
1	10
α	01
α^2	11

3. La cadena de bits representa la cadena de símbols $\alpha 1 \alpha 0 \alpha^2 \alpha^2$. Multipliquem cada parell de símbols per la matriu generadora:
$$\alpha 0 \alpha^2 1 \quad \alpha \alpha^2 \alpha^2 \alpha \quad \alpha^2 \alpha^2 1 1$$
El resultat en bits serà
$$01001110 \quad 01111101 \quad 11111010$$

4. La matriu generadora sistemàtica serà:
$$\begin{pmatrix} 1 & 0 & \alpha & \alpha^2\\ 0 & 1 & 0 & 1 \end{pmatrix}.$$

Per tant, com a matriu de control podem agafar

$$\begin{pmatrix} \alpha & 0 & 1 & 0 \\ \alpha^2 & 1 & 0 & 1 \end{pmatrix}.$$

5. Com que a la matriu de control hi ha dues columnes iguals i no hi ha cap columna nul·la, la distància mínima és 2.
6. No es pot corregir cap error, es pot corregir un esborrall i es pot detectar un error.
7. De les tres paraules codificades només té error la paraula del mig (multiplicada per la matriu de control dona $\neq 0$).

Torna a l'exercici (p.93)

Solució de l'Exercici 75

1. El polinomi és irreductible perquè té grau 2 i no té arrels ($f(0) = 2$, $f(1) = 2$ i $f(2) = 1$). Si fem totes les potències de $\alpha = [x]$ veiem que són diferents fins que arribem a $\alpha^8 = 1$. Per això el polinomi és primitiu.
2.

exp.	*vect.*
0	00
1	10
α	01
α^2	11
α^3	12
α^4	20
α^5	02
α^6	22
α^7	21

3. Com que els elements de $\mathbb{Z}_3[x]/x^2 + 2x + 2$ representen per dos trits cadascun, per poder passar la cadena de trits a cadena de símbols haurem d'agrupar els trits de 2 en 2. Així, la cadena de trits 01211022 la separem com

$$(01)(21)(10)(22).$$

A cada parella de trits li fem correspondre un símbol seguint la taula de l'apartat anterior. Obtenim la cadena de símbols

$$\alpha\alpha^7 1\alpha^6.$$

Ara, per poder codificar la cadena de símbols, la separem en blocs de $k = 2$ símbols:

$$(\alpha\alpha^7)(1\alpha^6).$$

Multipliquem cada bloc per la matriu generadora:

$$\begin{pmatrix} \alpha & \alpha^7 \end{pmatrix}\begin{pmatrix} 1 & \alpha & \alpha^2 & \alpha^3 \\ 0 & \alpha^4 & 0 & 1 \end{pmatrix} = \begin{pmatrix} \alpha & 2 & \alpha^3 & \alpha^2 \end{pmatrix}$$

$$\begin{pmatrix} 1 & \alpha^6 \end{pmatrix}\begin{pmatrix} 1 & \alpha & \alpha^2 & \alpha^3 \\ 0 & \alpha^4 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & \alpha^3 & \alpha^2 & \alpha \end{pmatrix}$$

i obtenim la cadena de símbols

$$\alpha, 2, \alpha^3, \alpha^2 \quad 1, \alpha^3, \alpha^2\alpha$$

que correspon a la cadena de trits

$$01201211 \quad 10121101.$$

4. La matriu generadora és equivalent a
$$\begin{pmatrix} 1 & \alpha & \alpha^2 & \alpha^3 \\ 0 & 1 & 0 & 2 \end{pmatrix},$$
que és equivalent a
$$\begin{pmatrix} 1 & 0 & \alpha^2 & 1 \\ 0 & 1 & 0 & 2 \end{pmatrix}.$$
Per tant, com a matriu de control podem agafar
$$H = \begin{pmatrix} \alpha^6 & 0 & 1 & 0 \\ 2 & 1 & 0 & 1 \end{pmatrix}.$$
5. Com que hi ha dues columnes linealment dependents i no hi ha cap columna nul·la, la distància mínima és 2.
6. No es pot corregir cap error, es pot corregir un esborrall i es pot detectar un error.

   La cadena de trits representa el vector $\alpha\alpha^3 x\alpha^6$. Perquè aquest vector sigui del codi, cal que en multiplicar-lo per H ens doni el vector nul.
$$H \cdot \begin{pmatrix} \alpha \\ \alpha^3 \\ x \\ \alpha^6 \end{pmatrix} = \begin{pmatrix} \alpha^7 + x \\ 0 \end{pmatrix}.$$
   Deduïm que
$$x + \alpha^7 = 0.$$
   Per tant, $x = -\alpha^7 = \alpha^3$. La paraula codi corregida és $\alpha\alpha^3\alpha^3\alpha^6$, que correspon a la cadena de trits
$$01121222.$$

Torna a l'exercici (p.94)

Solució de l'Exercici 76

Hem vist que una matriu de control era
$$H = \begin{pmatrix} 0 & 2 & 2 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 \\ 2 & 2 & 0 & 0 & 0 & 1 \end{pmatrix}$$

La síndrome del vector rebut serà
$$\begin{pmatrix} 0 & 2 & 2 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 \\ 2 & 2 & 0 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 2 \\ 1 \\ 2 \\ 1 \\ 2 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ 2 \\ 1 \end{pmatrix} = 2h_2$$
Deduïm que s'ha produït un error a la segona posició de valor 2 i que la paraula enviada era
$$\begin{pmatrix} 2 & 1 & 2 & 1 & 2 & 1 \end{pmatrix} - \begin{pmatrix} 0 & 2 & 0 & 0 & 0 & 0 \end{pmatrix} = \begin{pmatrix} 2 & 2 & 2 & 1 & 2 & 1 \end{pmatrix}$$

Torna a l'exercici (p.96)

Solució de l'Exercici 77(a)

En el primer cas, la síndrome és

$$\begin{pmatrix} 0 & 2 & 2 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 \\ 2 & 2 & 0 & 0 & 0 & 1 \end{pmatrix}\begin{pmatrix} 1 \\ 2 \\ 0 \\ 1 \\ 0 \\ 2 \end{pmatrix} = \begin{pmatrix} 2 \\ 2 \\ 2 \end{pmatrix}$$

Aquesta síndrome no és múltiple de cap columna de H, per tant, deduïm que s'ha produït més d'un error. Però sí que es pot escriure de manera única com a combinació lineal de dues columnes com $h_2 + h_5$. Per tant, deduïm que s'ha produït un error a la segona posició de valor 1 i un error a la cinquena posició de valor 1, i que la paraula enviada era

$$\begin{pmatrix} 1 & 2 & 0 & 1 & 0 & 2 \end{pmatrix} - \begin{pmatrix} 0 & 1 & 0 & 0 & 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 1 & 0 & 1 & 2 & 2 \end{pmatrix}$$

Torna a l'exercici (p.96)

Solució de l'Exercici 77(b)

En el segon cas, la síndrome és

$$\begin{pmatrix} 0 & 2 & 2 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 \\ 2 & 2 & 0 & 0 & 0 & 1 \end{pmatrix}\begin{pmatrix} 2 \\ 2 \\ 2 \\ 2 \\ 2 \\ 2 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix}$$

Aquesta síndrome no és ni nul·la ni múltiple de cap columna de H. Però sí que es pot escriure com a combinació lineal de dues columnes, tot i que es pot fer de dues maneres diferents: $h_4 + h_6$ o bé $2h_2 + h_5$. Per tant, deduïm que s'han produït dos errors i que la paraula enviada era

$$\begin{pmatrix} 2 & 2 & 2 & 2 & 2 & 2 \end{pmatrix} - \begin{pmatrix} 0 & 0 & 0 & 1 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 2 & 2 & 2 & 1 & 2 & 1 \end{pmatrix}$$

o bé

$$\begin{pmatrix} 2 & 2 & 2 & 2 & 2 & 2 \end{pmatrix} - \begin{pmatrix} 0 & 2 & 0 & 0 & 1 & 0 \end{pmatrix} = \begin{pmatrix} 2 & 0 & 2 & 2 & 1 & 2 \end{pmatrix}$$

Torna a l'exercici (p.96)

Solució de l'Exercici 78

1. 3.
2. 3.
3. 1132321031.

Torna a l'exercici (p.96)

Solució de l'Exercici 79

6. 01110101.
7. 01.

Torna a l'exercici (p.97)

4.5 Apèndix: Repàs d'àlgebra lineal i matrius

Repàs d'espais vectorials

Un **espai vectorial** sobre $\mathbb{F}$ és un conjunt V amb dues operacions suma '+' i producte '·' que satisfan les condicions de la llista. Els elements de V s'anomenen **vectors**, i els de $\mathbb{F}$ s'anomenen **escalars**.

1. El conjunt V és **tancat per la suma**:
   $\mathbf{x}+\mathbf{y} \in V$ per tot $\mathbf{x}, \mathbf{y}, \in V$.
2. La suma és **commutativa**:
   $\mathbf{x}+\mathbf{y}=\mathbf{y}+\mathbf{x}$ per tot $\mathbf{x}, \mathbf{y} \in V$.
3. La suma és **associativa:**
   $(\mathbf{x}+\mathbf{y})+\mathbf{z}=\mathbf{x}+(\mathbf{y}+\mathbf{z})$ per tot $\mathbf{x}, \mathbf{y}, \mathbf{z} \in V$.
4. Existeix un **element neure** $\mathbf{0} \in V$ tal que $\mathbf{x}+\mathbf{0}=\mathbf{x}$ per tot $\mathbf{x} \in V$.
5. Per tot $\mathbf{x} \in V$ existeix un **element oposat** $-\mathbf{x}$ pel qual $\mathbf{x}+(-\mathbf{x})=\mathbf{0}$.
6. El conjunt V és **tancat** per la multiplicació per escalars:
   $\alpha \cdot \mathbf{x} \in V$ per tot $\mathbf{x} \in V$.
7. El producte és **distributiu** sobre la suma d'escalars:
   $(\alpha+\beta) \cdot \mathbf{x}=\alpha \cdot \mathbf{x}+\beta \cdot \mathbf{x}$ per tot $\alpha, \beta \in \mathbb{F}$ i $\mathbf{x} \in V$.
8. El producte és **distributiu** sobre la suma de vectors:
   $\alpha \cdot(\mathbf{x}+\mathbf{y})=\alpha \cdot \mathbf{x}+\alpha \cdot \mathbf{y}$ per tot $\alpha, \beta \in \mathbb{F}$ i $\mathbf{x}, \mathbf{y} \in V$.
9. El producte per escalars i el producte a $\mathbb{F}$ són **compatibles**:
   $(\alpha\beta) \cdot \mathbf{x}=\alpha \cdot(\beta \cdot \mathbf{x})$ per tot $\alpha, \beta \in \mathbb{F}$ i $\mathbf{x} \in V$.
10. La **unitat** $1 \in \mathbb{F}$ satisfà $1 \cdot \mathbf{x}=\mathbf{x}$ per tot $\mathbf{x} \in V$

Definició

Un **subespai vectorial** de V és un conjunt tancat per la suma i el producte per escalars. És a dir,
- Si $\alpha \in \mathbb{F}$ i $v \in V$, aleshores $\alpha v \in V$.
- Si $v_1, v_2 \in V$, aleshores $v_1+v_2 \in V$.

Relacionat: codi lineal (p.82)

Definició

Sigui V un espai vectorial i $\mathbf{x}_1, \ldots, \mathbf{x}_n \in V$. Diem que $\mathbf{x}_1, \ldots, \mathbf{x}_n$ són **linealment dependents** si existeixen $\alpha_1, \ldots, \alpha_n \in \mathbb{F}$ no tots nuls pels quals

$$\alpha_1 \mathbf{x}_1+\ldots+\alpha_n \mathbf{x}_n=\mathbf{0}.$$

Altrament, direm que són **linealment independents**.

En particular, un únic vector és linealment dependent si i només si és el vector nul. Dos vectors són linealment dependents si i només si són proporcionals, és a dir, un vector és el producte de l'altre per un escalar.

Relacionat: distància mínima (p.90)

Definició

Un conjunt $\{\mathbf{x}_1, \ldots, \mathbf{x}_n\} \subseteq V$ és un **sistema de generadors** d'un subespai vectorial S si tot element de S es pot escriure com a combinació lineal de $\mathbf{x}_1, \ldots, \mathbf{x}_n$.

Definició

Un conjunt $\{\mathbf{x}_1, \ldots, \mathbf{x}_n\} \subseteq V$ és una **base** del subespai vectorial S si és un sistema de generadors que és linealment indepedent. Relacionat: matriu generadora (p.83)

Proposició 1

Totes les bases d'un subespai vectorial tenen el mateix nombre d'elements.

Definició

La **dimensió** d'un subespai vectorial $S \subseteq V$ és el nombre d'elements que té qualsevol de les seves bases. Relacionat: dimensió d'un codi lineal (p.82)

Definició

Si E és un K-subespai vectorial de F i $\dim F = n$, aleshores un **sistema d'equacions impícites** de E és un sistema homogeni d'equacions de K^n les solucions del qual són els (vectors de coordenades dels) elements de E.

Base sistemàtica: Si E és un subespai vectorial de F, $\dim F = n$, $\dim E = k$ i B és una base de F, aleshores una **base sistemàtica** de E en les posicions $\{j_1, \ldots, j_k\}$ (posicions sistemàtiques) és una base $S = \{s_1, \ldots, s_k\}$ on

- $(coord_B(s_i))_{j_r} = 0$ per tot $r \neq i$
- $(coord_B(s_i))_{j_i} = 1$.

Sempre existeix un conjunt de posicions sistemàtiques i una base sistemàtica en aquestes posicions. El conjunt de posicions sistemàtiques i la base sistemàtica són únics si afegim la condició $(coord_B(s_i))_l = 0$ for all $l < j_i$. Aquesta base s'obté per transformacions gaussianes.

Relacionat: matriu generadora sistemàtica (p.85)

Diem G a la matriu $k \times n$ següent:

$$\begin{pmatrix} \leftarrow & coord_B(s_1) & \rightarrow \\ & \vdots & \\ \leftarrow & coord_B(s_k) & \rightarrow \end{pmatrix}.$$

La submatriu de G formada per les columnes en les posicions sistemàtiques és la matriu identitat $k \times k$ i la submatriu de G formada per les columnes en les posicions no sistemàtiques és una matriu $k \times (n-k)$, que podem anaomenar $\tilde{G}$, que té l'element de la fila r i columna "corresponent a" l igual a $(coord_B(s_r))_l$.

Els elements de E seran combinacions lineals dels elements de S i tindran la forma $u = \lambda_1 s_1, \ldots, \lambda_k s_k = (\lambda_1 \ \ldots \ \lambda_k)G$. Si diem $(x_1, \ldots, x_n) = coord_B(u)$, aleshores, $x_{j_i} = \lambda_i$, per tota posició sistemàtica j_i, mentres que per les posicions no sistemàtiques, $x_l = \sum_i \lambda_i (coord_B(s_i))_l = \sum_i (coord_B(s_i))_l x_{j_i}$. Això ens permet obtenir un sistema de $n-k$ equacions implícites d'un subespai a partir de la base sistemàtica on les equacions són $-\sum_i (coord_B(s_i))_l x_{j_i} + x_l = 0$ per tot $l \notin \{j_1, \ldots, j_k\}$. Diem H a la matriu d'aquest sistema d'equacions. La submatriu de H formada per les columnes en les posicions no sistemàtiques és la matriu identitat $(n-k) \times (n-k)$ i la submatriu de H formada per les columnes en les posicions sistemàtiques és una matriu $(n-k) \times k$ que té l'element de la fila l i columna r igual a $-(coord_B(s_r))_l$, és a dir, la submatriu és $-\tilde{G}^T$.

Relacionat: matrius generadores i de control sistemàtiques (p.88)

Definició

El **complement ortogonal** d'un subespai E, que denotem $E^\perp$, és l'espai generat per les files d'una matriu d'un sistema d'equacions implícites de E.

Relacionat: codi dual (p.87)

És independent de la matriu seleccionada.

Té dimensió $n-k$.

$(E^\perp)^\perp = E$

Repàs de matrius

Una **matriu** $m \times n$ és un conjunt de $m \cdot n$ elements organitzats en m **files** horitzontals i n **columnes** verticals.

La matriu $n \times m$ que conté com a files les columnes de la matriu anterior i que conté com a columnes les files de la matriu anterior s'anomena la seva **transposda**.

Per exemple, la primera de les matrius següents és una matriu 2×3 mentre que la segona matriu és la seva transposada.

$$A = \begin{pmatrix} 5 & 1 & 3 \\ 9 & 8 & 2 \end{pmatrix}, \quad A^T = \begin{pmatrix} 5 & 9 \\ 1 & 8 \\ 3 & 2 \end{pmatrix}.$$

Anomenem a_{ij} l'element d'A que es troba a la i-èssima fila i a la j-èssima columna.

Una matriu és **quadrada** si té tantes files com columnes. La **diagonal principal** d'una matriu quadrada està formada pel primer element de la primera fila, el segon element de la segona fila, el tercer element de la tercera fila, i així fins al darrer element de la darrera fila.

Per exemple, la matriu següent és quadrada i la seva diagonal principal és $4, 7, 1$:

$$\begin{pmatrix} 4 & 5 & 0 \\ 2 & 7 & 9 \\ 8 & 6 & 1 \end{pmatrix}$$

La **matriu identitat** d'ordre i és la matriu quadrada amb 1 a la diagonal principal i 0 a la resta de posicions. Per exemple, la matriu identitat d'ordre 3 és

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

Per multiplicar una matriu per un vector (vertical), multipliquem cadascuna de les files de la matriu pel vector i deixem el resultat a la mateixa altura que ocupa la fila. Per exemple,

$$\begin{pmatrix} 5 & 1 & 3 \\ 9 & 8 & 2 \end{pmatrix} \begin{pmatrix} 4 \\ 6 \\ 5 \end{pmatrix} = \begin{pmatrix} 41 \\ 94 \end{pmatrix}.$$

En canvi, per multiplicar un vector (horitzontal) per una matriu, multipliquem el vector per cadascuna de les columnes de la matriu i deixem el resultat a la mateixa posició que ocupa la columna. Per exemple,

$$\begin{pmatrix} 3 & 7 \end{pmatrix} \begin{pmatrix} 5 & 1 & 3 \\ 9 & 8 & 2 \end{pmatrix} = \begin{pmatrix} 78 & 59 & 23 \end{pmatrix}.$$

Per multiplicar dues matrius, multipliquem la matriu de l'esquerra per cadascuna de les columnes de la matriu de la dreta. Per exemple,

$$\begin{pmatrix} 5 & 1 & 3 \\ 9 & 8 & 2 \end{pmatrix} \begin{pmatrix} 4 & 1 \\ 6 & 3 \\ 5 & 2 \end{pmatrix} = \begin{pmatrix} 41 & 14 \\ 94 & 37 \end{pmatrix}.$$

5 Teoria de codis: codis cíclics

5.1 Codis cíclics

Definició

Diem que els **desplaçaments circulars** d'una paraula $(c_0, c_1, \dots, c_{n-1}) \in \mathbb{F}_q^n$ són totes les paraules $(c_i, c_{i+1}, \dots, c_{n-1}, c_0, c_1, \dots, c_{i-1})$ amb $0 \leq i \leq n-1$.

Exemple. *Els desplaçaments circulars de* 2 5 3 4 6 1 *seran*

2	5	3	4	6	1
5	3	4	6	1	2
3	4	6	1	2	5
4	6	1	2	5	3
6	1	2	5	3	4
1	2	5	3	4	6

Diem que un codi lineal és **cíclic** si conté tots els desplaçaments circulars de totes les seves paraules.

Exercici 80

Considerem el conjunt de paraules $\{0000, 0101, 1010, 1111\} \subseteq \mathbb{Z}_2^4$.

1. Demostreu que és un codi lineal.
2. Quina dimensió té?
3. Doneu-ne una matriu generadora.
4. Demostreu que és un codi cíclic.

Solució (p.120)

Exercici 81

Suposem que tenim un codi sobre $\mathbb{F}_{11}$ cíclic de longitud 12 i dimensió 7. La codificació sistemàtica en les darreres posicions d'un vector d'informació i és

$$10 \;\; 1 \;\; 10 \;\; 0 \;\; 1 \;\; 10 \;\; 0 \;\; 2 \;\; 8 \;\; 3 \;\; 9 \;\; 1.$$

Doneu la codificació sistemàtica en les primeres posicions del mateix vector d'informació.

Solució (p.121)

Polinomi generador

Per treballar amb codis cíclics, identifiquem els vectors amb polinomis

$$(v_0, v_1, \dots, v_{n-1}) \leftrightarrow v_0 + v_1 x + v_2 x^2 + \cdots + v_{n-1} x^{n-1}.$$

Per això, sovint indexarem dins de $0 \dots n-1$ en comptes de $1 \dots n$.

Exemple. *En l'exemple $C = \{0000, 0101, 1010, 1111\} \subseteq \mathbb{Z}_2^4$, les paraules del codi les identificaríem amb polinomis de la manera següent:*

$$\begin{array}{lcl}
0000 & \longrightarrow & 0 + 0x + 0x^2 + 0x^3 = 0 \\
0101 & \longrightarrow & 0 + 1x + 0x^2 + 1x^3 = x + x^3 \\
1010 & \longrightarrow & 1 + 0x + 1x^2 + 0x^3 = 1 + x^2 \\
1111 & \longrightarrow & 1 + 1x + 1x^2 + 1x^3 = 1 + x + x^2 + x^3
\end{array}$$

En un codi cíclic, diem que el **polinomi generador** és el polinomi que representa una paraula no nul·la del codi i que
- té grau mínim,
- és mònic (el coeficient de grau més gran és 1).

Lema 15: Lema fonamental dels codis cíclics

Suposem que C és un codi cíclic de longitud n i dimensió k.
Sigui $g(x)$ un polinomi generador de C, aleshores

1. $g(x)$ és únic amb aquesta propietat.
2. $v \in C \iff v(x)$ és divisible per $g(x)$
   és a dir, les paraules del codi són els múltiples de $g(x)$.
3. $g(x)$ és un divisor de $x^n - 1$.
4. Si el polinomi generador és $g(x) = g_0 + g_1 x + g_2 x^2 + \cdots + g_r x^r$, aleshores com a matriu generadora podem agafar
$$\begin{pmatrix}
g_0 & g_1 & \dots & g_r & 0 & \dots & & & 0 \\
0 & g_0 & g_1 & \dots & g_r & 0 & \dots & & 0 \\
0 & 0 & g_0 & g_1 & \dots & g_r & 0 & \dots & 0 \\
\vdots & & \ddots & \ddots & \ddots & \ddots & \ddots & & \vdots \\
& & & & & & & & \\
0 & 0 & \dots & \dots & 0 & g_0 & g_1 & \dots & g_r
\end{pmatrix}.$$
5. $g(x)$ té grau $n - k$.

Demostració. *1. Si $g(x)$ i $g'(x)$ són tots dos mònics i de grau mínim, aleshores $g(x)-g'(x)$ és un polinomi que representa una paraula del codi de grau més petit que el mínim d'entre els que representen paraules no nul·les.*

Per tant, $g(x)-g'(x)$ ha de ser nul.

2. *D'una banda, si multipliquem $g(x)$ per un monomi x^i amb $i+\mathrm{grau}(g)<n$, el resultat correspon a una paraula del codi.*

   D'aquí és fàcil deduir que qualsevol polinomi de la forma $g(x)\cdot f(x)$ amb grau total més petit que n pertany a C.

   Per tant, si $v(x)$, amb grau total més petit que n, és divisible per $g(x)$, aleshores $v\in C$.

   D'altra banda, suposem que v pertany al codi i que el polinomi corresponent té quocient $q(x)$ i residu $r(x)$ en dividir-lo per $g(x)$.

   Aleshores $r(x)=v(x)-q(x)g(x)$ representa una paraula del codi però té el grau més petit que $g(x)$. Per tant, ha de ser nul.

   Això vol dir que $v(x)$ és múltiple de $g(x)$.

3. *Suposem que la paraula corresponent a $g(x)$ és $(g_0,g_1,\dots,g_{n-1})$.*

   Com que C és cíclic, $(g_{n-1},g_0,g_1,\dots,g_{n-2})$ ha de pertànyer a C.

   Però $g_{n-1}+g_0x+g_1x^2\dots,g_{n-2}x^{n-1}=x\cdot g(x)-g_{n-1}x^n+g_{n-1}=x\cdot g(x)-g_{n-1}(x^n-1)$.

   Pel punt anterior sabem que $g(x)$ ha de dividir $x\cdot g(x)-g_{n-1}(x^n-1)$ i, per tant, $g(x)$ ha de dividir x^n-1.

4 *Es dedueix del punt 2.*

5 *Es dedueix del punt anterior.*

□

Recíprocament, es pot demostrar el següent:

Qualsevol polinomi $g(x)\in\mathbb{F}_q[x]$ que divideixi x^n-1 genera un codi cíclic de $\mathbb{F}_q^n$.

És a dir, si per alguns enters n i q, existeix un polinomi $g(x)=g_rx^r+g_{r-1}x^{r-1}+\dots+g_1x+g_0\in\mathbb{F}_q[x]$ que divideixi x^n-1, aleshores, equivalentment,

- La matriu de n columnes

$$\begin{pmatrix} g_0 & g_1 & \dots & g_r & 0 & \dots & & & 0\\ 0 & g_0 & g_1 & \dots & g_r & 0 & \dots & & 0\\ 0 & 0 & g_0 & g_1 & \dots & g_r & 0 & \dots & 0\\ \vdots & & \ddots & \ddots & \ddots & \ddots & \ddots & & \vdots\\ & & & & & & & & \\ 0 & 0 & \dots & \dots & 0 & g_0 & g_1 & \dots & g_r \end{pmatrix}$$

  genera un codi cíclic de $\mathbb{F}_q^n$ de dimensió $n-r$,
- El conjunt de paraules correponent al conjunt de polinomis $\{a(x)g(x) : a(x)\in\mathbb{F}_q[x],\ \text{amb grau}(a(x))<n-r\}$ és un codi cíclic de dimensió $n-r$.

Exercici 82

Considerem el codi cíclic format per les paraules $\{0000, 0101, 1010, 1111\} \subseteq \mathbb{Z}_2^4$.

1. Quina és la seva longitud n?
2. Doneu-ne el polinomi generador.
3. Comproveu que és un divisor de $x^n - 1$.
4. Comproveu que el seu grau és $n - k$.

Solució (p.121)

Matrius generadores

Una matriu té **forma de cascada** (de grau r) si és de la forma

$$A = \begin{pmatrix} a_0 & a_1 & \dots & a_r & 0 & & \dots & 0 \\ 0 & a_0 & a_1 & \dots & a_r & 0 & & 0 \\ 0 & 0 & a_0 & a_1 & \dots & a_r & 0 & 0 \\ \vdots & & \ddots & & & & \ddots & 0 \\ 0 & \dots & & 0 & a_0 & a_1 & \dots & a_r \end{pmatrix}$$

amb $a_0 \neq 0$, $a_r \neq 0$.

Exemple. *Les següents matrius de $\mathbb{Z}_7$ tenen forma de cascada.*

$$\begin{pmatrix} 4 & 2 & 0 & 3 & 5 & 1 & 0 & 0 & 0 \\ 0 & 4 & 2 & 0 & 3 & 5 & 1 & 0 & 0 \\ 0 & 0 & 4 & 2 & 0 & 3 & 5 & 1 & 0 \\ 0 & 0 & 0 & 4 & 2 & 0 & 3 & 5 & 1 \end{pmatrix}$$

$$\begin{pmatrix} 5 & 6 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 5 & 6 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 5 & 6 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 5 & 6 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 5 & 6 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 5 & 6 & 1 \end{pmatrix}$$

Observem que en una matriu cascada, el grau r coincideix amb la diferència entre el nombre de columnes i el nombre de files.

Observem també que, si A és una matriu cascada, aleshores $A = (Q|P)$, on

(1) Q és una matriu quadrada, triangular superior i tal que els valors dins de cada súper-diagonal coincideixen entre ells. A més, són no nuls el valor corresponent a la diagonal principal i a la r-èssima súper-diagonal, i és zero el valor de les súper-diagonals més enllà de la r-èssima.

(2) Si k és el nombre de files de A, aleshores la concatenació de a_0 amb la fila inferior de la matriu P d'una banda i la primera fila de A d'una altra banda, coincideixen en les primeres $\min(r + 1, k)$ posicions.

Una matriu té **forma de precascada** si és de la forma $(Q|P)$ on Q i P satisfan les propietats (1) i (2).

En aquest cas,

$$A=\left(\begin{array}{ccccccc|ccc} a_0 & a_1 & \dots & a_r & 0 & \dots & 0 & * & * & * \\ 0 & a_0 & a_1 & \dots & a_r & \ddots & \vdots & * & & * \\ 0 & 0 & a_0 & a_1 & \dots & a_r & 0 & \vdots & & \vdots \\ \vdots & & \ddots & a_0 & & & a_r & & & \\ \vdots & & & \ddots & a_0 & & a_{r-1} & \vdots & & \vdots \\ \vdots & & & & \ddots & \ddots & \vdots & * & * & * \\ 0 & \dots & \dots & \dots & & 0 & a_0 & a_1 & \dots & a_r \end{array}\right) \text{ si } r<k \qquad \text{o bé} \qquad A=\left(\begin{array}{ccccccc|cccc} a_0 & a_1 & \dots & & & & a_{k-1} & * & * & * & * \\ 0 & a_0 & a_1 & \dots & & & a_{k-2} & * & & & * \\ 0 & 0 & a_0 & a_1 & \dots & & a_{k-3} & \vdots & & & \vdots \\ \vdots & & \ddots & a_0 & & & & & & & \\ \vdots & & & \ddots & a_0 & & & \vdots & & & \vdots \\ \vdots & & & & \ddots & \ddots & \vdots & * & * & * & * \\ 0 & \dots & \dots & \dots & & 0 & a_0 & a_1 & \dots & \dots & a_r \end{array}\right) \text{ si } r\geq k$$

amb $a_0 \neq 0$, $a_r \neq 0$.

Si $a_0 = 1$ diem que la matriu té forma de **precascada normalitzada**.

Exemple. *Vegem com podem convertir una matriu com ara* $A=\begin{pmatrix} 1 & 0 & 0 & 1 & 3 \\ 0 & 1 & 0 & 0 & 2 \\ 0 & 0 & 1 & 3 & 4 \end{pmatrix}$ *definida sobre* $\mathbb{F}_7$*, en una matriu equivalent en forma de precascada normalitzada.*

$$\begin{pmatrix} 1 & 0 & 0 & 1 & 3 \\ 0 & 1 & 0 & 0 & 2 \\ 0 & 0 & 1 & 3 & 4 \end{pmatrix} \sim_{f_1' = f_1 + 3f_2} \begin{pmatrix} 1 & 3 & 0 & 1 & 2 \\ 0 & 1 & 0 & 0 & 2 \\ 0 & 0 & 1 & 3 & 4 \end{pmatrix} \sim_{\substack{f_1' = f_1 + 4f_3 \\ f_2' = f_2 + 3f_3}} \begin{pmatrix} 1 & 3 & 4 & 6 & 4 \\ 0 & 1 & 3 & 2 & 0 \\ 0 & 0 & 1 & 3 & 4 \end{pmatrix}$$

Qualsevol matriu que sigui equivalent a una matriu de la forma $(I|P)$, serà també equivalent a una *única* matriu en forma de precascada normalitzada.
En efecte, diguem $a_0 = 1$ i sigui $a_1, \dots, a_r$ la darrera fila de P. Definim

$$Q=\begin{pmatrix} a_0 & a_1 & \dots & a_r & 0 & \dots & 0 \\ 0 & a_0 & a_1 & \dots & a_r & \ddots & \vdots \\ 0 & 0 & a_0 & a_1 & \dots & a_r & 0 \\ \vdots & & \ddots & a_0 & & & a_r \\ \vdots & & & \ddots & a_0 & & a_{r-1} \\ \vdots & & & & \ddots & \ddots & \vdots \\ 0 & \dots & \dots & \dots & & 0 & a_0 \end{pmatrix} \text{ si } r<k \qquad \text{o bé} \qquad Q=\begin{pmatrix} a_0 & a_1 & \dots & & & & a_{k-1} \\ 0 & a_0 & a_1 & \dots & & & a_{k-2} \\ 0 & 0 & a_0 & a_1 & \dots & & a_{k-3} \\ \vdots & & \ddots & a_0 & & & \\ \vdots & & & \ddots & a_0 & & \\ \vdots & & & & \ddots & \ddots & \vdots \\ 0 & \dots & \dots & \dots & & 0 & a_0 \end{pmatrix} \text{ si } r\geq k$$

El producte de matrius $Q(I \mid P)$ és equivalent també a $(I \mid P)$ i té forma de precascada normalitzada.

Exemple. *En l'exemple anterior tindríem* $Q=\begin{pmatrix} 1 & 3 & 4 \\ 0 & 1 & 3 \\ 0 & 0 & 1 \end{pmatrix}$

i $QA=\begin{pmatrix} 1 & 3 & 4 \\ 0 & 1 & 3 \\ 0 & 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 0 & 0 & 1 & 3 \\ 0 & 1 & 0 & 0 & 2 \\ 0 & 0 & 1 & 3 & 4 \end{pmatrix}=\begin{pmatrix} 1 & 3 & 4 & 6 & 4 \\ 0 & 1 & 3 & 2 & 0 \\ 0 & 0 & 1 & 3 & 4 \end{pmatrix}.$

Lema 16

El codi lineal generat per una matriu G de k files i n columnes és cíclic si i només si es compleixen les tres condicions següents:

- G és sistematitzable en les primeres posicions (és a dir, $G \sim (I \mid P)$ per una (única) matriu P, de mida $k \times (n-k)$).
- La matriu en forma de precascada normalitzada equivalent a G és una matriu cascada.
- Si $a_1, \dots, a_{n-k}$ és la darrera fila de P, el polinomi $1 + a_1 x + \dots + a_{n-k}x^{n-k}$ divideix $x^n - 1$.

En aquest cas, el polinomi generador del codi és $a_{n-k}^{-1}(1 + a_1 x + \dots + a_{n-k}x^{n-k})$.

Exercici 83

Quina o quines de les següents matrius sobre $\mathbb{F}_7$ generen un codi cíclic?

1. $G_1 = \begin{pmatrix} 1 & 0 & 0 & 0 & 2 & 4 \\ 0 & 1 & 0 & 0 & 0 & 6 \\ 0 & 0 & 1 & 0 & 6 & 0 \\ 0 & 0 & 0 & 1 & 2 & 4 \end{pmatrix}$

2. $G_2 = \begin{pmatrix} 1 & 0 & 0 & 0 & 2 & 4 \\ 0 & 1 & 0 & 0 & 6 & 0 \\ 0 & 0 & 1 & 0 & 0 & 6 \\ 0 & 0 & 0 & 1 & 2 & 4 \end{pmatrix}$

3. $G_3 = \begin{pmatrix} 1 & 0 & 0 & 6 & 0 \\ 0 & 1 & 0 & 0 & 6 \\ 0 & 0 & 1 & 2 & 4 \end{pmatrix}$

Solució (p.122)

Codis cíclics primitius

Si un codi està definit sobre $\mathbb{F}_q$ i la seva longitud és $n = q - 1$, aleshores diem que el codi és **primitiu**.

Exercici 84

Demostreu que en aquest cas $x - \beta$ divideix $x^n - 1$ per a tot $\beta \in \mathbb{F}_q^*$.

Solució (p.123)

Exercici 85

Demostreu que si $\alpha_1, \dots, \alpha_r$ són elements de $\mathbb{F}_q \setminus \{0\}$ diferents entre ells, aleshores $(x - \alpha_1) \cdot \cdots \cdot (x - \alpha_r)$ és el polinomi generador d'un codi cíclic primitiu definit a $\mathbb{F}_q$.

Solució (p.123)

L'interès dels codis primitius és precisament una conseqüència del darrer exercici.

Per construir un codi cíclic sobre $\mathbb{F}_q$, podem agafar $n = q - 1$, i uns quants elements diferents de $\mathbb{F}_q$, que anomenem $\alpha_1, \alpha_2, \dots, \alpha_r$. Aleshores el polinomi $(x - \alpha_1) \cdot (x - \alpha_2) \cdot \cdots \cdot (x - \alpha_r)$ sabem que és el polinomi generador d'un codi cíclic.

Exemple. *Per construir un codi cíclic sobre $\mathbb{F}_{11} = \mathbb{Z}_{11}$, podem agafar el polinomi*

$$\begin{aligned} (x-3)(x-6)(x-10) &= x^3 + (-3-6-10)x^2 + \\ &\quad ((-3)(-6) + (-3)(-10) + (-6)(-10))x + (-3)(-6)(-10) \\ &= x^3 + 3x^2 + (7+8+5)x + 7 \\ &= x^3 + 3x^2 + 9x + 7, \end{aligned}$$

que dividirà $x^{10} - 1$ per l'exercici anterior. Per tant, és el polinomi generador d'un codi cíclic.

Quina serà la seva matriu generadora?

$$\begin{pmatrix}
7 & 9 & 3 & 1 & 0 & 0 & 0 & 0 & 0 & 0\\
0 & 7 & 9 & 3 & 1 & 0 & 0 & 0 & 0 & 0\\
0 & 0 & 7 & 9 & 3 & 1 & 0 & 0 & 0 & 0\\
0 & 0 & 0 & 7 & 9 & 3 & 1 & 0 & 0 & 0\\
0 & 0 & 0 & 0 & 7 & 9 & 3 & 1 & 0 & 0\\
0 & 0 & 0 & 0 & 0 & 7 & 9 & 3 & 1 & 0\\
0 & 0 & 0 & 0 & 0 & 0 & 7 & 9 & 3 & 1
\end{pmatrix}$$

Exemple. *Per construir un codi cíclic sobre $\mathbb{F}_9 = \mathbb{Z}_3/(x^2+2x+2)$, considerem que α sigui la classe de x. Tindrem*

$$\begin{array}{rcl}
\alpha^2 & = & \alpha+1\\
\alpha^3 & = & \alpha^2+\alpha = 2\alpha+1\\
\alpha^4 & = & 2\alpha^2+\alpha = 2\\
\alpha^5 & = & 2\alpha\\
\alpha^6 & = & 2\alpha^2 = 2\alpha+2\\
\alpha^7 & = & 2\alpha^2+2\alpha = \alpha+2\\
\alpha^8 & = & \alpha^2+2\alpha = 1
\end{array}$$

Com que $\alpha, \alpha^2, \alpha^3$ són tots diferents, considerem el polinomi

$$\begin{array}{rcl}
(x-\alpha)(x-\alpha^2)(x-\alpha^3) & = & x^3+(-\alpha-\alpha^2-\alpha^3)x^2+((-\alpha)(-\alpha^2)+(-\alpha)(-\alpha^3)\\
& & \quad +(-\alpha^2)(-\alpha^3))x+(-\alpha)(-\alpha^2)(-\alpha^3)\\
& = & x^3+(2\alpha+1)x^2+(\alpha^3+\alpha^4+\alpha^5)x+(-\alpha^6)\\
& = & x^3+\alpha^3x^2+\alpha x+\alpha^2
\end{array}$$

Sabem segur (per l'exercici) que aquest polinomi dividirà x^8-1 i, per tant, serà el polinomi generador d'un codi cíclic.

Quina serà la seva matriu generadora?

$$\begin{pmatrix}
\alpha^2 & \alpha & \alpha^3 & 1 & 0 & 0 & 0 & 0\\
0 & \alpha^2 & \alpha & \alpha^3 & 1 & 0 & 0 & 0\\
0 & 0 & \alpha^2 & \alpha & \alpha^3 & 1 & 0 & 0\\
0 & 0 & 0 & \alpha^2 & \alpha & \alpha^3 & 1 & 0\\
0 & 0 & 0 & 0 & \alpha^2 & \alpha & \alpha^3 & 1
\end{pmatrix}$$

Aquesta construcció la podem fer *només* si el codi és primitiu, és a dir, si $n = q-1$.

Polinomi de control

Si C és un codi cíclic de longitud n i polinomi generador $g(x)$, aleshores el **polinomi de control** de C es defineix com

$$h(x) = \frac{x^n-1}{g(x)}.$$

El polinomi de control compleix que

$$v(x) \in C \Longleftrightarrow v(x)h(x) = 0 \mod x^n-1.$$

Exercici 86

1. Demostreu que $g = x^4 + 4x^3 + 6x + 3$ genera un codi cíclic primitiu sobre $\mathbb{F}_7 = \mathbb{Z}_7$.
2. Doneu-ne el polinomi de control.
3. Quina longitud i quina dimensió té aquest codi?
4. Doneu-ne una matriu generadora.
5. Es pot deduir la distància mínima a partir de la matriu generadora?
6. Corregiu la paraula següent amb esborralls: $(???235)$.
7. Comproveu si la paraula obtinguda en l'apartat anterior pertany al codi mitjançant el polinomi de control.

Solució (p.123)

Exercici 87

Sobre $\mathbb{F}_2$ considerem la matriu

$$G = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}.$$

1. Demostreu que el codi generat per G és cíclic.
2. Trobeu els polinomis generador i de control.

Solució (p.125)

Matrius de control

Una matriu de control del codi cíclic C es pot trobar per tres procediments:

1. A partir d'una matriu generadora sistemàtica, $G = (I|P)$,

$$H_1 = (-P^T|I).$$

2. A partir del polinomi $h^*(x)$ recíproc del de control (té els coeficients en ordre invers),

$$H_2 = \text{matriu generadora del codi cíclic generat per } h^*(x).$$

3 Si g té $n-k$ arrels $\beta_1, \beta_2, \dots, \beta_{n-k}$, totes elles diferents,

$$H_3 = \begin{pmatrix} 1 & \beta_1 & \beta_1^2 & \dots & \beta_1^{n-1} \\ 1 & \beta_2 & \beta_2^2 & \dots & \beta_2^{n-1} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 1 & \beta_{n-k} & \beta_{n-k}^2 & \dots & \beta_{n-k}^{n-1} \end{pmatrix}.$$

En aquest cas, les síndromes de $v(x)$ seran $v(\beta_1)$, $v(\beta_2)$, $v(\beta_3)\dots$

Codificació sistemàtica

Per codificar sistemàticament una informació i de k símbols, podem fer-ho per dos procediments:

- Multipliquem i per una matriu generadora sistemàtica G. La codificació que obtenim és sistemàtica en les posicions on hi hagi la identitat dins de G.
- Suposem que $R(x)$ és el residu de dividir $i(x)x^{n-k}$ entre $g(x)$. Llavors $i(x)x^{n-k} - R(x)$ és múltiple de $g(x)$ i és una codificació de i sistemàtica en les últimes posicions.

Exercici 88

Considerem el codi cíclic generat per $g = x^4 + 4x^3 + 6x + 3$ sobre $\mathbb{F}_7 = \mathbb{Z}_7$. Codifiqueu de forma sistemàtica la informació (11) mitjançant el polinomi generador.

Solució (p.125)

Distància mínima prevista

Sigui α un element primitiu de $\mathbb{F}_q$. Sigui C un codi de $\mathbb{F}_q^n$.
La **distància mínima prevista** de C és el màxim enter δ tal que hi ha $\delta - 1$ arrels de g que són potències consecutives de α $(\alpha^b, \alpha^{b+1}, \dots, \alpha^{b+\delta-2})$.

Lema 17

Es compleix que, si d és la distància mínima real del codi, aleshores $d \geq \delta$.

Exercici 89

Considerem el codi sobre $\mathbb{F}_2$ generat per la matriu

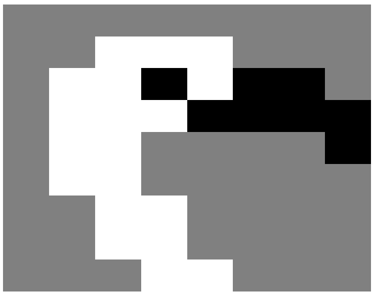
$$G = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}.$$

1. Trobeu una matriu de control de dues maneres diferents.
2. Quina és la distància mínima?
3. Codifiqueu de manera sistemàtica la informació 10110 mitjançant divisió de polinomis.

Solució (p.125)

5.2 L'exemple del faisà

Suposem una imatge digital.



La representem amb dígits de $\mathbb{F}_3 = \mathbb{Z}_3$.

1	1	1	1	1	1	1	1
1	1	2	2	2	1	1	1
1	2	2	0	2	0	0	1
1	2	2	2	0	0	0	0
1	2	2	1	1	1	1	0
1	2	2	1	1	1	1	1
1	1	2	2	1	1	1	1
1	1	2	2	1	1	1	1
1	1	1	2	2	1	1	1

La podem pensar també com si els seus elements fossin de $\mathbb{F}_9 = \mathbb{Z}_3/(x^2+2x+2)$. La representació vectorial dels elements d'aquest cos ve donada per la taula següent, on $\alpha = [x]$:

0	00
α^0	10
α^1	01
α^2	11
α^3	12
α^4	20
α^5	02
α^6	22
α^7	21

1	1	1	1	1	1	1	1		α^2	α^2	α^2	α^2
1	1	2	2	2	1	1	1		α^2	α^6	α^7	α^2
1	2	2	0	2	0	0	1		α^3	α^4	α^4	α
1	2	2	2	0	0	0	0		α^3	α^6	0	0
1	2	2	1	1	1	1	0	$\leftrightarrow$	α^3	α^7	α^2	1
1	2	2	1	1	1	1	1		α^3	α^7	α^2	α^2
1	1	2	2	1	1	1	1		α^2	α^6	α^2	α^2
1	1	2	2	1	1	1	1		α^2	α^6	α^2	α^2
1	1	1	2	2	1	1	1		α^2	α^3	α^7	α^2

Considerem el codi cíclic sobre $\mathbb{F}_9$ primitiu amb polinomi generador $g(x) = (x-\alpha)(x-\alpha^2)(x-\alpha^3)(x-\alpha^4) = x^4 + \alpha^6 x^3 + x^2 + \alpha^3 x + \alpha^2$.

Com que el codi és primitiu, té longitud $n = 9 - 1 = 8$. Com que el grau del polinomi generador és $n - k = 4$, aleshores la dimensió del codi és $k = 4$.

Això vol dir que, en codificar, agafem blocs de $k = 4$ símbols i els codifiquem, de manera que obtenim blocs de $n = 8$ símbols.

La distància mínima prevista és 5. D'acord amb la fita de Singleton, podem concloure que aquest codi té distància mínima 5.

Si fem codificació directa, aleshores simplement multipliquem els blocs de quatre símbols (polinomis de grau 3) pel polinomi generador (de grau 4), amb la qual cosa obtenim un bloc de 8 elements (que correspon a un polinomi de grau 7).

Els polinomis corresponents a la imatge són

$$\begin{array}{cccccl}
\alpha^2 & \alpha^2 & \alpha^2 & \alpha^2 & & \alpha^2+\alpha^2x+\alpha^2x^2+\alpha^2x^3 \\
\alpha^2 & \alpha^6 & \alpha^7 & \alpha^2 & & \alpha^2+\alpha^6x+\alpha^7x^2+\alpha^2x^3 \\
\alpha^3 & \alpha^4 & \alpha^4 & \alpha & & \alpha^3+\alpha^4x+\alpha^4x^2+\alpha x^3 \\
\alpha^3 & \alpha^6 & 0 & 0 & & \alpha^3+\alpha^6x \\
\alpha^3 & \alpha^7 & \alpha^2 & 1 & \leftrightarrow & \alpha^3+\alpha^7x+\alpha^2x^2+x^3 \\
\alpha^3 & \alpha^7 & \alpha^2 & \alpha^2 & & \alpha^3+\alpha^7x+\alpha^2x^2+\alpha^2x^3 \\
\alpha^2 & \alpha^6 & \alpha^2 & \alpha^2 & & \alpha^2+\alpha^6x+\alpha^2x^2+\alpha^2x^3 \\
\alpha^2 & \alpha^6 & \alpha^2 & \alpha^2 & & \alpha^2+\alpha^6x+\alpha^2x^2+\alpha^2x^3 \\
\alpha^2 & \alpha^3 & \alpha^7 & \alpha^2 & & \alpha^2+\alpha^3x+\alpha^7x^2+\alpha^2x^3
\end{array}$$

En multiplicar pel polinomi generador obtenim les paraules codificades.

Per exemple, per codificar la darrera fila $i(x)=\alpha^2+\alpha^3x+\alpha^7x^2+\alpha^2x^3$, la multipliquem per $g(x)$ i ens queda $\alpha^4+\alpha x+\alpha x^2+\alpha^4x^3+\alpha^5x^4+\alpha^6x^5+\alpha x^6+\alpha^2x^7$.

$$i(x)g(x)=\alpha^2g(x)+\alpha^3xg(x)+\alpha^7x^2g(x)+\alpha^2x^3g(x)$$

$$\begin{aligned}
\alpha^2g(x) &= \alpha^2x^4+\alpha^8x^3+\alpha^2x^2+\alpha^5x+\alpha^4 \\
&= \alpha^2x^4+x^3+\alpha^2x^2+\alpha^5x+\alpha^4 \\
\alpha^3xg(x) &= \alpha^3x^5+\alpha^9x^4+\alpha^3x^3+\alpha^6x^2+\alpha^5x \\
&= \alpha^3x^5+\alpha x^4+\alpha^3x^3+\alpha^6x^2+\alpha^5x \\
\alpha^7x^2g(x) &= \alpha^7x^6+\alpha^{13}x^5+\alpha^7x^4+\alpha^{10}x^3+\alpha^9x^2 \\
&= \alpha^7x^6+\alpha^5x^5+\alpha^7x^4+\alpha^2x^3+\alpha x^2 \\
\alpha^2x^3g(x) &= \alpha^2x^7+\alpha^8x^6+\alpha^2x^5+\alpha^5x^4+\alpha^4x^3 \\
&= \alpha^2x^7+x^6+\alpha^2x^5+\alpha^5x^4+\alpha^4x^3
\end{aligned}$$

$$\begin{aligned}
i(x)g(x) &= \alpha^2x^7+(1+\alpha^7)x^6+(\alpha^2+\alpha^5+\alpha^3)x^5 \\
&\quad+(\alpha^5+\alpha^7+\alpha+\alpha^2)x^4+(\alpha^4+\alpha^2+\alpha^3+1)x^3 \\
&\quad+(\alpha^3+\alpha^6+\alpha^2)x^2+(\alpha^5+\alpha^5)x+\alpha^4
\end{aligned}$$

Ara, fent servir la taula de correspondència, escrivim cada potència de α en notació vectorial i fem la suma. Per exemple, el coeficient de x^6 es correspon a

$$1+\alpha^7\to(1,0)+(2,1)=(0,1)\to\alpha$$

El resultat és

$$\alpha^4+\alpha x+\alpha x^2+\alpha^4x^3+\alpha^5x^4+\alpha^6x^5+\alpha x^6+\alpha^2x^7.$$

Fem ara el mateix amb totes les files:

$$
\begin{array}{cccccccc}
\alpha^4 & \alpha^6 & 0 & 1 & \alpha & \alpha^5 & \alpha^7 & \alpha^2 \\
\alpha^4 & \alpha^3 & 1 & 0 & \alpha^7 & \alpha^5 & \alpha & \alpha^2 \\
\alpha^5 & \alpha^2 & \alpha^6 & \alpha^7 & 0 & \alpha^5 & \alpha^2 & \alpha \\
\alpha^5 & \alpha^5 & 1 & \alpha^4 & \alpha^5 & \alpha^6 & 0 & 0 \\
\alpha^5 & \alpha^4 & 1 & \alpha^5 & \alpha & \alpha^2 & 0 & 1 \\
\alpha^5 & \alpha^4 & 1 & \alpha^2 & \alpha^7 & \alpha^3 & \alpha^7 & \alpha^2 \\
\alpha^4 & \alpha^3 & \alpha^5 & \alpha^7 & \alpha^2 & 1 & \alpha^7 & \alpha^2 \\
\alpha^4 & \alpha^3 & \alpha^5 & \alpha^7 & \alpha^2 & 1 & \alpha^7 & \alpha^2 \\
\alpha^4 & \alpha & \alpha & \alpha^4 & \alpha^5 & \alpha^6 & \alpha & \alpha^2
\end{array}
\leftrightarrow
\begin{array}{cccccccccccccccc}
2&0&2&2&0&0&1&0&0&1&0&2&2&1&1&1 \\
2&0&1&2&1&0&0&0&2&1&0&2&0&1&1&1 \\
0&2&1&1&2&2&2&1&0&0&0&2&1&1&0&1 \\
0&2&0&2&1&0&2&0&0&2&2&2&0&0&0&0 \\
0&2&2&0&1&0&0&2&0&1&1&1&0&0&1&0 \\
0&2&2&0&1&0&1&1&2&1&1&2&2&1&1&1 \\
2&0&1&2&0&2&2&1&1&1&1&0&2&1&1&1 \\
2&0&1&2&0&2&2&1&1&1&1&0&2&1&1&1 \\
2&0&0&1&0&1&2&0&0&2&2&2&0&1&1&1
\end{array}
$$

Si apliquem la codificació sistemàtica, aleshores cada polinomi l'hem de multiplicar per x^{n-k} i restar-li el residu de dividir pel polinomi generador.

Per exemple, per codificar la darrera fila $i(x) = \alpha^2 + \alpha^3 x + \alpha^7 x^2 + \alpha^2 x^3$, la multipliquem per x^{8-4} i ens queda $\alpha^2 x^4 + \alpha^3 x^5 + \alpha^7 x^6 + \alpha^2 x^7$. En dividir aquest darrer polinomi per $g(x)$, ens queda residu $R(x) = \alpha^3 + \alpha^6 x + \alpha^2 x^3$. Aleshores

$$
\begin{aligned}
i(x)x^{n-k} - R(x) &= \alpha^2 x^7 + \alpha^7 x^6 + \alpha^3 x^5 + \alpha^2 x^4 + \alpha^6 x^3 + \alpha^2 x + \alpha^7 \\
&\leftrightarrow (\alpha^7 \alpha^2 0 \alpha^6 \alpha^2 \alpha^3 \alpha^7 \alpha^2)
\end{aligned}
$$

que correspon a la imatge

$$
\begin{array}{cccccccccccccccc}
2&1&1&1&0&0&2&2&1&1&1&2&2&1&1&1
\end{array}
$$

Fem ara el mateix amb totes les files:

$$
\begin{array}{cccccccc}
\alpha^2 & \alpha^2 & \alpha^2 & \alpha^2 & \alpha^2 & \alpha^2 & \alpha^2 & \alpha^2 \\
\alpha^2 & \alpha^7 & \alpha^4 & \alpha^3 & \alpha^2 & \alpha^6 & \alpha^7 & \alpha^2 \\
\alpha^3 & \alpha & \alpha & \alpha^4 & \alpha^3 & \alpha^4 & \alpha^4 & \alpha \\
1 & \alpha^2 & \alpha^4 & \alpha^3 & \alpha^3 & \alpha^6 & 0 & 0 \\
\alpha^5 & \alpha^4 & 0 & \alpha & \alpha^3 & \alpha^7 & \alpha^2 & 1 \\
1 & \alpha^2 & \alpha^5 & \alpha^6 & \alpha^3 & \alpha^7 & \alpha^2 & \alpha^2 \\
0 & \alpha^6 & 0 & 0 & \alpha^2 & \alpha^6 & \alpha^2 & \alpha^2 \\
0 & \alpha^6 & 0 & 0 & \alpha^2 & \alpha^6 & \alpha^2 & \alpha^2 \\
\alpha^7 & \alpha^2 & 0 & \alpha^6 & \alpha^2 & \alpha^3 & \alpha^7 & \alpha^2
\end{array}
\leftrightarrow
\begin{array}{cccccccccccccccc}
1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1 \\
1&1&2&1&2&0&1&2&1&1&2&2&2&1&1&1 \\
1&2&0&1&0&1&2&0&1&2&2&0&2&0&0&1 \\
1&0&1&1&2&0&1&2&1&2&2&2&0&0&0&0 \\
0&2&2&0&0&0&0&1&1&2&2&1&1&1&1&0 \\
1&0&1&1&0&2&2&2&1&2&2&1&1&1&1&1 \\
0&0&2&2&0&0&0&0&1&1&2&2&1&1&1&1 \\
0&0&2&2&0&0&0&0&1&1&2&2&1&1&1&1 \\
2&1&1&1&0&0&2&2&1&1&1&2&2&1&1&1
\end{array}
$$

Observem que, en aquest cas, la imatge original queda replicada en les darreres posicions.

Suposem ara que aquesta imatge s'ha enviat i que el canal de transmissió ha generat certs errors.

$$
\begin{array}{cccccccccccccccc}
1&1&1&1&1&1&1&1&1&1&1&1&1&1&1&1 \\
1&1&2&1&2&0&1&2&1&1&2&2&2&1&1&1 \\
1&2&0&1&0&1&2&0&1&2&2&0&2&0&0&1 \\
1&0&1&1&2&0&1&2&1&2&2&2&0&0&0&0 \\
0&2&2&0&0&0&0&1&1&2&2&1&1&1&1&0 \\
1&0&1&1&0&2&2&2&1&2&2&1&1&1&1&1 \\
0&0&2&2&0&0&0&0&1&1&2&2&1&1&1&1 \\
0&0&2&2&0&0&0&0&1&1&2&2&1&1&1&1 \\
2&1&2&2&0&0&2&2&1&1&1&2&2&1&1&0
\end{array}
$$

El receptor genera una matriu de control per verificar si hi ha hagut errors. El polinomi de control és $h(x) = \frac{x^n-1}{g} = x^4 + \alpha^2 x^3 + x^2 + \alpha^7 x + \alpha^2$.

Per tant, podem agafar com a matriu de control

$$H = \begin{pmatrix} 1 & \alpha^2 & 1 & \alpha^7 & \alpha^2 & 0 & 0 & 0 \\ 0 & 1 & \alpha^2 & 1 & \alpha^7 & \alpha^2 & 0 & 0 \\ 0 & 0 & 1 & \alpha^2 & 1 & \alpha^7 & \alpha^2 & 0 \\ 0 & 0 & 0 & 1 & \alpha^2 & 1 & \alpha^7 & \alpha^2 \end{pmatrix}$$

En multiplicar les primeres 8 paraules per H, s'obté el vector nul. Però, en multiplicar la darrera per H, obtenim

$$\begin{pmatrix} 1 & \alpha^2 & 1 & \alpha^7 & \alpha^2 & 0 & 0 & 0 \\ 0 & 1 & \alpha^2 & 1 & \alpha^7 & \alpha^2 & 0 & 0 \\ 0 & 0 & 1 & \alpha^2 & 1 & \alpha^7 & \alpha^2 & 0 \\ 0 & 0 & 0 & 1 & \alpha^2 & 1 & \alpha^7 & \alpha^2 \end{pmatrix} \begin{pmatrix} \alpha^7 \\ \alpha^6 \\ 0 \\ \alpha^6 \\ \alpha^2 \\ \alpha^3 \\ \alpha^7 \\ 1 \end{pmatrix} = \begin{pmatrix} \alpha^4 \\ \alpha^2 \\ 0 \\ \alpha^7 \end{pmatrix}.$$

Si fos associat a un vector d'error de pes 1, la síndrome seria múltiple d'una columna. Comprovem que no és així. Busquem una combinació lineal de dues columnes que doni aquesta síndrome. Observem que

$$\begin{pmatrix} \alpha^4 \\ \alpha^2 \\ 0 \\ \alpha^7 \end{pmatrix} = \alpha^2 H^2 + \alpha^5 H^8.$$

Per tant, considerarem que l'error és $e = (0\alpha^2 00000\alpha^5)$. La paraula codi correcta és

$(\alpha^7\alpha^6 0\alpha^6\alpha^2\alpha^3\alpha^7 1) - (0\alpha^2 00000\alpha^5) = (\alpha^7\alpha^2 0\alpha^6\alpha^2\alpha^3\alpha^7\alpha^2)$.

Com que el codi és sistemàtic, sabem que la redundància és a l'esquerra i que la part d'informació correspon als símbols $\alpha^2\alpha^3\alpha^7\alpha^2$.

5.3 Solucions

Solució de l'Exercici 80

1. És un subespai vectorial perquè totes les combinacions lineals de dues de les quatre paraules pertanyen al codi:

   $$\begin{array}{ccccc} 0000 & + & 0000 & = & 0000 \\ 0000 & + & 0101 & = & 0101 \\ 0000 & + & 1010 & = & 1010 \\ 0101 & + & 0101 & = & 0000 \\ 0101 & + & 1010 & = & 1111 \\ 0101 & + & 1111 & = & 1010 \\ 1010 & + & 1010 & = & 0000 \\ 1010 & + & 1111 & = & 0101 \\ 1111 & + & 1111 & = & 0000 \end{array}$$

   Per tant, és un codi lineal.

2. La dimensió és 2 perquè és el màxim nombre de paraules linealment independents.

3. Qualsevol de les tres matrius següents és matriu generadora

$$\begin{pmatrix} 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 \end{pmatrix},$$

i també qualsevol de les anteriors intercanviant les dues files.

4. És un codi cíclic perquè qualsevol desplaçament circular de les seves paraules dona una altra paraula del codi. En efecte,
   - tots els desplaçaments circulars de 0000 donen la mateixa paraula 0000,
   - tots els desplaçaments circulars de 0101 donen la mateixa paraula 0101 o bé la paraula 1010,
   - tots els desplaçaments circulars de 1010 donen la mateixa paraula 1010 o bé la paraula 0101,
   - tots els desplaçaments circulars de 1111 donen la mateixa paraula 1111.

Torna a l'exercici (p.108)

Solució de l'Exercici 81

Com que és un codi de dimensió 7 sistemàtic en les darreres posicions, deduïm que el bloc d'informació corresponent a la paraula codi

$$\overbrace{10\ 1\ 10\ 0\ 1}^{n-k=5}\ \overbrace{10\ 0\ 2\ 8\ 3\ 9\ 1}^{k=7}$$

és

$$10\ 0\ 2\ 8\ 3\ 9\ 1.$$

Si volem la codificació sistemàtica de 10 0 2 8 3 9 1 en les primeres posicions, estem buscant un vector que sigui del codi i que sigui de la forma

$$(10\ 0\ 2\ 8\ 3\ 9\ 1\ r_1\ r_2\ r_3\ r_4\ r_5),$$

on r_1, r_2, r_3, r_4, r_5 ens venen donats de manera únivoca pel bloc d'informació.

Però, d'altra banda, com que el codi és cíclic, sabem que la paraula següent també és del codi: $(10\ 0\ 2\ 8\ 3\ 9\ 1\ 10\ 1\ 10\ 0\ 1)$.

Com que la codidificació del bloc d'informació és única, per força hem de tenir

$$r_1 = 10\ r_2 = 1\ r_3 = 10\ r_4 = 0\ r_5 = 1.$$

Per tant, la paraula codi demanada ha de ser

$$(10\ 0\ 2\ 8\ 3\ 9\ 1\ 10\ 1\ 10\ 0\ 1).$$

Torna a l'exercici (p.108)

Solució de l'Exercici 82

1. La longitud és $n = 4$.
2. Els polinomis que representen les 4 paraules del codi són
   - 0,
   - $x + x^3$,
   - $1 + x^2$,
   - $1 + x + x^2 + x^3$,

   dels quals el de grau mínim sense comptar el 0 és $x^2 + 1$. Per tant, aquest és el polinomi generador del codi.
3.

$$\begin{array}{rrr|l}
x^4 & & +1 & x^2+1 \\ \cline{4-4}
-(x^4 & +x^2 &) & x^2+1 \\ \cline{1-3}
 & x^2 & +1 & \\
 & -(x^2 & +1) & \\ \cline{2-3}
 & & 0 &
\end{array}$$

Veiem que la divisió és exacta.

4. $\text{grau}(g) = 2$ i $n - k = 4 - 2 = 2$.

Torna a l'exercici (p.111)

Solució de l'Exercici 83

1. Per analitzar G_1 i G_2, considerem $Q = \begin{pmatrix} 1 & 2 & 4 & 0 \\ 0 & 1 & 2 & 4 \\ 0 & 0 & 1 & 2 \\ 0 & 0 & 0 & 1 \end{pmatrix}$

   Observem que la forma de precascada de G_1 és

$$Q \cdot G_1 = \begin{pmatrix} 1 & 2 & 4 & 0 \\ 0 & 1 & 2 & 4 \\ 0 & 0 & 1 & 2 \\ 0 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 & 0 & 2 & 4 \\ 0 & 1 & 0 & 0 & 0 & 6 \\ 0 & 0 & 1 & 0 & 6 & 0 \\ 0 & 0 & 0 & 1 & 2 & 4 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 4 & 0 & 5 & 2 \\ 0 & 1 & 2 & 4 & 6 & 1 \\ 0 & 0 & 1 & 2 & 3 & 1 \\ 0 & 0 & 0 & 1 & 2 & 4 \end{pmatrix}$$

   Com que la forma de precascada de G_1 no té forma de cascada, G_1 no genera un codi cíclic.

2. De la seva banda, la forma de precascada de G_2 és

$$Q \cdot G_2 = \begin{pmatrix} 1 & 2 & 4 & 0 \\ 0 & 1 & 2 & 4 \\ 0 & 0 & 1 & 2 \\ 0 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 & 0 & 2 & 4 \\ 0 & 1 & 0 & 0 & 6 & 0 \\ 0 & 0 & 1 & 0 & 0 & 6 \\ 0 & 0 & 0 & 1 & 2 & 4 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 4 & 0 & 0 & 0 \\ 0 & 1 & 2 & 4 & 0 & 0 \\ 0 & 0 & 1 & 2 & 4 & 0 \\ 0 & 0 & 0 & 1 & 2 & 4 \end{pmatrix}$$

   En aquest cas, la forma de precascada de G_2 té forma de cascada. Per veure si G_2 genera un codi cíclic, quedarà veure si $1 + 2x + 4x^2$ divideix $x^6 - 1$.

$$\begin{array}{r|l}
x^6 \qquad\qquad\qquad\qquad\qquad\qquad +6 & 4x^2 + 2x + 1 \\ \cline{2-2}
-(x^6 + 4x^5 + 2x^4 \qquad\qquad\qquad\quad) & 2x^4 + 6x^3 \quad + 2x + 6 \\ \cline{1-1}
3x^5 + 5x^4 \qquad\qquad\qquad +6 & \\
-(3x^5 + 5x^4 + 6x^3 \qquad\qquad\quad) & \\ \cline{1-1}
x^3 \qquad\qquad +6 & \\
-(x^3 + 4x^2 + 2x \quad) & \\ \cline{1-1}
3x^2 + 5x + 6 & \\
-(3x^2 + 5x + 6) & \\ \cline{1-1}
0 &
\end{array}$$

   Com que la divisió és exacta, concloem que G_2 genera un codi cíclic.

3. Consider $Q_3 = \begin{pmatrix} 1 & 2 & 4 \\ 0 & 1 & 2 \\ 0 & 0 & 1 \end{pmatrix}$

   Observem que la forma de precascada de G_3 és

$$Q_3 \cdot G_3 = \begin{pmatrix} 1 & 2 & 4 \\ 0 & 1 & 2 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 & 6 & 0 \\ 0 & 1 & 0 & 0 & 6 \\ 0 & 0 & 1 & 2 & 4 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 4 & 0 & 0 \\ 0 & 1 & 2 & 4 & 0 \\ 0 & 0 & 1 & 2 & 4 \end{pmatrix}$$

   Tornem a tenir el cas en què la forma de precascada de G_3 té forma de cascada. Per veure si G_3 genera un codi cíclic, quedarà veure si $1 + 2x + 4x^2$ divideix $x^5 - 1$.

$$
\begin{array}{rrrrrr|l}
x^5 & & & & & +6 & 4x^2+2x+1 \\
\hline
-(x^5 & +4x^4 & +2x^3 & & &) & 2x^3+6x^2+2 \\
\cline{1-6}
 & 3x^4 & +5x^3 & & & +6 & \\
 & -(3x^4 & +5x^3 & +6x^2 & &) & \\
\cline{2-6}
 & & & x^2 & & +6 & \\
 & & & -(x^2 & +4x & +2) & \\
\cline{4-6}
 & & & & 3x & +4 &
\end{array}
$$

Com que en aquest cas la divisió no és exacta, G_3 tampoc generarà un codi cíclic.

Podem veure, per exemple, que la paraula (40012), que és desplaçament circular de (12400), no pertany al codi i, per tant, efectivament, el codi no pot ser cíclic.

Perquè (40012) fos paraula del codi, hauria de ser de la forma

$$
\begin{pmatrix} x & y & z \end{pmatrix}
\begin{pmatrix} 1 & 2 & 4 & 0 & 0 \\ 0 & 1 & 2 & 4 & 0 \\ 0 & 0 & 1 & 2 & 4 \end{pmatrix}
= \begin{pmatrix} x & 2x+y & 4x+2y+z & 4y+2z & 4z \end{pmatrix},
$$

és a dir, s'hauria de complir

$$
\begin{array}{rcl}
x & = & 4 \\
2x+y & = & 0 \\
4x+2y+z & = & 0 \\
4y+2z & = & 1 \\
4z & = & 2
\end{array}
$$

que no té solució, perquè per satisfer les tres primeres igualtats ens caldria $x = 4$, $y = 6$, $z = 0$, però aleshores les altres igualtats no se satisfarien.

Torna a l'exercici (p.113)

Solució de l'Exercici 84

Si el codi és primitiu, aleshores $n = q - 1$.

Que $x - \beta$ divideix $x^n - 1 = x^{q-1} - 1$ és equivalent al fet que β sigui una arrel de $x^{q-1} - 1$. I sabem que qualsevol element β del cos finit de q elements satisfà $\beta^{q-1} = 1$. Per tant β és arrel de $x^{q-1} - 1$.
Torna a l'exercici (p.113)

Solució de l'Exercici 85

Es dedueix de l'exercici anterior i del fet que $(x-\alpha_1), \ldots, (x-\alpha_r)$ són tots irreductibles. Torna a l'exercici (p.113)

Solució de l'Exercici 86

1. Cal demostrar que g divideix $x^6 - 1$.

$$
\begin{array}{rrrrrrr|l}
x^6 & & & & & & +6 & x^4+4x^3+6x+3 \\
\hline
-(x^6 & +4x^5 & & +6x^3 & +3x^2 & &) & x^2+3x+2 \\
\cline{1-7}
 & 3x^5 & & +x^3 & +4x^2 & & +6 & \\
 & -(3x^5 & +5x^4 & & +4x^2 & +2x &) & \\
\cline{2-7}
 & & 2x^4 & +x^3 & & +5x & +6 & \\
 & & -(2x^4 & +x^3 & & +5x & +6) & \\
\cline{3-7}
 & & & & & & 0 &
\end{array}
$$

2. El polinomi de control serà $h(x) = (x^6 - 1)/g = x^2 + 3x + 2$.
3. La longitud és $n = 6$, perquè és un codi primitiu. La dimensió la podem deduir del fet que el grau del polinomi generador, que en el nostre cas és $\text{grau}(x^4 + 4x^3 + 6x + 3) = 4$, ha de ser $n - k = 6 - k$. Per tant, $k = 2$.
4. El polinomi generador
$$x^4 + 4x^3 + 6x + 3 = 3 + 6x + 0x^2 + 4x^3 + x^4$$
correspon a la paraula
$$(360410).$$
Pel lema fonamental dels codis cíclics, deduïm que
$$G = \begin{pmatrix} 3 & 6 & 0 & 4 & 1 & 0 \\ 0 & 3 & 6 & 0 & 4 & 1 \end{pmatrix}$$
5. Les paraules del codi seran combinacions lineals de les dues files de G, és a dir, tindran la forma
$$\begin{pmatrix} a & b \end{pmatrix}\begin{pmatrix} 3 & 6 & 0 & 4 & 1 & 0 \\ 0 & 3 & 6 & 0 & 4 & 1 \end{pmatrix} = \begin{pmatrix} 3a & 6a+3b & 6b & 4a & a+4b & b \end{pmatrix}.$$
   - Si $a = 0$ i $b \neq 0$, aleshores el pes és 4.
   - Si $a \neq 0$ i $b = 0$, aleshores el pes és 4.
   - Si $a \neq 0$ i $b \neq 0$, aleshores el pes serà com a mínim 4, ja que $3a \neq 0$, $6b \neq 0$, $4a \neq 0$, $b \neq 0$.

   Per tant, la distància mínima ha de ser 4.
6. La paraula $\begin{pmatrix} x & y & z & 2 & 3 & 5 \end{pmatrix}$ ha de ser de la forma
$$\begin{pmatrix} a & b \end{pmatrix}\begin{pmatrix} 3 & 6 & 0 & 4 & 1 & 0 \\ 0 & 3 & 6 & 0 & 4 & 1 \end{pmatrix} = \begin{pmatrix} 3a & 6a+3b & 6b & 4a & a+4b & b \end{pmatrix}.$$
De la darrera posició deduïm que $b = 5$.
De la penúltima posició deduïm que
$$a + 4b = 3 \implies a + 20 = 3 \implies a = -17 = 21 - 17 = 4.$$
La paraula del codi serà, doncs,
$$\begin{pmatrix} 4 & 5 \end{pmatrix}\begin{pmatrix} 3 & 6 & 0 & 4 & 1 & 0 \\ 0 & 3 & 6 & 0 & 4 & 1 \end{pmatrix} = \begin{pmatrix} 5 & 4 & 2 & 2 & 3 & 5 \end{pmatrix}.$$
7. Multipliquem el polinomi corresponent a la paraula (542235) pel polinomi de control i comprovem si ens dona $0 \mod x^n - 1$.
D'una banda,
$$(5 + 4x + 2x^2 + 2x^3 + 3x^4 + 5x^5)(x^2 + 3x + 2) = 5x^7 + 4x^6 + 2x + 3.$$
Si ara dividim $5x^7 + 4x^6 + 2x + 3$ entre $x^6 - 1$ ens dona quocient $5x + 4$ i residu 0:
$$\begin{array}{rrrr|l} & 5x^7 + 4x^6 & +2x+3 & & x^6 \quad +6 \\ \cline{5-5} -(5x^7 & & +2x &) & 5x+4 \\ \hline & 4x^6 & +3 & & \\ & -(4x^6 & +3) & & \\ \hline & & 0 & & \end{array}$$

Torna a l'exercici (p.115)

Solució de l'Exercici 87

1. Es pot veure que

$$\begin{pmatrix} 1&0&0&0&0&1&1&1\\ 0&1&0&0&0&1&0&0\\ 0&0&1&0&0&0&1&0\\ 0&0&0&1&0&0&0&1\\ 0&0&0&0&1&1&1&1 \end{pmatrix} \underset{\substack{f_1' = f_1+f_2+f_3+f_4+f_5\\ f_2' = f_2+f_3+f_4+f_5\\ f_3' = f_3+f_4+f_5\\ f_4' = f_4+f_5\\ f_5' = f_5}}{\sim}$$

$$\begin{pmatrix} 1&1&1&1&0&0&0&0\\ 0&1&1&1&1&0&0&0\\ 0&0&1&1&1&1&0&0\\ 0&0&0&1&1&1&1&0\\ 0&0&0&0&1&1&1&1 \end{pmatrix}$$

   Observem que aquesta matriu té forma de cascada i correspon al polinomi x^3+x^2+x+1. Si veiem que aquest polinomi divideix x^n-1, aleshores haurem demostrat que es tracta d'un codi cíclic.

$$\begin{array}{rrrrrrrrr|l}
x^8 & & & & & & & & +1 & x^3+x^2+x+1\\ \cline{10-10}
-(x^8 & +x^7 & +x^6 & +x^5 & & & & &) & x^5+x^4+x+1\\ \cline{1-9}
 & x^7 & +x^6 & +x^5 & & & & & +1 & \\
 & -(x^7 & +x^6 & +x^5 & +x^4 & & & &) & \\ \cline{2-9}
 & & & & x^4 & & & & +1 & \\
 & & & & -(x^4 & +x^3 & +x^2 & +x &) & \\ \cline{5-9}
 & & & & & x^3 & +x^2 & +x & +1 & \\
 & & & & & -(x^3 & +x^2 & +x & +1) & \\ \cline{6-9}
 & & & & & & & & 0 &
\end{array}$$

   En efecte, la divisió és exacta.

2. $g(x) = x^3+x^2+x+1$ and $h(x) = x^5+x^4+x+1$.

Torna a l'exercici (p.115)

Solució de l'Exercici 88

El residu de dividir $i(x)x^{n-k} = x^4+x^5$ entre g és $R(x) = 5x^3+x^2+x+2$:

$$\begin{array}{rrrrrr|l}
x^5 & +x^4 & & & & & x^4+4x^3+6x+3\\ \cline{7-7}
-(x^5 & +4x^4 & & +6x^2 & +3x &) & x+4\\ \cline{1-6}
 & 4x^4 & & +x^2 & +4x & & \\
 & -(4x^4 & +2x^3 & & +3x & +5) & \\ \cline{2-6}
 & & 5x^3 & +x^2 & +x & +2 &
\end{array}$$

Aleshores $i(x)x^{n-k} - R(x)$ correspon a la paraula codi 566211.

Torna a l'exercici (p.116)

Solució de l'Exercici 89

1. A la solució de l'exercici 87 hem vist que aquest és un codi cíclic i generat per $g(x) = 1 + x + x^2 + x^3$. Per tant, podem trobar una matriu de control fent la transformació genèrica de les matrius generadores del tipus $G = (I|P)$ (com aquesta), i fent servir el polinomi de control $h(x) = x^5 + x^4 + x + 1$. En el primer cas obtenim la matriu de control

$$H = \begin{pmatrix} 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 \end{pmatrix}.$$

   En el segon cas, com que $h^*(x) = 1 + x + x^4 + x^5$, obtenim la matriu de control

$$H' = \begin{pmatrix} 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \end{pmatrix}.$$

2. La distància mínima és 2 perquè a H hi ha dues columnes dependents.

3. La informació que cal codificar és $i = 10110$, que es correspon al polinomi $i(x) = 1 + x^2 + x^3$. Com que $n - k = 3$, $i(x)x^{n-k} = x^6 + x^5 + x^3$. Dividim aquest polinomi per $g(x)$ i obtenim quocient $x^3 + x + 1$ i residu 1. Per tant, $i(x)x^{n-k} - R(x) = x^6 + x^5 + x^3 + 1$, que es correspon amb la paraula 10010110.

Torna a l'exercici (p.116)

5.4 Apèndix: Repàs de més nocions de matrius

Una matriu és **quadrada** si té tantes files com columnes. La **diagonal principal** d'una matriu quadrada està formada pel primer element de la primera fila, el segon element de la segona fila, el tercer element de la tercera fila, i així fins al darrer element de la darrera fila. Una matriu quadrada és **triangular superior (o inferior)** si tots els elements que es troben per sota (o per sobre) de la diagonal principal són nuls. La primera súper-diagonal (o sub-diagonal) d'una matriu quadrada són els elements que es troben just a sobre (sota) de la diagonal principal. La segona súper-diagonal (o sub-diagonal) d'una matriu quadrada són els elements que es troben just a sobre (sota) de la primera súper-diagonal (sub-diagonal). I així es defineixen successivament totes les **súper-diagonals (o sub-diagonals)**. Per exemple, la matriu següent és triangular superior, la seva primera súper-diagonal és $1, 9$ i la seva segona súper-diagonal és 4:

$$\begin{pmatrix} 8 & 1 & 4 \\ 0 & 7 & 9 \\ 0 & 0 & 1 \end{pmatrix}.$$

Relacionat: matrius precascada (p.111)

6 Teoria de codis: matrius de Vandermonde i codis Reed-Solomon

6.1 Matrius de Vandermonde

- Les **matrius de Vandermonde** són una classe de matrius amb una estructura determinada que aporta propietats molt interessants.
- Tenen aplicacions en moltes àrees com les comunicacions digitals, el porcessat d'imatge i les antenes (MIMO), i s'empren en el càlcul de la Discrete Fourier Transform (DFT), la interpolació de funcions,...
- Nosaltres farem servir matrius de Vandermonde definides sobre un cos finit, però es poden definir sobre qualsevol cos.

Definició

Definició

Donats $v_1, v_2, \ldots, v_n \in \mathbb{F}_q$, la **matriu de Vandermonde** de $v_1, \ldots, v_n$ d'ordre r es defineix com

$$V_r(v_1, v_2, \ldots, v_n) = \begin{pmatrix} 1 & 1 & \ldots & 1 \\ v_1 & v_2 & \ldots & v_n \\ v_1^2 & v_2^2 & \ldots & v_n^2 \\ \vdots & \vdots & \vdots & \vdots \\ v_1^{r-1} & v_2^{r-1} & \ldots & v_n^{r-1} \end{pmatrix}$$

En aquest curs, només considerarem matrius de Vandermonde en les quals $v_i \neq v_j$ per tot $i \neq j$.

Exemple.

1. *Calculem* $V_3(1,2,3)$ *per* $1,2,3 \in \mathbb{F}_5$*:*

$$V_3(1,2,3) = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 2 & 3 \\ 1 & 4 & 4 \end{pmatrix}.$$

2. *Calculem* $V_3(0,1,2,3,4)$ *per* $0,1,2,3,4 \in \mathbb{F}_5$*:*

$$V_3(0,1,2,3,4) = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 2 & 3 & 4 \\ 0 & 1 & 4 & 4 & 1 \end{pmatrix}.$$

3. *Sigui* α *la classe de* x *a* $\mathbb{F}_9 = \mathbb{F}_3/(x^2+x+2)$. *Calculem* $V_4(1,\alpha,\alpha^3,\alpha^4,\alpha^6,\alpha^7)$ *a* $\mathbb{F}_9$*:*

$$V_4(1,\alpha,\alpha^3,\alpha^4,\alpha^6,\alpha^7) = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & \alpha & \alpha^3 & \alpha^4 & \alpha^6 & \alpha^7 \\ 1 & \alpha^2 & \alpha^6 & 1 & \alpha^4 & \alpha^6 \\ 1 & \alpha^3 & \alpha & \alpha^4 & \alpha^2 & \alpha^5 \end{pmatrix},$$

on hem fet servir la propietat que $\alpha^8 = 1$.

Determinants

Lema 18

El determinant de la matriu de Vandermonde $V_n(v_1, v_2, \ldots, v_n)$ és igual a

$$\det(V_n(v_1, v_2, \ldots, v_n)) = \prod_{1\le i<j\le n} (v_j - v_i)$$

Exemple. *A $\mathbb{F}_5$, la matriu $V_3(0,1,2)$ és* $\begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 2 \\ 0 & 1 & 4 \end{pmatrix}$.

El determinant de $V_3(0,1,2)$ és igual a $4-2=2$.
Fent servir el lema, el determinant és $(2-0)(2-1)(1-0)=2$.

Demostració. *La prova es pot fer per inducció en n. Per $n=2$, és senzill veure que* $\begin{vmatrix} 1 & 1 \\ v_1 & v_2 \end{vmatrix} = v_2 - v_1$.

$$\text{Per } n>2, \quad |V_n(v_1,v_2,\dots,v_n)| = \begin{vmatrix} 1 & 1 & \dots & 1 \\ v_1 & v_2 & \dots & v_n \\ v_1^2 & v_2^2 & \dots & v_n^2 \\ \vdots & \vdots & \vdots & \vdots \\ v_1^{n-1} & v_2^{n-1} & \dots & v_n^{n-1} \end{vmatrix}.$$

Per cada $i \geq 2$, podem restar a la i-èssima fila l'anterior fila multiplicada per v_1 i obtenir així

$$\begin{vmatrix} 1 & 1 & \dots & 1 \\ 0 & v_2 - v_1 & \dots & v_n - v_1 \\ 0 & v_2^2 - v_1 v_2 & \dots & v_n^2 - v_1 v_n \\ \vdots & \vdots & \vdots & \vdots \\ 0 & v_2^{n-1} - v_1 v_2^{n-2} & \dots & v_n^{n-1} - v_1 v_n^{n-2} \end{vmatrix} =$$

$$\begin{vmatrix} v_2 - v_1 & \dots & v_n - v_1 \\ v_2(v_2 - v_1) & \dots & v_n(v_n - v_1) \\ \vdots & \vdots & \vdots \\ v_2^{n-2}(v_2 - v_1) & \dots & v_n^{n-2}(v_n - v_1) \end{vmatrix}.$$

Això és igual a $(v_2 - v_1)\cdot \dots \cdot (v_n - v_1)|V_{n-1}(v_2,\dots,v_n)|$. I, per la hipòtesis d'inducció, és igual a $(v_2 - v_1)\cdot \dots \cdot (v_n - v_1)\prod_{2\leq i<j\leq n}(v_j - v_i) = \prod_{1\leq i<j\leq n}(v_j - v_i)$.

□

Exercici 90

A $\mathbb{F}_7$,

1. Calculeu la matriu de Vandermonde de rang 4 de $6,5,4,3$.
2. Calculeu el seu determinant per menors.
3. Calculeu el seu determinant fent servir el lema i comproveu que coincideixen.

Solució (p.144)

Exercici 91

A $\mathbb{F}_9 = \mathbb{Z}_3[x]/x^2+2x+2$, anomenem α a la classe de x.

1. Calculeu la matriu de Vandermonde de rang 4 de $\alpha, \alpha^3, \alpha^5, \alpha^7$.
2. Calculeu el seu determinant per menors.
3. Calculeu el seu determinant fent servir el lema i comproveu que coincideixen.

Solució (p.144)

Exercici 92

Calculeu el determinant de $V_4(1, \alpha, \alpha^3, \alpha^4)$, on α és la classe de x de $\mathbb{F}_3[x]/x^2 + x + 2$.

- Per menors .
- Pel resultat del lema.

Solució (p.145)

- Recordem que, per tot cos $\mathbb{F}$ i tot $a, b \in \mathbb{F}$, $ab = 0$ si i només si $a = 0$ o $b = 0$.
- Per tant, $\det(V_n(v_1, v_2, \ldots, v_n)) = 0$ si i només si $v_i = v_j$ per algun $i \neq j$.
- Obtenim, així, el següent corol·lari:

Corol·lari 1

La matriu $V_n(v_1, v_2, \ldots, v_n)$ és invertible si i només si $v_i \neq v_j$ per tot $1 \le i < j \le n$.

- Així, agafant $v_i \neq v_j$ per tot $1 \le i < j \le n$, podem garantir que $V_n(v_1, v_2, \ldots, v_n)$ té rang n.

Matrius de producte nul

Teorema 11

Sigui w un element primitiu de $\mathbb{F}_q$. Per tot $1 \le k \le q - 2$, el producte de les matrius

$$V_k(1, w, w^2, \ldots, w^{q-2}) \quad \text{i} \quad V_{q-1}(w, w^2, \ldots, w^{q-1-k})$$

és la matriu $k \times k$ nul·la.

Exemple. *Agafem $q = 5, k = 2$ i $w = 3$, ja que 3 és primitiu a $\mathbb{Z}_5$. Aleshores*

- $V_k(1, w, w^2, w^3) = V_2(1, 3, 3^2, 3^3) = V_2(1, 3, 4, 2) = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 3 & 4 & 2 \end{pmatrix}$
- $V_{q-1}(w, w^2, \ldots, w^{q-1-k}) = V_4(3, 3^2) = V_4(3, 4) = \begin{pmatrix} 1 & 1 \\ 3 & 4 \\ 4 & 1 \\ 2 & 4 \end{pmatrix}$
- *Ara podem comprovar que es compleix la propietat*

$$\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 3 & 4 & 2 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 3 & 4 \\ 4 & 1 \\ 2 & 4 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$

Exemple. *Agafem $q = 4, k = 1$: Per construir $\mathbb{F}_4$ ens cal un polinomi irreductible de grau 2 de $\mathbb{Z}_2[x]$. Els polinomis de grau 2 de $\mathbb{Z}_2[x]$ són únicament x^2, $x + 1$, $x^2 + x$, $x^2 + x + 1$, dels quals l'únic irreductible és $x^2 + x + 1$. Per tant, agafem $\mathbb{F}_4 = \mathbb{Z}_2[x]/x^2 + x + 1$. La classe de x, que anomenem α, compleix que $\alpha^2 = \alpha + 1$ i és, en efecte, un element primitu. Ara podem fer els càlculs:*

- $V_k(1, \alpha, \alpha^2, \ldots, \alpha^{q-2}) = V_1(1, \alpha, \alpha^2) = \begin{pmatrix} 1 & 1 & 1 \end{pmatrix}$
- $V_{q-1}(\alpha, \alpha^2, \ldots, \alpha^{q-1-k}) = V_3(\alpha, \alpha^2) = \begin{pmatrix} 1 & 1 \\ \alpha & \alpha^2 \\ \alpha^2 & \alpha \end{pmatrix}$
- *Ara podem comprovar que es compleix la propietat*

$$\begin{pmatrix} 1 & 1 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ \alpha & \alpha^2 \\ \alpha^2 & \alpha \end{pmatrix} = \begin{pmatrix} 0 & 0 \end{pmatrix}$$

Exemple. *Agafem $q = 4, k = 2$. Aleshores*

- $V_k(1,\alpha,\alpha^2,\dots,\alpha^{q-2}) = V_2(1,\alpha,\alpha^2) = \begin{pmatrix} 1 & 1 & 1 \\ 1 & \alpha & \alpha^2 \end{pmatrix}$
- $V_{q-1}(\alpha,\alpha^2,\dots,\alpha^{q-1-k}) = V_3(\alpha) = \begin{pmatrix} 1 \\ \alpha \\ \alpha^2 \end{pmatrix}$
- *Ara podem comprovar que es compleix la propietat*
$\begin{pmatrix} 1 & 1 & 1 \\ 1 & \alpha & \alpha^2 \end{pmatrix}\begin{pmatrix} 1 \\ \alpha \\ \alpha^2 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix}$

Demostració.

- *Pel lema anterior, $A = V_k(1,w,w^2,\dots,w^{q-2})$ i $B = V_{q-1}(w,w^2,\dots,w^{q-1-k})$ tenen rang màxim.*
- *Ara comprovarem que AB és la matriu nul·la. Per veure-ho, comprovarem que el producte de la fila i-èssima de A per la columna j-èssima de B és 0.*
- *Siguin i i j dos índex que satisfan $1 \le i \le k$ i $1 \le j \le q-1-k$.*
  - *La fila i-èssima de la matriu A és igual a $(1, w^{i-1}, (w^2)^{i-1}, \dots, (w^{q-2})^{i-1})$.*
  - *La columna j-èssima de B és $((w^j)^0, (w^j)^1, \dots, (w^j)^{q-1})$.*
- *El producte d'aquests dos vectors és igual a*

$$\sum_{r=1}^{q-1} w^{(i-1)(r-1)} w^{j(r-1)} = \sum_{r=1}^{q-1} w^{(i+j-1)(r-1)}.$$

- *La suma anterior és una sèrie geomètrica i, per tant, és igual a*

$$\frac{(w^{i+j-1})^{q-1} - 1}{w^{i+j-1} - 1}.$$

- *A causa de l'elecció dels valors de i i j, i pel fet que w és primitiu, sabem que $w^{i+j-1} \neq 1$ (denominador no nul).*
  Però, per altra banda, $(w^{i+j-1})^{q-1} = 1$ (numerador nul).
- *Per tant, el resultat de la suma és zero.*

□

Avaluació polinòmica

▸ ***Vector d'avaluacions d'un polinomi***

Sigui f el poliniomi definit com $f(x) = a_0 + a_1 x + \cdots + a_{n-1}x^{n-1}$, amb $a_0, \dots, a_{n-1} \in \mathbb{F}_q$.

Llavors es compleix la següent igualtat. Per tot $\beta \in \mathbb{F}_q$,

$$\begin{pmatrix} 1 & \beta & \beta^2 & \dots & \beta^{n-1} \end{pmatrix}\begin{pmatrix} a_0 \\ a_1 \\ a_2 \\ \vdots \\ a_{n-1} \end{pmatrix} = f(\beta)$$

Per tant, agafant w un element primitiu,

$$\begin{pmatrix} 1 & 1 & 1 & 1 & \dots & 1 \\ 1 & w & w^2 & w^3 & \dots & w^{(n-1)} \\ 1 & w^2 & w^4 & w^6 & \dots & w^{2(n-1)} \\ 1 & w^3 & w^6 & w^9 & \dots & w^{3(n-1)} \\ \vdots & & & & & \vdots \\ 1 & w^{n-1} & w^{2(n-1)} & w^{3(n-1)} & \dots & w^{(n-1)(n-1)} \end{pmatrix} \begin{pmatrix} a_0 \\ a_1 \\ \vdots \\ a_{n-1} \end{pmatrix} = \begin{pmatrix} f(1) \\ f(w) \\ \vdots \\ f(w^{n-1}) \end{pmatrix}.$$

▸ ***Interpolació polinòmica i matrius de Vandermonde***

Teorema 12

- Sigui $n = q-1$. Per cada vector $u = (u_0, \dots, u_{n-1}) \in \mathbb{F}_q^n$ existeix un únic polinomi f_u de grau com a molt $n-1$ que satisfà
$$f_u(w^i) = u_i$$
per tot $i \in \{0, \dots, n-1\}$.
- Aquest polinomi es pot calcular amb la fórmula
$$f_u = \sum_{i=0}^{n-1} u_i f_i \quad \text{on} \quad f_i = \prod_{\substack{j=0 \\ j \neq i}}^{n-1} \frac{x - w^j}{w^i - w^j}.$$

El polinomi del teorema és el **polinomi d'interpolació** de u.

- L'existència i unicitat de la solució és conseqüència del fet que el polinomi $f_u = a_0 + a_1 x + \cdots + a_{n-1} x^{n-1}$ està determinat per la solució del sistema lineal d'equacions
$$\begin{pmatrix} 1 & 1 & 1 & 1 & \dots & 1 \\ 1 & w & w^2 & w^3 & \dots & w^{(n-1)} \\ 1 & w^2 & w^4 & w^6 & \dots & w^{2(n-1)} \\ 1 & w^3 & w^6 & w^9 & \dots & w^{3(n-1)} \\ \vdots & & & & & \vdots \\ 1 & w^{n-1} & w^{2(n-1)} & w^{3(n-1)} & \dots & w^{(n-1)(n-1)} \end{pmatrix} \begin{pmatrix} a_0 \\ a_1 \\ \vdots \\ a_{n-1} \end{pmatrix} = \begin{pmatrix} u_0 \\ u_1 \\ \vdots \\ u_{n-1} \end{pmatrix}.$$
Aquesta és una matriu de Vandermonde quadrada i, per tant, té rang n. Així doncs, el sistema és compatible determinat.
- Per tant, per a qualsevol $u = (u_1, \dots, u_n) \in \mathbb{F}_q^n$ es compleix que
$$(u_1, \dots, u_n) = (f(1), f(w), f(w^2), \dots, f(w^{n-1}))$$
per un únic polinomi $f \in \mathbb{F}_q[x]$ de grau com a molt n.
- f_i és el polinomi d'interpolació del i-èssim vector canònic $(0, \dots, 0, 1, 0, \dots, 0)$, on l'1 es troba a la posició i-èssima.

6.2 Codis Reed-Solomon

- Van ser creats per Irving S. Reed i Gustave Solomon el 1960.
- Admeten matrius generadores del tipus Vandermonde.
- Ens centrarem en els codis Reed-Solomon (RS) que són codis cíclics primitius.
- Molt comuns: CD, DVD, Blu-Ray, QR, ADSL, DVB, HDMI, comunicacions per satèl·lit...

Matriu generadora

Definició

Sigui $n = q - 1$. Sigui w un element primitiu de $\mathbb{F}_q$. El codi **Reed-Solomon primitiu** sobre $\mathbb{F}_q$ i dimensió k és el codi lineal de $\mathbb{F}_q^n$ amb matriu generadora $G = V_k(1, w, \dots, w^{n-1})$, és a dir,

$$G = \begin{pmatrix} 1 & 1 & \dots & \dots & 1 \\ 1 & w & w^2 & \dots & w^{n-1} \\ 1 & w^2 & w^4 & \dots & w^{2(n-1)} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 1 & w^{k-1} & w^{(k-1)2} & \dots & w^{(k-1)(n-1)} \end{pmatrix}.$$

Aquest codi l'anomenem $RS_q(k)$.

Exemple ($RS_4(1)$).

- *Sigui* $\mathbb{F}_4 = \mathbb{Z}_2/(x^2+x+1)$.
- *Si* $\alpha = [x]$, *aleshores* $\mathbb{F}_4 = \{0, 1, \alpha, \alpha^2 = 1 + \alpha\}$.
- *El codi* $RS_4(1)$ *té longitud* $n = 4 - 1 = 3$ *i està generat per la matriu*

$$\begin{pmatrix} 1 & 1 & 1 \end{pmatrix}.$$

- *Per tant,* $RS_4(1) = \{(0,0,0), (1,1,1), (\alpha,\alpha,\alpha), (\alpha^2,\alpha^2,\alpha^2)\}$. *Aquest és el codi de* 3*-repetició de* $\mathbb{F}_4$*, i la seva dimensió és* $k = 1$.

Exemple ($RS_4(2)$).

- *Aquest codi també té longitud* $n = 3$ *i està generat per*

$$\begin{pmatrix} 1 & 1 & 1 \\ 1 & \alpha & \alpha^2 \end{pmatrix}.$$

- *El codi té dimensió* $k = 2$. *Té setze paraules, que s'obtenen multiplicant els següents vectors per la matriu anterior:*

$$\begin{aligned} \mathbb{F}_4^2 = \ & \{(0,0), (1,0), (\alpha,0), (\alpha^2,0), (0,1), (0,\alpha), (0,\alpha^2), \\ & (1,1), (1,\alpha), (1,\alpha^2), (\alpha,1), (\alpha,\alpha), (\alpha,\alpha^2), (\alpha^2,1), \\ & (\alpha^2,\alpha), (\alpha^2,\alpha^2)\} \end{aligned}$$

- *Les paraules són*

$$\begin{aligned} RS_4(2) = \ & \{(0,0,0), (1,1,1), (\alpha,\alpha,\alpha), (\alpha^2,\alpha^2,\alpha^2), (1,\alpha,\alpha^2), \\ & (\alpha,\alpha^2,1), (\alpha^2,1,\alpha), (0,\alpha^2,\alpha), (\alpha^2,\alpha,0), (\alpha,0,\alpha^2), \\ & (\alpha^2,0,1), (0,1,\alpha^2), (1,\alpha^2,0), (\alpha,1,0), (1,0,\alpha), \\ & (0,1,\alpha)\}. \end{aligned}$$

Matriu de control

- Pel teorema 11, els codis RS primitius tenen una matriu de control que és la matriu transposada d'una matriu Vandermonde.
- Sigui $H = V_n(w, w^2, \dots, w^{n-k})^T$, és a dir,

$$H = \begin{pmatrix} 1 & w & w^2 & \dots & w^{n-1} \\ 1 & w^2 & w^4 & \dots & w^{2(n-1)} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 1 & w^{n-k} & w^{(n-k)2} & \dots & w^{(n-k)(n-1)} \end{pmatrix}.$$

- Aquesta matriu té rang $n-k$.
- Com vam veure, el producte de G i H és la matriu nul·la.
- Per tant, $RS_q(k)$ també admet la següent definició, que és equivalent.

Definició

Donat un element primitiu $w \in \mathbb{F}_q$, el **codi Reed-Solomon primitiu** sobre $\mathbb{F}_q$ de dimensió k, $RS_q(k)$, és el codi lineal de $\mathbb{F}_q^n$ amb $n = q-1$ que té matriu de control

$$H = \begin{pmatrix} 1 & w & w^2 & \dots & w^{n-1} \\ 1 & w^2 & w^4 & \dots & w^{2(n-1)} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 1 & w^{n-k} & w^{(n-k)2} & \dots & w^{(n-k)(n-1)} \end{pmatrix}.$$

Exemple. 1. *El codi $RS_4(1)$ té matriu de control*

$$\begin{pmatrix} 1 & \alpha & \alpha^2 \\ 1 & \alpha^2 & \alpha \end{pmatrix}.$$

Podem comprovar que la síndrome dels vectors

$$RS_4(1) = \{(0,0,0),(1,1,1),(\alpha,\alpha,\alpha),(\alpha^2,\alpha^2,\alpha^2)\}$$

és el vector zero.

2. *El codi $RS_4(2)$ té matriu de control*

$$\begin{pmatrix} 1 & \alpha & \alpha^2 \end{pmatrix}.$$

Podem comprovar que la sídrome de les paraules del codi és zero.

Distància mínima

- Recordatori: Per tot codi lineal, $d \leq n-k+1$.
- Els codis en què $d = n-k+1$ s'anomenem codis Maximum Distance Separable (MDS).
- Els MDS són interessants perquè, donat n i k, garanteixen la màxima capacitat correctora.

Lema 19

La distància mínima de $RS_q(k)$ és $n-k+1$. Per tant, els codis Reed-Solomon són MDS.

Demostració. *Calculem la distància mínima a partir de H. La distància mínima és el cardinal del mínim conjunt de columnes de H que és linealment dependent.*

- *Agafem $n-k$ columnes $\{j_1,\dots,j_{n-k}\}$, amb $0 \le j_1,\dots,j_{n-k} \le n-1$.*
- *La submatriu amb aquestes columnes té determinant*

$$\begin{vmatrix} w^{j_1} & w^{j_2} & \dots & w^{j_{n-k}} \\ w^{2j_1} & w^{2j_2} & \dots & w^{2j_{n-k}} \\ w^{3j_1} & w^{3j_2} & \dots & w^{3j_{n-k}} \\ \vdots & \vdots & \vdots & \vdots \\ w^{(n-k)j_1} & w^{(n-k)j_2} & \dots & w^{(n-k)j_{n-k}} \end{vmatrix} = w^{j_1} w^{j_2} \cdot \dots \cdot w^{j_{n-k}} \cdot \left| V_{n-k}(w^{j_1}, w^{j_2}, \dots, w^{j_{n-k}}) \right|.$$

- *Per les propietats que hem vist, aquest determinant és diferent de zero. Per tant, les columnes són linealment independents.*
- *Així doncs, la distància mínima serà més gran que $n-k$.*
- *Com que les columnes són vectors de $\mathbb{F}_q^{n-k}$, qualsevol conjunt de més de $n-k$ columnes serà linealment dependent.*
- *Per tant, $d = n-k+1$.*

$\square$

Exemple. *Pels següents exemples calculem la distància de dues maneres.*

1. *La distància mínima de $RS_4(1) = \{(0,0,0),(1,1,1),(\alpha,\alpha,\alpha),(\alpha^2,\alpha^2,\alpha^2)\}$ és el pes mínim d'entre les paraules no nul·les. Aquests pesos són $3,3,3$ i, per tant, la distància mínima és 3. La distància mínima coincideix amb $n-k+1 = 3-1+1$.*

2. *Ara considerem*

$$\begin{aligned} RS_4(2) = \ & \{(0,0,0),(1,1,1),(\alpha,\alpha,\alpha),(\alpha^2,\alpha^2,\alpha^2),(1,\alpha,\alpha^2), \\ & (\alpha,\alpha^2,1),(\alpha^2,1,\alpha),(0,\alpha^2,\alpha),(\alpha^2,\alpha,0),(\alpha,0,\alpha^2), \\ & (\alpha^2,0,1),(0,1,\alpha^2),(1,\alpha^2,0),(\alpha,1,0),(1,0,\alpha), \\ & (0,1,\alpha)\}. \end{aligned}$$

   Els pesos de les paraules no nul·les són $3,3,3,3,3,3,2,2,2,2,2,2,2,2,2$. Per tant, la distància mínima és 2, que coincideix amb $n-k+1 = 3-2+1$.

Definició com a codi d'avaluació

Ara veurem una tercera defineció dels codis RS per mitjà de l'avaluació de polinomis.

- Sigui $\mathbb{F}_q[x]^{<k}$ el conjunt dels polinomis amb coeficients a $\mathbb{F}_q$ de grau inferior a k.
- Qualsevol element $a \in \mathbb{F}_q[x]^{<k}$ és del tipus

$$a = a_0 + a_1 x + a_2 x^2 + \dots + a_{k-1} x^{k-1},$$

  amb $a_i \in \mathbb{F}_q$.
- Avaluant el polinomi $a(x)$ a w^{i-1} obtenim

$$\begin{aligned} a(w^{i-1}) &= a_0 + a_1 w^{i-1} + a_2 w^{(i-1)2} + \dots + a_{k-1} w^{(i-1)(k-1)} \\ &= \begin{pmatrix} a_0 & a_1 & a_2 & \dots & a_{k-1} \end{pmatrix} \begin{pmatrix} 1 \\ w^{i-1} \\ w^{(i-1)2} \\ \vdots \\ w^{(i-1)(k-1)} \end{pmatrix} \end{aligned}$$

  que coincideix amb el resultat del producte del vector $(a_0,\dots,a_{k-1})$ per la i-èssima columna de la matriu G definida abans (G).

- Per tant, el producte del vector $(a_0, \ldots, a_{k-1})$ per la matriu G és exactament el vector $(a(1), a(w), a(w^2), \ldots, a(w^{n-1}))$.

Les propietats que hem vist abans ens permeten definir els codis Reed-Solomon primitius com el conjunt de paraules obtingudes per l'avaluació de polinomis en diversos punts:

Definició

El **codi Reed-Solomon primitiu** sobre $\mathbb{F}_q$ de dimensió k, $RS_q(k)$, és el conjunt

$$RS_q(k) = \left\{(a(1), a(w), a(w^2), \ldots, a(w^{n-1})) : a \in \mathbb{F}_q[x]^{<k}\right\},$$

on w és un element primitiu de $\mathbb{F}_q$.

Exemple.

1. *Les paraules del codi* $RS_4(1) = \{(0,0,0), (1,1,1), (\alpha,\alpha,\alpha), (\alpha^2,\alpha^2,\alpha^2)\}$ *són, respectivament, l'avaluació dels polinomis constants*

$$0, 1, \alpha, \alpha^2$$

que, com a polinomis, tenen grau inferior a 1.

2. *Les setze paraules del codi* $RS_4(2)$ *són, respectivament, l'avaluació dels polinomis*

$$0, 1, \alpha, \alpha^2$$

que, com a polinomis, tenen grau inferior a 1 *i els polinomis*

$$x, \alpha x, \alpha^2 x, x+1, \alpha x+1, \alpha^2 x+1, x+\alpha,$$
$$\alpha x+\alpha, \alpha^2 x+\alpha, x+\alpha^2, \alpha x+\alpha^2, \alpha^2 x+\alpha^2$$

que tenen grau 1.

▸ ***Detecció d'errors***

- Abans hem provat que per cada vector $u = (u_0, \ldots, u_{n-1})$ a $\mathbb{F}_q^n$ existeix un únic polinomi f_u de grau com a molt $n-1$ tal que $f_u(w^i) = u_i$ per tot $i \in \{0, \ldots, n-1\}$.
- Per tant, cada u de $\mathbb{F}_q^n$ és del tipus

$$(f(1), f(w), f(w^2), \ldots, f(w^{n-1}))$$

per un únic polinomi $f \in \mathbb{F}_q[x]$ de grau inferior a n.
- Per tant, podem **detectar** les paraules del codi amb f_u:
Un vector $u = (u_0, \ldots, u_{n-1}) \in \mathbb{F}_q^n$ és del codi si i només si el seu polinomi interpolador f_u satisfà $\text{grau}(f_u) < k$.

Definició com a codi cíclic primitiu

Encara podem definir els codis RS d'una altra manera:

- Els elements $u \in \mathbb{F}_q[x]^{<n}$ són de la forma

$$u(x) = u_0 + u_1 x + u_2 x^2 + \cdots + u_{n-1} x^{n-1}$$

amb $u_i \in \mathbb{F}_q$.

- Observem que avaluar u a w^i dona

$$\begin{array}{rcl} u(w^i) & = & u_0 + u_1 w^i + u_2 w^{i\cdot 2} + \cdots + u_{n-1} w^{i(n-1)} \\ & = & \begin{pmatrix} 1 & w^i & w^{i\cdot 2} & \ldots & w^{i(n-1)} \end{pmatrix} \begin{pmatrix} u_0 \\ u_1 \\ u_2 \\ \vdots \\ u_{n-1} \end{pmatrix} \end{array}$$

  que, si $i \leq n-k$, és exactament el producte de la fila i-èssima de H (H) pel vector $(u_0, \ldots, u_{n-1})^T$.
- Per tant, el producte de H pel vector $(u_0, \ldots, u_{n-1})^T$ és igual a

$$(u(w), u(w^2), \ldots, u(w^{n-k}))^T.$$

- Per la definició de la matriu de control, podem veure que $RS_q(k)$ és el conjunt de vectors $u = (u_0, \ldots, u_{n-1}) \in \mathbb{F}_q^n$ pels quals el polinomi

$$u_0 + u_1 x + \cdots + u_{n-1} x^{n-1}$$

  s'anul·la a w^j per tot $1 \leq j \leq n-k$.

Definició

El **codi Reed-Solomon primitiu** sobre $\mathbb{F}_q$ i dimensió k, $RS_q(k)$, és el conjunt

$$\left\{(u_0, u_1, \ldots, u_{n-1}) \in \mathbb{F}_q^n : u(w) = u(w^2) = \cdots = u(w^{n-k}) = 0\right\}.$$

Exemple.

1. *Volem comprovar si $u = (\alpha, 0, \alpha^2)$ pertany a $RS_4(1)$.*
   - *Agafem el polinomi $u(x) = \alpha \cdot 1 + 0 \cdot x + \alpha^2 \cdot x^2 = \alpha + \alpha^2 x^2$ i l'avaluem a α, α^2:*

$$\begin{array}{rcl} u(\alpha) & = & \alpha + \alpha^4 = 0, \\ u(\alpha^2) & = & \alpha + \alpha^6 = \alpha + 1 \neq 0 \end{array}$$

   Com que $u(\alpha^2) \neq 0$, u no pertany a $RS_4(1)$.
2. *Ara bé, com que $u(\alpha) = 0$, u pertany a $RS_4(2)$.*

- Per tant, les paraules es corresponen amb múltiples dels polinomis $(x - w^j)$, amb $1 \leq j \leq n-k$.
- Per tant, totes les paraules són múltiples de

$$g(x) = (x - w) \cdot \ldots \cdot (x - w^{n-k}).$$

- Com que $n = q - 1$, $g(x)$ divideix $x^n - 1$. Per tant, $RS_q(k)$ admet una altra definició equivalent:

Definició

$RS_q(k)$ és el **codi cíclic primitiu** sobre $\mathbb{F}_q$ amb polinomi generador $g(x) = (x - w) \cdot \ldots \cdot (x - w^{n-k})$.

Quatre definicions diferents per als codis RS primitius

Així doncs, hem vist quatre definicions equivalents de $RS_q(k)$.
Suposem que w és un element primitiu de $\mathbb{F}_q$.

A partir de la matriu generadora	$G = \begin{pmatrix} 1 & 1 & 1 & \dots & 1 \\ 1 & w & w^2 & \dots & w^{n-1} \\ 1 & w^2 & w^4 & \dots & w^{2(n-1)} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 1 & w^{k-1} & w^{(k-1)2} & \dots & w^{(k-1)(n-1)} \end{pmatrix}.$
A partir de la matriu de control	$H = \begin{pmatrix} 1 & w & w^2 & \dots & w^{n-1} \\ 1 & w^2 & w^4 & \dots & w^{2(n-1)} \\ 1 & w^3 & w^6 & \dots & w^{3(n-1)} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 1 & w^{n-k} & w^{(n-k)2} & \dots & w^{(n-k)(n-1)} \end{pmatrix}.$
Com a codi d'avaluació	$RS_q(k) = \left\{(a(1), a(w), a(w^2), \dots, a(w^{n-1})) : a \in \mathbb{F}_q[x]^{<k}\right\}.$
Com a codi cíclic primitiu	$g(x) = (x-w)(x-w^2)\cdot\dots\cdot(x-w^{n-k}),$ $RS_q(k) = \left\{(u_0, u_1, \dots, u_{n-1}) \in \mathbb{F}_q^n : u(w) = u(w^2) = \dots = u(w^{n-k}) = 0\right\}.$

Exercici 93

1. Comproveu que $w = 2$ és un element primitiu de $\mathbb{F}_5$.
2. Doneu una matriu generadora de $RS_5(2)$.
3. Doneu una matriu generadora de $RS_5(1)$.
4. Doneu una matriu de control de $RS_5(2)$.
5. Doneu una matriu de control de $RS_5(1)$.
6. Doneu la llista de paraules de $RS_5(2)$.
7. Doneu la llista d'elements de $\mathbb{F}_5[x]^{<2}$.
8. Digueu quina paraula de $RS_5(2)$ surt quan avaluem $3x+2$ en les potències de 2.
9. Digueu quin polinomi de $\mathbb{F}_5[x]^{<2}$, quan l'avaluem a les potències de 2, ens dona $(0,1,3,2)$.
10. Escolliu dues paraules u, v de $RS_5(2)$. Comproveu que els polinomis $u(x), v(x)$ s'anul·len quan els avaluem en $2, 2^2, \dots, 2^{n-k}$.

Solució (p.146)

Exercici 94

1. Quins ordres poden tenir els elements de $\mathbb{Z}_{13}$?
2. Comproveu que $w = 7$ és un element primitiu de $\mathbb{Z}_{13}$.
3. Doneu una taula d'equivalències de les potències de w.
4. Volem construir un codi C de Reed-Solomon primitiu sobre $\mathbb{Z}_{13}$ capaç de corregir dos errors, basat en l'element primitiu $w = 7$. Quina longitud i quina dimensió hem d'agafar?
5. Doneu el polinomi generador del codi.
6. Considerem la matriu generadora de C construïda fent servir el polinomi generador. Doneu les 3 primeres files d'aquesta matriu generadora.
7. Considerem ara la matriu generadora de C construïda fent servir l'element primitiu $w = 7$. Doneu les 3 primeres files d'aquesta matriu generadora.
8. Considerem la matriu de control H de C que s'obté fent servir l'element primitiu $w = 7$. Doneu les 3 primeres files d' H.

Solució (p.148)

Exercici 95

1. Construcció d'un cos finit.
   (a) Comproveu que el polinomi $x^3 + x + 1$ és irreductible i primitiu sobre $\mathbb{F}_2$.
   (b) Anomenem α a la classe de x dins de $\mathbb{F}_2/(x^3 + x + 1)$. Doneu-ne una taula exponencial-vectorial.
2. Definiu un codi RS primitiu sobre el cos de l'apartat anterior capaç de corregir dos errors.
   (a) Quina distància mínima hem d'agafar? Doneu-ne la longitud i la dimensió.
   (b) Doneu-ne el polinomi generador.
   (c) Doneu-ne una matriu generadora G a partir del polinomi generador.
   (d) Doneu una matriu de control H que tingui com a primera fila les potències no nul·les de α.
   (e) Calculeu el resultat de multiplicar la primera fila de G per la primera fila de H.
   (f) Calculeu $G \cdot H^T$.

Solució (p.149)

Codis RS no primitius

- Els codis Reed-Solomon que hem vist fins ara són primitius, compleixen $n = q - 1$, on q és el nombre d'elements del cos. Això permet definir-los de quatre maneres diferents i treure profit de totes les propietats que se'n deriven.
- Però, existeixen codis Reed-Solomon que no són primitius. Aquests codis no són cíclics, en general, però admeten una definició com a codi d'avaluació.
- Ara farem un incís per veure aquests codis més generals.

Definició

Siguin $w_1, \dots, w_n$ elements diferents de $\mathbb{F}_q$, i $k < n$. Aleshores diem que el conjunt de vectors

$$\{(p(w_1), p(w_2), \dots, p(w_n)) : p \in \mathbb{F}_q[x]^{<k}\}$$

és un codi Reed-Solomon.

- És un codi lineal de dimensió k i longitud n.
- En el cas que $w_i = w^{i-1}$, on w és un element primitiu de $\mathbb{F}_q$, i $q = n-1$, aquest codi és un codi $RS_q(k)$.
- Analitzant el pes de les paraules no nul·les del codi, podem veure que és un codi MDS.
- Aquests codis admeten una matriu generadora del tipus Vandermonde.

La següent referència conté molts exemples de codis RS primitius, demostracions dels resultats i proposa un algoritme de decodificació de codis RS primitius que presentem a continuació.

M. BRAS-AMORÓS. A Decoding Approach to Reed-Solomon Codes from Their Definition, *The American Mathematical Monthly*, Mathematical Association of America, vol. 125, n. 4, p. 320-338, març del 2018.

6.3 Descodificació

Correcció d'esborralls

Per corregir esborralls farem servir el mètode genèric: trobar els valors dels esborralls pels quals la síndrome del vector és el vector nul:

1. Suposem que rebem una paraula que té esborralls en les posicions $i_1, i_2, \dots, i_t$ (començant l'enumeració des de 0).
2. Sigui u la paraula rebuda, posant 0s a les posicions amb esborralls.
3. Considerem e un vector en què els elements en les posicions diferents de $i_1, i_2, \dots, i_t$ són tots zero. Els valors en les posicions $i_1, i_2, \dots, i_t$ són incògnites.
4. Buscarem el vector e tal que $u - e$ és una paraula del codi. O sigui, que $H(u-e)^T = 0$

Si fem servir la matriu de control de tipus Vandermonde $H = V_q(w, w^2, \dots, w^{n-k})^T$, es pot resoldre de la següent manera.

1. Construïm la següent matriu, que és una submatriu d'una matriu "tipus Vandermonde" de $w^{i_1}, w^{i_2}, \dots, w^{i_t}$ d'ordre t,

$$\begin{pmatrix} w^{i_1} & w^{i_2} & \dots & w^{i_t} \\ w^{2i_1} & w^{2i_2} & \dots & w^{2i_t} \\ \vdots & \vdots & \vdots & \vdots \\ w^{ti_1} & w^{ti_2} & \dots & w^{ti_t} \end{pmatrix}$$

2. Substituïm els esborralls per zero i calculem les síndromes $u(w), u(w^2), \dots, u(w^t)$.
3. Trobem els valors dels errors a través del sistema lineal

$$\begin{pmatrix} w^{i_1} & w^{i_2} & \dots & w^{i_t} \\ w^{2i_1} & w^{2i_2} & \dots & w^{2i_t} \\ \vdots & \vdots & \vdots & \vdots \\ w^{ti_1} & w^{ti_2} & \dots & w^{ti_t} \end{pmatrix} \begin{pmatrix} e_{i_1} \\ e_{i_2} \\ \vdots \\ e_{i_t} \end{pmatrix} = \begin{pmatrix} u(w) \\ u(w^2) \\ \vdots \\ u(w^t) \end{pmatrix}$$

Exercici 96

1. Comproveu que 3 és un element primitiu de $\mathbb{Z}_7$.
2. Volem construir un codi de Reed-Solomon primitiu sobre $\mathbb{Z}_7$ capaç de corregir 3 esborralls mitjançant l'element primitiu 3. Quina dimensió hem d'agafar?
3. Doneu-ne una matriu generadora.
4. Doneu-ne una matriu de control.
5. Doneu-ne un polinomi generador.
6. Corregiu els esborralls de la paraula $(5?6?4?)$
7. Trobeu el polinomi de grau menor que la dimesió que interpola la paraula corregida. Comproveu que, en efecte, el polinomi trobat interpola la paraula.

Solució (p.150)

Exercici 97

1. Digueu tots els cossos primers i tots els polinomis que podem utilitzar per construir el cos finit de 8 elements.
2. Escolliu una de les opcions de l'apartat anterior i doneu un element primitiu i la corresponent taula potencial-vectorial.
3. Doneu el polinomi generador d'un codi Reed-Solomon primitiu en sentit estricte capaç de corregir dos esborralls.
4. Quina longitud i quina dimensió té el codi?
5. Doneu una paraula no nul·la del codi.
6. Afegiu-li dos esborralls i corregiu la paraula obtinguda.

Solució (p.152)

Exercici 98

1. Comproveu que el polinomi $x^2 + x + 2$ és irreductible i primitiu a $\mathbb{Z}_3[x]$.
2. Doneu una taula exponencial-vectorial de $\mathbb{Z}_3[x]/x^2 + x + 2$, utilitzant $\alpha = [x]$.
3. Utilitzant aquest cos, construïm un codi C de Reed-Solomon primitiu en sentit estricte capaç de corregir tres esborralls en una mateixa paraula. Quina distància de disseny hem d'agafar?
4. Doneu el polinomi generador de C.
5. Quina és la dimensió de C?
6. Corregiu totes les paraules de la seqüència 0122012$??$2000000.
7. Quin polinomi generador tindrà el codi dual de C?

Solució (p.153)

Algoritme de descodificació

Algoritme

Sigui C un codi cíclic tal que $w, w^2, \dots w^{d-1}$ són les arrels del polinomi generador de C.
Input: $u \in \mathbb{F}_q^n$

1. Sigui t el mínim enter pel qual

$$\operatorname{rang}\begin{pmatrix} u(w) & \dots & u(w^t) \\ u(w^2) & \dots & u(w^{t+1}) \\ \vdots & \vdots & \vdots \\ u(w^{d-1-t}) & \dots & u(w^{d-2}) \end{pmatrix} = \operatorname{rang}\begin{pmatrix} u(w) & \dots & u(w^t) & u(w^{t+1}) \\ u(w^2) & \dots & u(w^{t+1}) & u(w^{t+2}) \\ \vdots & & \vdots & \vdots \\ u(w^{d-1-t}) & \dots & u(w^{d-2}) & u(w^{d-1}) \end{pmatrix}$$

   Aquesta t serà el nombre d'errors de u.

2. Trobem la solució $l_0, \dots, l_{t-1}$ del sistema lineal

$$\begin{pmatrix} u(w) & u(w^2) & \dots & u(w^t) \\ u(w^2) & u(w^3) & \dots & u(w^{t+1}) \\ \vdots & \vdots & \vdots & \vdots \\ u(w^t) & u(w^{t+1}) & \dots & u(w^{2t-1}) \end{pmatrix}\begin{pmatrix} l_0 \\ l_1 \\ \vdots \\ l_{t-1} \end{pmatrix} = \begin{pmatrix} -u(w^{t+1}) \\ -u(w^{t+2}) \\ \vdots \\ -u(w^{2t}) \end{pmatrix}$$

   i anomenem λ_u al polinomi $x^t + l_{t-1}x^{t-1} + \dots + l_1 x + l_0$. Diem que λ_u és el polinomi localitzador d'errors.

3. Trobem les posicions d'error a partir de les arrels de λ_u.

4. Calculem els valors dels errors per mitjà del sistema lineal

$$\begin{pmatrix} w^{i_1} & w^{i_2} & \dots & w^{i_t} \\ w^{2i_1} & w^{2i_2} & \dots & w^{2i_t} \\ \vdots & \vdots & \vdots & \vdots \\ w^{ti_1} & w^{ti_2} & \dots & w^{ti_t} \end{pmatrix}\begin{pmatrix} e_{i_1} \\ e_{i_2} \\ \vdots \\ e_{i_t} \end{pmatrix} = \begin{pmatrix} u(w) \\ u(w^2) \\ \vdots \\ u(w^t) \end{pmatrix}$$

5. ***Output:*** $c = u - e$.

▸ ***Detalls de l'algoritme***

Sigui C un codi cíclic tal que $w, w^2, \dots w^{d-1}$ són les arrels del polinomi generador de C.

Input: $u \in \mathbb{F}_q^n$

1. Sigui t el mínim enter pel qual

$$\operatorname{rang}\begin{pmatrix} u(w) & \dots & u(w^t) \\ u(w^2) & \dots & u(w^{t+1}) \\ \vdots & \vdots & \vdots \\ u(w^{d-1-t}) & \dots & u(w^{d-2}) \end{pmatrix} = \operatorname{rang}\begin{pmatrix} u(w) & \dots & u(w^{t+1}) \\ u(w^2) & \dots & u(w^{t+2}) \\ \vdots & & \vdots \\ u(w^{d-1-t}) & \dots & u(w^{d-1}) \end{pmatrix}$$

   Això vol dir:

Provem si es compleix per $t=0$: És cert que $\operatorname{rang}()=\operatorname{rang}\begin{pmatrix} u(w)\\ u(w^2)\\ \vdots\\ u(w^{d-1})\end{pmatrix}?$	$\rightarrow$	- Sí: aleshores $t=0$ - No: aleshores ho provem amb $t=1$: És cert que $\operatorname{rang}\begin{pmatrix} u(w)\\ u(w^2)\\ \vdots\\ u(w^{d-2})\end{pmatrix}=\operatorname{rang}\begin{pmatrix} u(w) & u(w^2)\\ u(w^2) & u(w^3)\\ \vdots & \vdots\\ u(w^{d-2}) & u(w^{d-1})\end{pmatrix}?$	$\rightarrow$	
- Sí: aleshores $t=1$ - No: aleshores ho provem amb $t=2$: És cert que $\operatorname{rang}\begin{pmatrix} u(w) & u(w^2)\\ u(w^2) & u(w^3)\\ \vdots & \vdots\\ u(w^{d-3}) & u(w^{d-2})\end{pmatrix}=\operatorname{rang}\begin{pmatrix} u(w) & u(w^2) & u(w^3)\\ u(w^2) & u(w^3) & u(w^4)\\ \vdots & \vdots & \vdots\\ u(w^{d-3}) & u(w^{d-2}) & u(w^{d-1})\end{pmatrix}?$	$\rightarrow$	- Sí: aleshores $t=2$ - No: aleshores ho provem amb $t=3$: ...		

Aquesta t serà el nombre d'errors de u.

2. Calculem la solució $l_0,\dots,l_{t-1}$ del sistema lineal

$$\begin{pmatrix} u(w) & u(w^2) & \dots & u(w^t)\\ u(w^2) & u(w^3) & \dots & u(w^{t+1})\\ \vdots & \vdots & \vdots & \vdots\\ u(w^t) & u(w^{t+1}) & \dots & u(w^{2t-1})\end{pmatrix}\begin{pmatrix} l_0\\ l_1\\ \vdots\\ l_{t-1}\end{pmatrix}=\begin{pmatrix} -u(w^{t+1})\\ -u(w^{t+2})\\ \vdots\\ -u(w^{2t})\end{pmatrix}$$

i anomenem λ_u al polinomi $x^t+l_{t-1}x^{t-1}+\dots+l_1x+l_0$. Diem que λ_u és el polinomi localitzador d'errors.

3. Trobem les posicions d'error a partir de les arrels de λ_u.

Si $\lambda_u(w^i)=0$ aleshores u té un error a la posició i-èsima (sempre començant per 0). Busquem les t posicions d'error, que anomenem $i_1,i_2,\dots,i_t$, de manera que compleixin

$$\lambda_u(w^{i_1})=0,\quad \lambda_u(w^{i_2})=0,\quad \dots,\quad \lambda_u(w^{i_t})=0.$$

4. Calculem els valors dels errors.

Un cop trobades les posicions d'error, $i_1,i_2,\dots,i_t$, aleshores construïm la matriu "tipus Vandermonde" (diem *tipus* perquè no és exactament Vandermonde, ja que la primera fila no és d'exponents 0, sinó d'exponents 1) de $w^{i_1},w^{i_2},\dots,w^{i_t}$ d'ordre t,

$$\begin{pmatrix} w^{i_1} & w^{i_2} & \dots & w^{i_t}\\ w^{2i_1} & w^{2i_2} & \dots & w^{2i_t}\\ \vdots & \vdots & \vdots & \vdots\\ w^{ti_1} & w^{ti_2} & \dots & w^{ti_t}\end{pmatrix}$$

i trobarem el valor dels errors per mitjà del sistema

$$\begin{pmatrix} w^{i_1} & w^{i_2} & \dots & w^{i_t}\\ w^{2i_1} & w^{2i_2} & \dots & w^{2i_t}\\ \vdots & \vdots & \vdots & \vdots\\ w^{ti_1} & w^{ti_2} & \dots & w^{ti_t}\end{pmatrix}\begin{pmatrix} e_{i_1}\\ e_{i_2}\\ \vdots\\ e_{i_t}\end{pmatrix}=\begin{pmatrix} u(w)\\ u(w^2)\\ \vdots\\ u(w^t)\end{pmatrix}$$

5. ***Output:*** $c=u-e$.

Exercici 99

Considerem el codi RS de l'Exercici 94.

1. Considerem la paraula $u = (3, 12, 0, 1, 1, 5, 3, 10, 1, 9, 1, 11)$. Si avaluem el polinomi $u(x) = 11x^{11}+x^{10}+9x^9+x^8+10x^7+3x^6+5x^5+x^4+x^3+12x+3$ en les primeres potències de w ens dona els valors següents: $u(w) = 2,\ u(w^2) = 9,\ u(w^3) = 8,\ u(w^4) = 10,\ u(w^5) = 1,\ u(w^6) = 0\dots$
   (a) Quants errors té la paraula u respecte de C?
   (b) Quin és el polinomi localitzador d'errors de u?
   (c) Quines són les posicions dels errors de u?
   (d) Quins són els valors dels errors de u?
   (e) Quina és la paraula corregida?
2. Considerem la paraula $v = (11, 11, 4, 0, 12, 1, 2, 2, 8, 5, 1, 11)$. Si avaluem el polinomi $v(x) = 11x^{11}+x^{10}+5x^9+8x^8+2x^7+2x^6+x^5+12x^4+4x^2+11x+11$ en les primeres potències de a ens dona els següents valors: $v(w) = 9,\ v(w^2) = 8,\ v(w^3) = 5,\ v(w^4) = 12,\ v(w^5) = 4,\ v(w^6) = 8\dots$
   (a) Quants errors té la paraula v respecte de C?
   (b) Quin és el polinomi localitzador d'errors de v?
   (c) Quines són les posicions dels errors de v?
   (d) Quins són els valors dels errors de v?
   (e) Quina és la paraula corregida?

Solució (p.153)

Exercici 100

1. Considerem el codi RS de l'exercici 95.
   (a) Codifiqueu de manera sistemàtica utilitzant el polinomi generador el primer bloc d'informació de la cadena de bits
   111110001111100011111111111110001010101010101010101000111111000...
   Doneu el resultat també com a cadena de bits.
   (b) Calculeu alguna síndrome de la paraula codificada.
2. Considerem el codi RS de l'exercici 95.
   (a) Rebem la cadena de bits 00110000000000010100. A quina cadena de símbols correspon?
   (b) Calculeu totes les síndromes de la paraula rebuda.
   (c) Quants errors té de símbol la paraula rebuda?
   (d) Quin és el polinomi localitzador d'errors?
   (e) Trobeu les posicions dels errors.
   (f) Calculeu el valor dels errors.
   (g) Doneu la cadena de bits corregida.
   (h) Quants errors de bit tenia la paraula enviada?

Solució (p.155)

6.4 Solucions

Solució de l'Exercici 90

1. A $\mathbb{F}_7$,
$$V_4(6,5,4,3) = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 6 & 5 & 4 & 3 \\ 6^2 & 5^2 & 4^2 & 3^2 \\ 6^3 & 5^3 & 4^3 & 3^3 \end{pmatrix} = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 6 & 5 & 4 & 3 \\ 1 & 4 & 2 & 2 \\ 6 & 6 & 1 & 6 \end{pmatrix}.$$

2. Anomenem $A = V_4(6,5,4,3)$. Els seus menors corresponents a la primera fila seran
$$A_{11} = \det\begin{pmatrix} 5 & 4 & 3 \\ 4 & 2 & 2 \\ 6 & 1 & 6 \end{pmatrix} = 60+12+48-36-10-96 = 4+5+6-1-3-5 = 6$$
$$A_{12} = \det\begin{pmatrix} 6 & 4 & 3 \\ 1 & 2 & 2 \\ 6 & 1 & 6 \end{pmatrix} = 72+3+48-36-12-24 = 2+3+6-1-5-3 = 2$$
$$A_{13} = \det\begin{pmatrix} 6 & 5 & 3 \\ 1 & 4 & 2 \\ 6 & 6 & 6 \end{pmatrix} = 144+18+60-72-72-30 = 4+4+4-2-2-2 = 6$$
$$A_{14} = \det\begin{pmatrix} 6 & 5 & 4 \\ 1 & 4 & 2 \\ 6 & 6 & 1 \end{pmatrix} = 24+24+60-96-72-5 = 3+3+4-5-2-5 = 5.$$
Per tant, $\det(A) = 1 \cdot A_{11} - 1 \cdot A_{12} + 1 \cdot A_{13} - 1 \cdot A_{14} = 6-2+6-5 = 5$.

3. Fent servir el lema,
$\det(A) = (3-4)(3-5)(3-6)(4-5)(4-6)(5-6) == (-1)(-2)(-3)(-1)(-2)(-1) = 12 = 5.$
Corroborem, per tant, que coincideixen.

Torna a l'exercici (p.128)

Solució de l'Exercici 91

0	0
1	1
α	α
α^2	$\alpha+1$
α^3	$\alpha^2+\alpha = 2\alpha+1$
α^4	$2\alpha^2+\alpha = 2$
α^5	2α
α^6	$2\alpha^2 = 2\alpha+2$
α^7	$2\alpha^2+2\alpha = \alpha+2$
α^8	$\alpha^2+2\alpha = 1$

1. $$V_4(\alpha,\alpha^3,\alpha^5,\alpha^7) = \begin{pmatrix} 1 & 1 & 1 & 1 \\ \alpha & \alpha^3 & \alpha^5 & \alpha^7 \\ (\alpha)^2 & (\alpha^3)^2 & (\alpha^5)^2 & (\alpha^7)^2 \\ (\alpha)^3 & (\alpha^3)^3 & (\alpha^5)^3 & (\alpha^7)^3 \end{pmatrix} = \begin{pmatrix} 1 & 1 & 1 & 1 \\ \alpha & \alpha^3 & \alpha^5 & \alpha^7 \\ \alpha^2 & \alpha^6 & \alpha^2 & \alpha^6 \\ \alpha^3 & \alpha & \alpha^7 & \alpha^5 \end{pmatrix}.$$

2. Anomenem $A = V_4(\alpha,\alpha^3,\alpha^5,\alpha^7)$. Els seus menors corresponents a la primera fila seran

$$\begin{aligned}
A_{11} &= \det\begin{pmatrix} \alpha^3 & \alpha^5 & \alpha^7 \\ \alpha^6 & \alpha^2 & \alpha^6 \\ \alpha & \alpha^7 & \alpha^5 \end{pmatrix} \\
&= \alpha^{3+2+5} + \alpha^{5+6+1} + \alpha^{6+7+7} - \alpha^{7+2+1} - \alpha^{6+7+3} - \alpha^{6+5+5} \\
&= \alpha^2 + \alpha^4 + \alpha^6 - \alpha^2 - \alpha^2 - \alpha^2 \\
&= \alpha^4 + \alpha^6 + \alpha^2 \\
&= (2) + (2\alpha + 2) + (\alpha + 1) = 2
\end{aligned}$$

i, de manera anàloga,

$$A_{12} = \det\begin{pmatrix} \alpha & \alpha^5 & \alpha^7 \\ \alpha^2 & \alpha^2 & \alpha^6 \\ \alpha^3 & \alpha^7 & \alpha^5 \end{pmatrix} = 1 + \alpha^6 + 1 - \alpha^4 - \alpha^4 - \alpha^6 = -\alpha^4 = 1,$$

$$A_{13} = \det\begin{pmatrix} \alpha & \alpha^3 & \alpha^7 \\ \alpha^2 & \alpha^6 & \alpha^6 \\ \alpha^3 & \alpha & \alpha^5 \end{pmatrix} = \alpha^4 + \alpha^4 + \alpha^2 - 1 - 1 - \alpha^2 = \alpha^4 = 2,$$

$$A_{14} = \det\begin{pmatrix} \alpha & \alpha^3 & \alpha^5 \\ \alpha^2 & \alpha^6 & \alpha^2 \\ \alpha^3 & \alpha & \alpha^7 \end{pmatrix} = \alpha^6 + 1 + 1 - \alpha^6 - \alpha^4 - \alpha^4 = -\alpha^4 = 1.$$

Per tant, $\det(A) = 1 \cdot A_{11} - 1 \cdot A_{12} + 1 \cdot A_{13} - 1 \cdot A_{14} = 2 - 1 + 2 - 1 = 2$.

3. Fent servir el lema,

$$\begin{aligned}
\det(A) &= (\alpha^7 - \alpha^5)(\alpha^7 - \alpha^3)(\alpha^7 - \alpha)(\alpha^5 - \alpha^3)(\alpha^5 - \alpha)(\alpha^3 - \alpha) \\
&= (\alpha + 2 - 2\alpha)(\alpha + 2 - 2\alpha - 1)(\alpha + 2 - \alpha)(2\alpha - 2\alpha - 1)(2\alpha - \alpha)(2\alpha + 1 - \alpha) \\
&= (-\alpha + 2)(-\alpha + 1)(2)(-1)(\alpha)(\alpha + 1) \\
&= (2\alpha + 2)(2\alpha + 1)(2)(2)(\alpha)(\alpha + 1) \\
&= \alpha^6\alpha^3\alpha^4\alpha^4\alpha\alpha^2 = \alpha^{6+3+4+4+1+2} = \alpha^{20} = \alpha^4 = 2
\end{aligned}$$

Corroborem, per tant, que coincideixen.

Torna a l'exercici (p.128)

Solució de l'Exercici 92

Utilitzarem la taula

pot.	pol.	vec.
0	0	00
α^0	1	10
α^1	α	01
α^2	$2\alpha + 1$	12
α^3	$2\alpha + 2$	22
α^4	2	20
α^5	2α	02
α^6	$\alpha + 2$	21
α^7	$\alpha + 1$	11

Calculem el determinant per menors:

$$\det(V_4(1,\alpha,\alpha^3,\alpha^4)) = \det\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & \alpha & \alpha^3 & \alpha^4 \\ 1 & \alpha^2 & \alpha^6 & 1 \\ 1 & \alpha^3 & \alpha & \alpha^4 \end{pmatrix} =$$

$$\det\begin{pmatrix} \alpha & \alpha^3 & \alpha^4 \\ \alpha^2 & \alpha^6 & 1 \\ \alpha^3 & \alpha & \alpha^4 \end{pmatrix} - \det\begin{pmatrix} 1 & 1 & 1 \\ \alpha^2 & \alpha^6 & 1 \\ \alpha^3 & \alpha & \alpha^4 \end{pmatrix} + \det\begin{pmatrix} 1 & 1 & 1 \\ \alpha & \alpha^3 & \alpha^4 \\ \alpha^3 & \alpha & \alpha^4 \end{pmatrix} - \det\begin{pmatrix} 1 & 1 & 1 \\ \alpha & \alpha^3 & \alpha^4 \\ \alpha^2 & \alpha^6 & 1 \end{pmatrix} =$$

$$= (\alpha^3+\alpha^6+\alpha^7-\alpha^5-\alpha-\alpha^2)-(\alpha^2+\alpha^3+\alpha^3-\alpha-\alpha-\alpha^6)+(\alpha^7+\alpha^7+\alpha^2-\alpha^6-\alpha^5-\alpha^5)-(\alpha^3+\alpha^6+\alpha^7-\alpha^5-\alpha-\alpha^2) =$$

$$= (\cancel{\alpha^3}+\cancel{\alpha^6}+\cancel{\alpha^7}-\cancel{\alpha^5}-\cancel{\alpha}-\cancel{\alpha^2})-(\cancel{\alpha^2}+\cancel{\alpha^3}+\alpha^3-\cancel{\alpha}-\alpha-\cancel{\alpha^6})+(\alpha^7+\alpha^7+\cancel{\alpha^2}-\cancel{\alpha^6}-\alpha^5-\alpha^5)-(\alpha^3+\cancel{\alpha^6}+\cancel{\alpha^7}-\cancel{\alpha^5}-\alpha-\cancel{\alpha^2}) =$$

$$= -\alpha^3+\alpha+\alpha^7+\alpha^7-\alpha^5-\alpha^5-\alpha^3+\alpha = (\alpha+\alpha)+(\alpha^7+\alpha^7)-(\alpha^3+\alpha^3)-(\alpha^5+\alpha^5) = \alpha^4\alpha+\alpha^4\alpha^7+\alpha^3+\alpha^5 =$$
$$= \alpha^5+\alpha^3+\alpha^3+\alpha^5 = (\alpha^5+\alpha^5)+(\alpha^3+\alpha^3) = \alpha+\alpha^7$$

veiem que el determinant és α^2.

Calculem el determinant pel lema:

$$(1-\alpha)(1-\alpha^3)(1-\alpha^4)(\alpha-\alpha^3)(\alpha-\alpha^4)(\alpha^3-\alpha^4) = \alpha^2\alpha^6\alpha^4\alpha^2\alpha^7\alpha^5 = \alpha^2.$$

Observem com els dos càlculs coincideixen.

Torna a l'exercici (p.129)

Solució de l'Exercici 93

1. L'element 2 és primitiu. En efecte, les seves potències són totes diferents fins a exponent $q-1=4$.

$$2^0 = 1,\ 2^1 = 2,\ 2^2 = 4,\ 2^3 = 3,\ 2^4 = 1.$$

2. Una matriu generadora de $RS_5(2)$ és

$$\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 2 & 4 & 3 \end{pmatrix}.$$

3. Una matriu generadora de $RS_5(1)$ és

$$\begin{pmatrix} 1 & 1 & 1 & 1 \end{pmatrix}.$$

4. En aquest cas, $n-k = 4-2 = 2$. Per això la matriu de control de $RS_5(2)$ tindrà 2 files i és aquesta matriu:

$$\begin{pmatrix} 1 & 2 & 4 & 3 \\ 1 & 4 & 1 & 4 \end{pmatrix}.$$

5. En aquest cas, $n-k = 4-1 = 3$. Per això la matriu de control de $RS_5(1)$ tindrà 2 files i és aquesta matriu:

$$\begin{pmatrix} 1 & 2 & 4 & 3 \\ 1 & 4 & 1 & 4 \\ 1 & 3 & 4 & 2 \end{pmatrix}.$$

6. La llista de paraules de $RS_5(2)$ és el conjunt de combinacions lineals de les files de
$$\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 2 & 4 & 3 \end{pmatrix}$$
Són:

$$\begin{aligned}
0(1111)+0(1243) &= (0000)\\
0(1111)+1(1243) &= (1243)\\
0(1111)+2(1243) &= (2431)\\
0(1111)+3(1243) &= (3124)\\
0(1111)+4(1243) &= (4312)\\
1(1111)+0(1243) &= (1111)\\
1(1111)+1(1243) &= (2304)\\
1(1111)+2(1243) &= (3042)\\
1(1111)+3(1243) &= (4230)\\
1(1111)+4(1243) &= (0423)\\
2(1111)+0(1243) &= (2222)\\
2(1111)+1(1243) &= (3410)\\
2(1111)+2(1243) &= (4103)
\end{aligned}
\qquad
\begin{aligned}
2(1111)+3(1243) &= (0341)\\
2(1111)+4(1243) &= (1034)\\
3(1111)+0(1243) &= (3333)\\
3(1111)+1(1243) &= (4021)\\
3(1111)+2(1243) &= (0214)\\
3(1111)+3(1243) &= (1402)\\
3(1111)+4(1243) &= (2140)\\
4(1111)+0(1243) &= (4444)\\
4(1111)+1(1243) &= (0132)\\
4(1111)+2(1243) &= (1320)\\
4(1111)+3(1243) &= (2013)\\
4(1111)+4(1243) &= (3201)
\end{aligned}$$

7. $\mathbb{F}_5[x]^{<2} = \{0,1,2,3,4,x,x+1,x+2,x+3,x+4,2x,2x+1,2x+2,2x+3,2x+4,3x,3x+1,3x+2,3x+3,3x+4,4x,4x+1,4x+2,4x+3,4x+4\}$.

8. Hem d'avaluar $a(x) = 3x+2$ en els valors
$$2^0 = 1,\ 2^1 = 2,\ 2^2 = 4,\ 2^3 = 3.$$
Ens queda
$$(a(1),a(2),a(4),a(3)) = (3\cdot 1+2, 3\cdot 2+2, 3\cdot 4+2, 3\cdot 3+2) = (0,3,4,1),$$
que, efectivament, és a la llista de paraules de $RS_5(2)$ que hem vist anteriorment.

9. Volem veure si podem interpolar el vector $(0,1,3,2)$ per un polinomi de $\mathbb{F}_5[x]^{<2}$.
Busquem $a = a_1x + a_0$ tal que
$$\begin{aligned}
a(2^0) = a(1) = a_1 + a_0 &= 0\\
a(2^1) = a(2) = 2a_1 + a_0 &= 1\\
a(2^2) = a(4) = 4a_1 + a_0 &= 3\\
a(2^3) = a(3) = 3a_1 + a_0 &= 2
\end{aligned}$$
Restant la primera equació a la segona obtenim que $a_1 = 1$. De la primera equació, deduïm que $a_0 = -1 = 4$. I veiem que aquesta solució és compatible amb les equacions tercera i quarta.
El polinomi buscat és, doncs, $a(x) = x+4$.

10. • Escollim la paraula $u = (2,0,1,3)$. Tindrem $u(x) = 2 + x^2 + 3x^3$. Com que $n = 4$ i $k = 2$, tindrem $n-k = 2$ i hem d'avaluar $u(x)$ en $2^1 = 2$ i $2^2 = 4$.
$$\begin{aligned}
u(2) &= 2+2^2+3\cdot 2^3 = 2+4+4 = 0\\
u(4) &= 2+4^2+3\cdot 4^3 = 2+1+2 = 0
\end{aligned}$$

Comprovem que, quan avaluem $u(x)$ en 2^1 i 2^2, dona 0 i, per tant, en efecte, u és una paraula de $RS_5(2)$.

- Escollim la paraula $v = (4, 1, 0, 3)$. Tindrem $v(x) = 4 + x + 3x^3$. Com que $n = 4$ i $k = 2$, tindrem $n - k = 2$ i hem d'avaluar $v(x)$ en $2^1 = 2$ i $2^2 = 4$.

$$\begin{aligned} v(2) &= 4 + 2 + 3 \cdot 2^3 = 4 + 2 + 4 = 0 \\ v(4) &= 4 + 4 + 3 \cdot 4^3 = 4 + 4 + 2 = 0 \end{aligned}$$

Comprovem que, quan avaluem $v(x)$ en 2^1 i 2^2, dona 0 i, per tant, en efecte, v és una paraula de $RS_5(2)$.

Torna a l'exercici (p.137)

Solució de l'Exercici 94

1. Els elements de $\mathbb{Z}_{13}$ poden tenir ordre 1, 2, 3, 4, 6, 12.
2. Les primeres potències de 7 són

7^0	1
7^1	$7 \neq 1$
7^2	$49 = 10 \neq 1$
7^3	$70 = 5 \neq 1$
7^4	$35 = 9 \neq 1$
7^5	$63 = 11 \neq 1$
7^6	$77 = 12 \neq 1$

Així veiem que l'ordre de 7 no és ni 1, ni 2, ni 3, ni 4, ni 6 i, per tant, ha de ser 12.

3.

7^0	1
7^1	7
7^2	10
7^3	5
7^4	9
7^5	11
7^6	12
7^7	$84 = 6$
7^8	$42 = 3$
7^9	$21 = 8$
7^{10}	$56 = 4$
7^{11}	$28 = 2$
7^{12}	$14 = 1$

També hauríem pogut utilitzar que $7^6 = -1$:

7^0	1
7^1	7
7^2	10
7^3	5
7^4	9
7^5	11
7^6	12
7^7	$7^6 \cdot 7 = -7 = 6$
7^8	$7^6 \cdot 7^2 = -10 = 3$
7^9	$7^6 \cdot 7^3 = -5 = 8$
7^{10}	$7^6 \cdot 7^4 = -9 = 4$
7^{11}	$7^6 \cdot 7^5 = -11 = 2$
7^{12}	$7^6 \cdot 7^7 = (-1)^2 = 1$

4. Per poder corregir dos errors hem d'agafar $d = 5$. Aleshores la longitud i la dimensió són

$$n = q - 1 = 12,$$

$$k = n - d + 1 = 8.$$

5. El polinomi generador és $(x-7)(x-7^2)(x-7^3)(x-7^4) = (x-7)(x-10)(x-5)(x-9) = x^4+(-7-10-5-9)x^3+(7\cdot10+7\cdot5+7\cdot9+10\cdot5+10\cdot9+5\cdot9)x^2+(-7\cdot10\cdot5-7\cdot10\cdot9-7\cdot5\cdot9-10\cdot5\cdot9)x+7\cdot10\cdot5\cdot9 = x^4+8x^3+(5+9+11+11+12+6)x^2+(-5\cdot5-5\cdot9-9\cdot9-11\cdot9)x+5\cdot6 = x^4+8x^3+2x^2+(1+7+10+5)x+4 = x^4+8x^3+2x^2+10x+4$.

6. Utilitzant el polinomi generador obtenim

$$\begin{pmatrix} 4 & 10 & 2 & 8 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 4 & 10 & 2 & 8 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 4 & 10 & 2 & 8 & 1 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

7.

$$\begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 7 & 7^2 & 7^3 & 7^4 & 7^5 & 7^6 & 7^7 & 7^8 & 7^9 & 7^{10} & 7^{11} \\ 1 & 7^2 & 7^4 & 7^6 & 7^8 & 7^{10} & 1 & 7^2 & 7^4 & 7^6 & 7^8 & 7^{10} \end{pmatrix} =$$

$$\begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 7 & 10 & 5 & 9 & 11 & 12 & 6 & 3 & 8 & 4 & 2 \\ 1 & 10 & 9 & 12 & 3 & 4 & 1 & 10 & 9 & 12 & 3 & 4 \end{pmatrix}$$

8.

$$\begin{pmatrix} 1 & 7 & 7^2 & 7^3 & 7^4 & 7^5 & 7^6 & 7^7 & 7^8 & 7^9 & 7^{10} & 7^{11} \\ 1 & 7^2 & 7^4 & 7^6 & 7^8 & 7^{10} & 7 & 7^2 & 7^4 & 7^6 & 7^8 & 7^{10} \\ 1 & 7^3 & 7^6 & 7^9 & 1 & 7^3 & 7^6 & 7^9 & 1 & 7^3 & 7^6 & 7^9 \end{pmatrix} =$$

$$\begin{pmatrix} 1 & 7 & 10 & 5 & 9 & 11 & 12 & 6 & 3 & 8 & 4 & 2 \\ 1 & 10 & 9 & 12 & 3 & 4 & 1 & 10 & 9 & 12 & 3 & 4 \\ 1 & 5 & 12 & 8 & 1 & 5 & 12 & 8 & 1 & 5 & 12 & 8 \end{pmatrix}$$

Torna a l'exercici (p.138)

Solució de l'Exercici 95

1. És irreductible perquè té grau 3 i no té arrels. És primitiu perquè l'ordre de la classe de x, que anomenem α, és $q-1=7$, com es pot desprendre de la taula:

exp.	*vect.*
α	010
α^2	001
α^3	110
α^4	011
α^5	111
α^6	101
α^7	100

2. (a) Hem d'agafar $d=5$. La longitud és $n=q-1=7$ i la dimensió és $k=n-d+1=3$.

   (b) El polinomi generador serà $(x-\alpha)(x-\alpha^2)(x-\alpha^3)(x-\alpha^4)=x^4-(\alpha+\alpha^2+\alpha^3+\alpha^4)x^3+(\alpha\alpha^2+\alpha\alpha^3+\alpha\alpha^4+\alpha^2\alpha^3+\alpha^2\alpha^4+\alpha^3\alpha^4)x^2-(\alpha^2\alpha^3\alpha^4+\alpha\alpha^3\alpha^4+\alpha\alpha^2\alpha^4+\alpha\alpha^2\alpha^3)x+\alpha\alpha^2\alpha^3\alpha^4=x^4+\alpha^3x^3+x^2+\alpha x+\alpha^3$.

   (c)
$$G=\begin{pmatrix} \alpha^3 & \alpha & 1 & \alpha^3 & 1 & 0 & 0 \\ 0 & \alpha^3 & \alpha & 1 & \alpha^3 & 1 & 0 \\ 0 & 0 & \alpha^3 & \alpha & 1 & \alpha^3 & 1 \end{pmatrix}$$

   (d)
$$H=\begin{pmatrix} 1 & \alpha & \alpha^2 & \alpha^3 & \alpha^4 & \alpha^5 & \alpha^6 \\ 1 & \alpha^2 & \alpha^4 & \alpha^6 & \alpha & \alpha^3 & \alpha^5 \\ 1 & \alpha^3 & \alpha^6 & \alpha^2 & \alpha^5 & \alpha & \alpha^4 \\ 1 & \alpha^4 & \alpha & \alpha^5 & \alpha^2 & \alpha^6 & \alpha^3 \end{pmatrix}$$

   (e) $\alpha^3+\alpha^2+\alpha^2+\alpha^6+\alpha^4=0$

   (f)
$$G\cdot H^T=\begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

Torna a l'exercici (p.138)

Solució de l'Exercici 96

1. Podem veure que les potències d'exponents $0,1,\dots,5$ són totes diferents: $3^0=1$, $3^1=3$, $3^2=2$, $3^3=6$, $3^4=4$, $3^5=5$.

2. D'una banda, la longitud haurà de ser $7-1=6$. Hem de garantir que $d-1$ sigui més gran o igual que 3, i, per tant, $d\geq 4$. Com que en els codis Reed-Solomon $d=n-k+1$, podem agafar $k=n-4+1=3$.

3. Una matriu generadora serà
$$\begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 3 & 2 & 6 & 4 & 5 \\ 1 & 2 & 4 & 1 & 2 & 4 \end{pmatrix}$$

4. Una matriu de control serà
$$\begin{pmatrix} 1 & 3 & 2 & 6 & 4 & 5 \\ 1 & 2 & 4 & 1 & 2 & 4 \\ 1 & 6 & 1 & 6 & 1 & 6 \end{pmatrix}$$

5. El polinomi generador serà $g(x)=(x-3)(x-3^2)(x-3^3)=(x-3)(x-2)(x-6)=x^3+(-3-2-6)x^2+(3\cdot 2+3\cdot 6+2\cdot 6)x+(-3\cdot 2\cdot 6)=x^3+3x^2+x+6$.

6. Substituïm els esborralls per zero i obtenim el polinomi associat a la paraula: $u(x) = 5 + 6x^2 + 4x^4$. Calculem les síndromes: $u(3) = 5+6\cdot 2+4\cdot 4 = 5+5+2 = 5$, $u(3^2) = u(2) = 5+6\cdot 4+4\cdot 2 = 5+3+1 = 2$, $u(3^3) = u(6) = u(-1) = 5 + 6 + 4 = 1$.

   Resolem el sistema
$$\begin{pmatrix} 3^1 & 3^3 & 3^5 \\ (3^1)^2 & (3^3)^2 & (3^5)^2 \\ (3^1)^3 & (3^3)^3 & (3^5)^3 \end{pmatrix}\begin{pmatrix} e_1 \\ e_3 \\ e_5 \end{pmatrix} = \begin{pmatrix} u(3) \\ u(3^2) \\ u(3^3) \end{pmatrix}$$

   És a dir,
$$\begin{pmatrix} 3 & 6 & 5 \\ 2 & 1 & 4 \\ 6 & 6 & 6 \end{pmatrix}\begin{pmatrix} e_1 \\ e_3 \\ e_5 \end{pmatrix} = \begin{pmatrix} 5 \\ 2 \\ 1 \end{pmatrix}.$$

   La solució del sistema la podem trobar, per exemple, invertint la matriu del sistema.

$$\begin{aligned}\begin{pmatrix} 3 & 6 & 5 \\ 2 & 1 & 4 \\ 6 & 6 & 6 \end{pmatrix}^{-1} &= \frac{1}{4+4+4-2-2-2}\begin{pmatrix} +3 & -2 & +6 \\ -6 & +2 & -3 \\ +5 & -2 & +5 \end{pmatrix}^T \\ &= \frac{1}{6}\begin{pmatrix} 3 & 5 & 6 \\ 1 & 2 & 4 \\ 5 & 5 & 5 \end{pmatrix}^T \\ &= 6\begin{pmatrix} 3 & 1 & 5 \\ 5 & 2 & 5 \\ 6 & 4 & 5 \end{pmatrix} \\ &= \begin{pmatrix} 4 & 6 & 2 \\ 2 & 5 & 2 \\ 1 & 3 & 2 \end{pmatrix}\end{aligned}$$

   Llavors la solució del sistema serà

$$\begin{pmatrix} e_1 \\ e_3 \\ e_5 \end{pmatrix} = \begin{pmatrix} 4 & 6 & 2 \\ 2 & 5 & 2 \\ 1 & 3 & 2 \end{pmatrix}\begin{pmatrix} 5 \\ 2 \\ 1 \end{pmatrix} = \begin{pmatrix} 6 \\ 1 \\ 6 \end{pmatrix}$$

   Per tant, deduïm que la paraula enviada era $(5,0,6,0,4,0) - (0,6,0,1,0,6) = (5,1,6,6,4,1)$.

7. Hem de resoldre el sistema

$$\begin{pmatrix} a_0 & a_1 & a_2 \end{pmatrix}\begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 3 & 2 & 6 & 4 & 5 \\ 1 & 2 & 4 & 1 & 2 & 4 \end{pmatrix} = \begin{pmatrix} 5 & 1 & 6 & 6 & 4 & 1 \end{pmatrix}.$$

   El podem resoldre a partir de la primera submatriu:

$$\begin{pmatrix} a_0 & a_1 & a_2 \end{pmatrix}\begin{pmatrix} 1 & 1 & 1 \\ 1 & 3 & 2 \\ 1 & 2 & 4 \end{pmatrix} = \begin{pmatrix} 5 & 1 & 6 \end{pmatrix}.$$

Calculem la matriu inversa de la matriu del sistema:

$$\begin{aligned}\begin{pmatrix}1&1&1\\1&3&2\\1&2&4\end{pmatrix}^{-1} &= \frac{1}{5+2+2-3-4-4}\begin{pmatrix}+1&-2&+6\\-2&+3&-1\\+6&-1&+2\end{pmatrix}^{T}\\ &= \frac{1}{5}\begin{pmatrix}1&5&6\\5&3&6\\6&6&2\end{pmatrix}\\ &= \begin{pmatrix}3&1&4\\1&2&4\\4&4&6\end{pmatrix}\end{aligned}$$

Aleshores, la solució del sistema serà

$$\begin{pmatrix}a_0&a_1&a_2\end{pmatrix}=\begin{pmatrix}5&1&6\end{pmatrix}\begin{pmatrix}3&1&4\\1&2&4\\4&4&6\end{pmatrix}=\begin{pmatrix}5&3&4\end{pmatrix}$$

i deduïm que el polinomi interpolador és $f = 4x^2 + 3x + 5$. Si ara l'avaluem a totes les potències de 3 obtenim $(f(3^0), f(3^1), f(3^2), f(3^3), f(3^4), f(3^5)) = (f(1), f(3), f(2), f(6), f(4), f(5)) = (5, 1, 6, 6, 4, 1)$, que comprovem que és la paraula corregida.

Torna a l'exercici (p.140)

Solució de l'Exercici 97

1. El cos primer ha de ser $\mathbb{Z}_2$ i els polinomis han de ser $x^3 + x^2 + 1$ o bé $x^3 + x + 1$, ja que són els únics polinomis de $\mathbb{Z}_2$ irreductibles de grau 3.

2. En els dos casos $\alpha = [x]$ és un element primitiu.

   La taula potencial-vectorial per a $\mathbb{Z}_2/x^3 + x^2 + 1$ és

0	000
α^0	100
α^1	010
α^2	001
α^3	101
α^4	111
α^5	110
α^6	011

   La taula potencial-vectorial per a $\mathbb{Z}_2/x^3 + x + 1$ és

0	000
α^0	100
α^1	010
α^2	001
α^3	110
α^4	011
α^5	111
α^6	101

3. Considerarem la segona construcció de $\mathbb{F}_8$. Per corregir dos esborralls cal una distància mínima ≥ 3. Agafem $d = 3$. El polinomi generador serà $g(x) = (x - \alpha)(x - \alpha^2) = x^2 + \alpha^4 x + \alpha^3$.

4. La longitud és $8 - 1 = 7$. La dimensió és $7 - \text{grau}(g) = 7 - 2 = 5$.

5. Com a paraula no nul·la del codi podem agafar $(0\alpha^3\alpha^4 1000)$, que correspon al polinomi $x \cdot g$.

6. Posem esborralls a les posicions primera i segona. Obtenim $(??\alpha^4 1000)$. El polinomi corresponent a la paraula rebuda, si substituïm els esborralls per zero, és $u(x) = \alpha^4 x^2 + x^3$.

   Resolem el sistema $\begin{pmatrix} 1 & \alpha \\ 1 & \alpha^2 \end{pmatrix}\begin{pmatrix} e_0 \\ e_1 \end{pmatrix} = \begin{pmatrix} u(\alpha) \\ u(\alpha^2) \end{pmatrix} = \begin{pmatrix} \alpha^4 \\ \alpha^5 \end{pmatrix}$ i obtenim que $e_0 = 0$ i $e_1 = \alpha^3$.

   Per tant, la paraula enviada ha de ser $(00\alpha^4 1000) - (0\alpha^3 00000) = (0\alpha^3\alpha^4 1000)$.

Torna a l'exercici (p.140)

Solució de l'Exercici 98

1. El polinomi és irreductible perquè té grau 2 i no té arrels ($f(0) = 2$, $f(1) = 1$ i $f(2) = 2$).

2.

0	00
1	10
α	01
α^2	12
α^3	22
α^4	20
α^5	02
α^6	21
α^7	11

3. Hem d'agafar distància prevista 4.

4. $g(x) = (x - \alpha)(x - \alpha^2)(x - \alpha^3) = x^3 + \alpha x^2 + \alpha^7 x + \alpha^2$.

5. La dimensió serà $n - \text{grau}(g) = 5$.

6. Tenim la paraula amb esborralls $(\alpha\alpha^3\alpha??000)$. El polinomi corresponent és $u(x) = \alpha x^2 + \alpha^3 x + \alpha$. Calculem $u(\alpha) = \alpha^3 + \alpha^4 + \alpha = 1$, $u(\alpha^2) = \alpha^5 + \alpha^5 + \alpha = \alpha^5$ i resolem el sistema $\begin{pmatrix} \alpha^3 & \alpha^4 \\ \alpha^6 & 1 \end{pmatrix}\begin{pmatrix} e_3 \\ e_4 \end{pmatrix} = \begin{pmatrix} 1 \\ \alpha^5 \end{pmatrix}$, d'on deduïm que $e_3 = \alpha^2$ i $e_4 = \alpha^3$. Per tant, la paraula corregida és $(\alpha, \alpha^3, \alpha, \alpha^6, \alpha^7, 0, 0, 0)$ corresponent a (0122012111000000).

7. El polinomi de control és $(x^8 - 1)/g = x^5 + \alpha^5 x^4 + \alpha x^3 + \alpha^3 x^2 + \alpha^3 x + \alpha^2$. El seu recíproc serà el generador del codi dual i és exactament $h* = \alpha^2 x^5 + \alpha^3 x^4 + \alpha^3 x^3 + \alpha x^2 + \alpha^5 x + 1$.

Torna a l'exercici (p.140)

Solució de l'Exercici 99

1. (a) El vector de síndromes de u és $\begin{pmatrix} 2 \\ 9 \\ 8 \\ 10 \end{pmatrix} = \begin{pmatrix} 7^{11} \\ 7^4 \\ 7^9 \\ 7^2 \end{pmatrix}$.

   Tenim $\text{rang}() \neq \text{rang}\begin{pmatrix} 2 \\ 9 \\ 8 \\ 10 \end{pmatrix}$. Per això sabem que s'ha produït com a mínim un error.

   Ara hem de veure si $\text{rang}\begin{pmatrix} 2 \\ 9 \\ 8 \end{pmatrix} = \text{rang}\begin{pmatrix} 2 & 9 \\ 9 & 8 \\ 8 & 10 \end{pmatrix}$.

   Observem que $\begin{pmatrix} 2 & 9 \\ 9 & 8 \\ 8 & 10 \end{pmatrix} = \begin{pmatrix} 7^{11} & 7^4 \\ 7^4 & 7^9 \\ 7^9 & 7^2 \end{pmatrix}$.

Com que $7^5\begin{pmatrix}7^{11}\\7^4\\7^9\end{pmatrix}=\begin{pmatrix}7^4\\7^9\\7^2\end{pmatrix}$, tenim que $\operatorname{rang}\begin{pmatrix}7^{11}\\7^4\\7^9\end{pmatrix}=\operatorname{rang}\begin{pmatrix}7^{11}&7^4\\7^4&7^9\\7^9&7^2\end{pmatrix}=1$.

Deduïm que s'ha produït un error.

(b) Hem de resoldre el sistema $7^{11}l_0=-7^4=7^6 7^4=7^{10}$, que té solució $l_0=7^{10-11}=7^{-1}=7^{11}=2$. Per tant, el polinomi localitzador d'errors és $x+2$.

(c) L'única arrel del polinomi localitzador d'errors és $x=-2=11=7^5$. Deduïm que l'error és a la cinquena posició (comptant des de 0).

(d) Per calcular el valor de l'error resolem $7^5 e_5=2=7^{11}$, que té solució $e_5=7^6=12$.

(e) La paraula corregida és $u-e=(3,12,0,1,1,5,3,10,1,9,1,11)-(0,0,0,0,0,12,0,0,0,0,0,0)=(3,12,0,1,1,6,3,10,1,9,1,11)$.

2. (a) El vector de síndromes de v és $\begin{pmatrix}9\\8\\5\\12\end{pmatrix}=\begin{pmatrix}7^4\\7^9\\7^3\\7^6\end{pmatrix}$.

Anomenem t al nombre d'errors.

Tenim $\operatorname{rang}()\neq\operatorname{rang}\begin{pmatrix}9\\8\\5\\12\end{pmatrix}$. Per tant, $t>0$.

D'altra banda, $\operatorname{rang}\begin{pmatrix}9\\8\\5\end{pmatrix}\neq\operatorname{rang}\begin{pmatrix}9&8\\8&5\\5&12\end{pmatrix}$, ja que $\operatorname{rang}\begin{pmatrix}7^4\\7^9\\7^3\end{pmatrix}\neq\operatorname{rang}\begin{pmatrix}7^4&7^9\\7^9&7^3\\7^3&7^6\end{pmatrix}$. Per tant, $t>1$.

Però $\operatorname{rang}\begin{pmatrix}9&8\\8&5\end{pmatrix}=\operatorname{rang}\begin{pmatrix}9&8&5\\8&5&12\end{pmatrix}$. Deduïm que s'han produït dos errors.

(b) Hem de resoldre el sistema $\begin{pmatrix}9&8\\8&5\end{pmatrix}\cdot\begin{pmatrix}l_0\\l_1\end{pmatrix}=\begin{pmatrix}-5\\-12\end{pmatrix}$.

Desenvolupem les equivalències següents:

$$\begin{pmatrix}9&8&5\\8&5&12\end{pmatrix}\sim_{f1'=f1-f2,f2=f2-8f1'}\begin{pmatrix}1&3&6\\0&7&3\end{pmatrix}\sim_{f2'=2f2,f1'=f1-3f2'}\begin{pmatrix}1&0&1\\0&1&6\end{pmatrix}$$

i deduïm que la solució és $l_0=-1=12$ i $l_1=-6=7$.

Per tant, el polinomi localitzador d'errors és $x^2+7x+12$.

(c) Les arrels del polinomi localitzador d'errors són $-3=10=7^2$ i $-4=9=7^4$. En conseqüència, les posicions d'error són la segona i la quarta (comptant des de 0).

(d) Per calcular el valor dels errors resolem el sistema

$$\begin{pmatrix}7^2&7^4\\7^4&7^8\end{pmatrix}\begin{pmatrix}e_2\\e_4\end{pmatrix}=\begin{pmatrix}9\\8\end{pmatrix},$$

és a dir,

$$\begin{pmatrix}10&9\\9&3\end{pmatrix}\begin{pmatrix}e_2\\e_4\end{pmatrix}=\begin{pmatrix}9\\8\end{pmatrix},$$

equivalent a

$$\begin{pmatrix}1&6\\0&1\end{pmatrix}\begin{pmatrix}e_2\\e_4\end{pmatrix}=\begin{pmatrix}1\\12\end{pmatrix}$$

i equivalent a

$$\begin{pmatrix}1&0\\0&1\end{pmatrix}\begin{pmatrix}e_2\\e_4\end{pmatrix}=\begin{pmatrix}7\\12\end{pmatrix},$$

que té solució $e_2=7$, $e_4=12$ i aquests són els valors dels errors.

(e) La paraula corregida és $v - e = (11, 11, 4, 0, 12, 1, 2, 2, 8, 5, 1, 11) - (0, 0, 7, 0, 12, 0, 0, 0, 0, 0, 0, 0) = (11, 11, 10, 0, 0, 1, 2, 2, 8, 5, 1, 11)$.

Torna a l'exercici (p.143)

Solució de l'Exercici 100

1. (a)
   - Separem la informació en blocs de tres bits:
   $$(111)(110)(001)(111)(100)(011)(111)(111)(111)(110)(001)(010)(101)(010)\dots$$
   - N'agafem els primers k blocs:
   $$(111)(110)(001)$$
   - Els passem a símbols:
   $$\alpha^5\alpha^3\alpha^2$$
   - Obtenim el polinomi d'informació:
   $$i(x) = \alpha^5 + \alpha^3 x + \alpha^2 x^2$$
   - El passem cap a la "part alta":
   $$x^{n-k} i(x) = x^4(\alpha^5 + \alpha^3 x + \alpha^2 x^2) = \alpha^5 x^4 + \alpha^3 x^5 + \alpha^2 x^6$$
   - Calculem la redundància:
   $$\begin{array}{rrrrrrr}
   \alpha^2x^6+ & \alpha^3x^5+ & \alpha^5x^4 & & & & \\
   -(\alpha^2x^6+ & \alpha^5x^5+ & \alpha^2x^4+ & \alpha^3x^3+ & \alpha^5x^2) & & \\
   \hline
    & \alpha^2x^5+ & \alpha^3x^4+ & \alpha^3x^3+ & \alpha^5x^2 & & \\
    & -(\alpha^2x^5+ & \alpha^5x^4+ & \alpha^2x^3+ & \alpha^3x^2+ & \alpha^5x) & \\
   \cline{2-6}
    & & \alpha^2x^4+ & \alpha^5x^3+ & \alpha^2x^2+ & \alpha^5x & \\
    & & -(\alpha^2x^4+ & \alpha^5x^3+ & \alpha^2x^2+ & \alpha^3x+ & \alpha^5) \\
   \cline{3-7}
    & & & & & \alpha^2x+ & \alpha^5
   \end{array}
   \quad
   \begin{array}{|rrrrr}
   x^4+ & \alpha^3x^3+ & x^2+ & \alpha x+ & \alpha^3 \\
   \hline
   \alpha^2x^2+ & \alpha^2x+ & \alpha^2 & &
   \end{array}$$

   Per tant, $R(x) = \alpha^2 x + \alpha^5$.
   - Calculem el polinomi $c(x) = x^{n-k} i(x) - R(x) = \alpha^5 + \alpha^2 x + \alpha^5 x^4 + \alpha^3 x^5 + \alpha^2 x^6$.
   - La paraula codificada en símbols serà:
   $$c = (\alpha^5\alpha^2 00\alpha^5\alpha^3\alpha^2)$$
   - La paraula codificada en bits serà:
   $$c = (111\ 001\ 000\ 000\ 111\ 110\ 001)$$

   (b) Calculem $c(\alpha)$ o, equivalentment, calculem el producte de c per la primera fila de H: $c(\alpha) = \alpha^5 \cdot 1 + \alpha^2 \cdot \alpha + 0 \cdot \alpha^2 + 0 \cdot \alpha^3 + \alpha^5 \cdot \alpha^4 + \alpha^3 \cdot \alpha^5 + \alpha^2 \cdot \alpha^6 = \alpha^5 + \alpha^3 + \alpha^2 + \alpha + \alpha = 0$.

2. (a) $u = \alpha^2 1000\alpha 1$.

   (b) El polinomi corresponent a u és $u(x) = x^6 + \alpha x^5 + x + \alpha^2$. Calculem les 4 síndromes:
   $$\begin{array}{rcl}
   u(\alpha) & = & \alpha^6 + \alpha^6 + \alpha + \alpha^2 = \alpha^4 \\
   u(\alpha^2) & = & \alpha^5 + \alpha^4 + \alpha^2 + \alpha^2 = 1 \\
   u(\alpha^3) & = & \alpha^4 + \alpha^2 + \alpha^3 + \alpha^2 = \alpha^6 \\
   u(\alpha^4) & = & \alpha^3 + 1 + \alpha^4 + \alpha^2 = 0
   \end{array}$$

(c) Anomenem t al nombre d'errors. Tenim rang() $\neq$ rang $\begin{pmatrix} \alpha^4 \\ 1 \\ \alpha^6 \\ 0 \end{pmatrix}$, per tant, $t > 0$. I tenim rang $\begin{pmatrix} \alpha^4 \\ 1 \\ \alpha^6 \end{pmatrix} \neq$ rang $\begin{pmatrix} \alpha^4 & 1 \\ 1 & \alpha^6 \\ \alpha^6 & 0 \end{pmatrix}$, per tant, $t > 1$. Com que rang $\begin{pmatrix} \alpha^4 & 1 \\ 1 & \alpha^6 \end{pmatrix}$ = rang $\begin{pmatrix} \alpha^4 & 1 & \alpha^6 \\ 1 & \alpha^6 & 0 \end{pmatrix} = 2$, deduïm que $t = 2$.

(d) Resolem el sistema $\begin{pmatrix} \alpha^4 & 1 \\ 1 & \alpha^6 \end{pmatrix}\begin{pmatrix} l_0 \\ l_1 \end{pmatrix} = \begin{pmatrix} \alpha^6 \\ 0 \end{pmatrix}$. De la segona fila tenim que $l_0 = \alpha^6 l_1$, i substituint a la primera equació tenim $\alpha^4\alpha^6 l_1 + l_1 = \alpha^6$, és a dir, $(\alpha^3 + 1)l_1 = \alpha^6$. Deduïm que $l_1 = \frac{\alpha^6}{\alpha^3+1} = \frac{\alpha^6}{\alpha} = \alpha^5$ i que $l_0 = \alpha^6\alpha^5 = \alpha^4$.
El polinomi localitzador d'errors serà $\lambda(x) = x^2 + l_1 x + l_0 = x^2 + \alpha^5 x + \alpha^4$.

(e) Observem que $\lambda(\alpha^0) = 1 + \alpha^5 + \alpha^4 = 0$ i que $\lambda(\alpha^4) = \alpha + \alpha^2 + \alpha^4 = 0$. Per tant, les seves arrels són α^0 i α^4.
Tindrem error a les posicions indexades amb 0 i 4, és a dir a la primera i la cinquena posicions.

(f) Per calcular els valors dels errors hem de resoldre el sistema

$$\begin{pmatrix} \alpha^0 & \alpha^4 \\ (\alpha^0)^2 & (\alpha^4)^2 \end{pmatrix}\begin{pmatrix} e_0 \\ e_4 \end{pmatrix} = \begin{pmatrix} u(\alpha) \\ u(\alpha^2) \end{pmatrix}$$

és a dir,

$$\begin{pmatrix} 1 & \alpha^4 \\ 1 & \alpha \end{pmatrix}\begin{pmatrix} e_0 \\ e_4 \end{pmatrix} = \begin{pmatrix} \alpha^4 \\ 1 \end{pmatrix}.$$

La solució del sistema és $e_0 = \alpha^5$ i $e_4 = \alpha^3$, que són els valors dels errors demanats.

(g) La paraula d'errors serà $e = (\alpha^5 000\alpha^3 00)$ i, per tant, la paraula corregida serà $u - e = (\alpha^2 1000\alpha 1) - (\alpha^5 000\alpha^3 00) = (\alpha^3 100\alpha^3\alpha 1)$ que correspon a la cadena de bits

110100000000110010100.

(h) La paraula enviada tenia 5 errors de bit:

0011000000000**00**0010100

1101000000000**11**0010100

Torna a l'exercici (p.143)

6.5 Apèndix: Repàs de determinants

El **determinant** és una valor que associem a una matriu quadrada A i que denotem per $\det(A)$ o $|A|$. En els casos en què el nombre de files sigui com a molt 3 tenim les fórmules següents:

$$\begin{aligned} \det\begin{pmatrix} a_{11} \end{pmatrix} &= a_{11}, \\ \det\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} &= a_{11}a_{22} - a_{12}a_{21}, \\ \det\begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{pmatrix} &= a_{11}a_{22}a_{33} + a_{21}a_{32}a_{13} + a_{12}a_{23}a_{31} - a_{11}a_{23}a_{32} - a_{13}a_{22}a_{31} - a_{12}a_{21}a_{33}. \end{aligned}$$

Per exemple,

$$\begin{aligned}
\det\begin{pmatrix} 4 \end{pmatrix} &= 4,\\
\det\begin{pmatrix} 4 & 5\\ 2 & 7 \end{pmatrix} &= 28-10=18,\\
\det\begin{pmatrix} 4 & 5 & 0\\ 2 & 7 & 9\\ 8 & 6 & 1 \end{pmatrix} &= 28+0+360-216-0-10=162.
\end{aligned}$$

Per a casos més grans, definim el **menor** complementari d'a_{ij}, que denotem A_{ij}, com el determinant de la matriu que obtenim eliminant la fila i-èssima i la columna j-èssima de A. Aleshores podem calcular el determinant de A per alguna de les fórmules equivalents següents.
Desenvolupament de menors per files:

$$\begin{aligned}
\det(A) &= a_{11}A_{11} - a_{12}A_{12} + a_{13}A_{13} - a_{14}A_{14} + \dots\\
&= -a_{21}A_{21} + a_{22}A_{22} - a_{23}A_{23} + a_{24}A_{24} - \dots\\
&= a_{31}A_{31} - a_{32}A_{32} + a_{33}A_{33} - a_{34}A_{34} + \dots\\
&= -a_{41}A_{41} + a_{42}A_{42} - a_{43}A_{43} + a_{44}A_{44} - \dots\\
&\vdots
\end{aligned}$$

O bé desenvolupament de menors per columnes:

$$\begin{aligned}
\det(A) &= a_{11}A_{11} - a_{21}A_{21} + a_{31}A_{31} - a_{41}A_{41} + \dots\\
&= -a_{12}A_{12} + a_{22}A_{22} - a_{32}A_{32} + a_{42}A_{42} - \dots\\
&= a_{13}A_{13} - a_{23}A_{23} + a_{33}A_{33} - a_{43}A_{43} + \dots\\
&= -a_{14}A_{14} + a_{24}A_{24} - a_{34}A_{34} + a_{44}A_{44} - \dots\\
&\vdots
\end{aligned}$$

Relacionat: determinant d'una matriu Vandermonde (p.127)

Una matriu quadrada és invertible si i només si el seu determinant és diferent de zero.

Així, un sistema d'equacions on la matriu del sistema sigui una matriu quadrada amb determinant diferent de zero, tindrà solució i la solució serà única.

TEMA 2

Problemes d’examen

Índex

1 Aritmètica modular i polinomial, cossos finits

1. Calculeu el màxim comú divisor de 365 i 70 i expresseu-lo com a combinació lineal de 365 i 70.

   Solució:

   Construïm la taula de l'algoritme d'Euclides:

1	0	1	−4	5	
0	1	−5	21	−26	
		5	4	1	2
365	70	15	10	5	0

   Deduïm que $\mathrm{mcd}(365, 70) = 5$ i que $5 \cdot 365 - 26 \cdot 70 = 5$.

2. (a) Trobeu el màxim comú divisor de 985 i 318 utilitzant divisions successives.
   (b) Doneu la successió de tots els residus obtinguts.
   (c) Expresseu tots els residus com a combinació lineal de 985 i 318.

   Solució:

   (a) Les divisions successives ens donen la taula següent:

1	0	1	−10	31	−41	
0	1	−3	31	−96	127	
		3	10	3	1	
985	318	31	8	7	1	0

   Per tant, el màxim comú divisor és 1.

   (b) La successió de residus és 985, 318, 31, 8, 7 i 1.

   (c) Podem expressar els residus com a combinació lineal de 985 i 318 de la manera següent:

$$\begin{array}{rcrcrcrcr}
985 & = & 1(985) & + & 0(318) & = & 985 & + & 0 \\
318 & = & 0(985) & + & 1(318) & = & 0 & + & 318 \\
31 & = & 1(985) & - & 3(318) & = & 985 & - & 954 \\
8 & = & -10(985) & + & 31(318) & = & -9850 & + & 9858 \\
7 & = & 31(985) & - & 96(318) & = & 30535 & - & 30528 \\
1 & = & -41(985) & + & 127(318) & = & -40385 & + & 40386
\end{array}$$

3. (a) Trobeu el quocient i el residu per a les següents parelles de valors de dividends i divisors:
   - 98 i 12
   - 987 i 123
   - 9876 i 1234
   - 98765 i 12345

   (b) Deduïu quins són el quocient i el residu de dividir 987654321 entre 123456789.

   (c) Comproveu-ho i justifiqueu els passos.

   Solució:

   (a)
   - $q = 8$, $r = 2$
   - $q = 8$, $r = 3$
   - $q = 8$, $r = 4$
   - $q = 8$, $r = 5$

   (b) Intuïm que $q = 8$, $r = 9$.

(c) Calculem $123456789 \cdot 8$ i ens dona 987654312. Si li sumem 9 ens dona 987654321. Per tant, $987654321 = 123456789 \cdot 8 + 9$ i, com que $9 < 123456789$, per força 9 és el residu i 8 el quocient.

4. Per a cadascuna de les següents congruències
   - justifiqueu si tenen solució o si no en tenen,
   - digueu quantes solucions tenen,
   - doneu totes les solucions mòdul 60.

(a) $32x \equiv 58(60)$

(b) $53x \equiv 17(60)$

(c) $39x \equiv 18(60)$

Solució:

(a) $32x \equiv 58(60)$ no té solució perquè $\mathrm{mcd}(32, 60) = 4$ no divideix 58.

(b) $53x \equiv 17(60)$ té solució perquè $\mathrm{mcd}(53, 60) = 1$ divideix 17. $53x \equiv 17(60)$ no es pot simplificar més. Resolem primer $53x' \equiv 1(60)$:

1	0	1	−7	8	−15	
0	1	−1	8	−9	17	
		1	7	1	1	
60	53	7	4	3	1	0

Deduïm que $(60) \cdot (-15) + (53) \cdot (17) = 1$ i, per tant, $53 \cdot 17 \equiv 1 \mod 60$.

Multiplicant-ho tot per 17, es complirà $53(17 \cdot 17) = 53 \cdot 289 = 53 \cdot 49 =\equiv 17(60)$. Per tant, $x \equiv 49(60)$ és *una* solució.

$53x \equiv 17(60)$ només té una solució, ja que $\mathrm{mcd}(53, 60) = 1$. La solució és $x \equiv 49(60)$.

(c) $39x \equiv 18(60)$ té solució perquè $\mathrm{mcd}(39, 60) = 3$ divideix 18.

$39x \equiv 18(60)$ queda simplificada com $13x \equiv 6(20)$ i per això resolem primer $13x' \equiv 1(20)$:

1	0	1	−1	2	
0	1	−1	2	−3	
		1	1	1	
20	13	7	6	1	0

Deduïm que $(20) \cdot (2) + (13) \cdot (-3) = 1$ i, per tant, $13 \cdot 17 \equiv 1 \mod 20$.

Multiplicant-ho tot per 6, es complirà $13(17 \cdot 6) = 13 \cdot 102 = 13 \cdot 2 \equiv 6(20)$. Per tant, $x \equiv 2(20)$ és *una* solució.

$39x \equiv 18(60)$ tenia solució $x \equiv 2(20)$. Totes les seves solucions mòdul 60 seran $x = 2, 22, 42(60)$. Observem que n'hi ha $3 = \mathrm{mcd}(39, 60)$.

5. Quantes solucions tenen aquestes equacions amb congruències? Doneu-ne les solucions.

(a) $26x \equiv 3 \mod 13$

(b) $13x \equiv 3 \mod 26$

(c) $26x \equiv 0 \mod 13$

(d) $9x \equiv -3 \mod 15$

(e) $5x \equiv 4 \mod 7$

(f) $5x \equiv 7 \mod 7$

Solució:

(a) 0 solucions, (b) 0 solucions, (c) 13 solucions, que són $x \equiv 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12 \mod 13$, (d) 3 solucions, que són $x \equiv 3, 8, 13 \mod 15$, (e) 1 solució, que és $x \equiv 5 \mod 7$, (f) 1 solució, que és $x \equiv 0 \mod 7$.

6. Sigui $b = 124$
   (a) És b primer?
   (b) Si ho és calculeu $\phi(b)$ i si no expresseu-lo com a producte de potències de primers.
   (c) Troba c tal que b, c no siguin coprimers i que el seu màxim comú divisor sigui diferent de b i c.
   (d) Doneu els residus successius de la taula de divisions successives de b i c.
   (e) Qui és $\mathrm{mcd}(b, c)$?
   (f) Expresseu $\mathrm{mcd}(b, c)$ com a combinació lineal entera de b i c.
   (g) És $\mathbb{Z}_b$ un cos?
   (h) Per què?
   (i) Quants elements invertibles hi ha a $\mathbb{Z}_b$?
   (j) Doneu un element invertible de $\mathbb{Z}_b$ diferent de 1 i $b - 1$.
   (k) Doneu el seu invers.
   (l) Quants divisors de zero no nuls hi ha a $\mathbb{Z}_b$?
   (m) Doneu, si existeix, un divisor de zero no nul de $\mathbb{Z}_b$.
   (n) Doneu, si existeix, un element no nul de $\mathbb{Z}_b$ que multiplicat per l'element de l'apartat anterior doni zero.

   Solució:

   (a) No.
   (b) $124 = 2^2 \cdot 31$.
   (c) Escollim, per exemple, $c = 20$.
   (d) En el nostre cas, 124, 20, 4, 0.
   (e) 4.
   (f) $4 = 1 \cdot 124 - 6 \cdot 20$.
   (g) No.
   (h) Perquè 124 no és primer.
   (i) $\varphi(124) = \varphi(2^2)\varphi(31) = (4 - 2)30 = 60$.
   (j) Per exemle, 5, ja que és coprimer amb 124.
   (k) Aplicant el teorema d'Euler, l'invers de 5 serà $5^{\varphi(124)-1} = 5^{59}$. Sabem que $5^3 = 125 = 1$. Per tant, $5^{59} = 5^{57}5^2 = 5^2 = 25$. També haguéssim pogut aplicar divisions successives:

1	0	1	−1	
0	1	−24	**25**	
		24	1	
124	5	4	1	0

   (l) $124 - 60 - 1 = 63$.
   (m) 4, ja que 4 no és coprimer amb 124.
   (n) 31, ja que $4 \cdot 31 = 124 = 0$ a $\mathbb{Z}_{124}$.

7. Sigui l'anell $\mathbb{Z}_{27}$.
   (a) És un cos?
   (b) Quants elements invertibles té i quins són?
   (c) Quants divisors de zero té?
   (d) Busqueu un element primitiu.

(e) Busqueu un element diferent de $0, 1$ que no sigui primitiu. Quin ordre té?

Solució:

(a) No és un cos, (b) $\phi(27) = 3^3 - 3^2 = 18$ invertibles, que són $\{1, 2, 4, 5, 7, 8, 10, 11, 13, 14, 16, 17, 19, 20, 22, 23, 25, 26\}$ (c) 8, (d) per exemple, el 2, (e) 4, que té ordre 9.

8. (a) És $\mathbb{Z}_{11}$ un cos? Per què?
   (b) Quants elements invertibles té $\mathbb{Z}_{11}$?
   (c) Doneu la llista de tots els invertibles de $\mathbb{Z}_{11}$ i els seus inversos.
   (d) Comproveu que 2 és un element primitiu de $\mathbb{Z}_{11}$.
   (e) Quants elements primitius té $\mathbb{Z}_{11}$? Doneu-los tots.

   Solució:

   (a) Sí, perquè 11 és primer.
   (b) Té 10 elements invertibles, que són tots menys el 0, perquè és un cos. És a dir, $\{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$.
   (c)

element	invers
1	1
2	6
3	4
4	3
5	9
6	2
7	8
8	7
9	5
10	10

   (d) És primitiu perquè el seu ordre és 11. És a dir, totes les seves potències amb exponent més petit que 10 són diferents. Ho podem comprovar a la taula següent:

2^0	1
2^1	2
2^2	4
2^3	8
2^4	5
2^5	10
2^6	9
2^7	7
2^8	3
2^9	6
2^{10}	1

   (e) El nombre d'elements primitius és $\phi(\phi(11)) = \phi(10) = \phi(5)\phi(2) = 4$. Els elements primitius són 2^j, on $\text{mcd}(j, \phi(11)) = \text{mcd}(j, 10) = 1$, és a dir, $2^1, 2^3, 2^7, 2^9$, que correspon a $2, 8, 7, 6$.

9. Sigui l'anell $\mathbb{Z}_{16}$.
   (a) És un cos?
   (b) Quants elements invertibles té?
   (c) Quins són tots els elements invertibles?
   (d) Doneu un element invertible diferent de 1 i el seu invers.
   (e) Demostreu que un element $\alpha \in \mathbb{Z}_{16}$ és primitiu si i només si $\alpha^4 \neq 1$.

(f) Utilitzeu l'apartat anterior per veure que $\mathbb{Z}_{16}$ no té elements primitius.

Solució:

(a) No és un cos perquè $16 = 2^4$ no és primer. (b) $\phi(16) = 2^4 - 2^3 = 8$ invertibles. (c) $\{1, 3, 5, 7, 9, 11, 13, 15\}$. (d) 3 i 11, o bé 5 i 13, o bé 7 i 7, o bé 9 i 9, o bé 15 i 15. (e) Un element α és primitiu si i només si el seu ordre és $\phi(16) = 8$. Si el seu ordre és 8, aleshores, per definició d'ordre, $\alpha^4 \neq 1$. D'altra banda, si $\alpha^4 \neq 1$ voldrà dir que α és primitiu perquè no tindrà ordre cap dels divisors de 4 $(1, 2, 4)$. En efecte, $\alpha^1 \neq 1$ perquè, si no, altrament, $\alpha^4 = (\alpha^1)^4 = 1$; $\alpha^2 \neq 1$ perquè, si no, altrament, $\alpha^4 = (\alpha^2)^2 = 1$; $\alpha^4 \neq 1$ per hipòtesi. (f) Els únics elements que poden ser primitius són els invertibles. Però $1^4 = 1$, $3^4 = 81 = 1$, $5^4 = 25^2 = 9^2 = 1$, $7^4 = 49^2 = 1^2 = 1$, $9^4 = 81^2 = 1^2 = 1$, $11^4 = (-5)^4 = 25^2 = 9^2 = 1$, $13^2 = (-3)^4 = 81 = 1$, $15^2 = (-1)^4 = 1$. Per l'apartat anterior, no són primitius.

10. (a) És $\mathbb{Z}_{27}$ un cos? Per què?
    (b) Quants elements de $\mathbb{Z}_{27}$ són invertibles?
    (c) Justifiqueu per què té invers el 8 a $\mathbb{Z}_{27}$.
    (d) Trobeu l'invers de 8 a $\mathbb{Z}_{27}$ utilitzant la identitat de Bézout.
    (e) Trobeu l'invers de 8 a $\mathbb{Z}_{27}$ utilitzant el teorema d'Euler.
    (f) Comproveu que l'element trobat és, en efecte, l'invers.

Solució:

(a) No, perquè 27 no és primer.

(b) $\phi(27) = 27 - 9 = 18$.

(c) Perquè $\mathrm{mcd}(8, 27) = 1$

(d) Utilitzem l'algoritme d'Euclides per trobar els coeficients de la identitat de Bézout:

1	0	1	−2	3
0	1	−3	7	−10
		3	2	1
27	8	3	2	1

Deduïm que $3 \cdot 27 + (-10) \cdot 8 = 1$. Reduint mòdul 27 obtenim $(-10) \cdot 8 = 17 \cdot 8 = 1$ i, per tant, l'invers de 8 mòdul 27 és 17.

(e) Pel teorema d'Euler tenim que $8^{18} = 1 \mod 27$, d'on deduïm que a $\mathbb{Z}_{27}$, l'invers de 8 és 8^{17}. Podem calcular aquesta potència de moltes maneres diferents. En posem una de possible: com que podem reduir els exponents per múltiples de $\phi(27) = 18$, tenim $8^{17} = 2^{3 \cdot 17} = 2^{17-1-1} = 2^{15} = 2^5 \cdot 2^5 \cdot 2^5 = 32 \cdot 32 \cdot 32 = 5 \cdot 5 \cdot 5 = 125 = 19 + 25 = 17 + 27 = 17$.

(f) Es tracta de comprovar que $8 \cdot 17 = 1$ a $\mathbb{Z}_{27}$ i, com en l'apartat anterior, hi ha moltes maneres de fer-ho. En proposem una: $8 \cdot 17 = 8 \cdot (10 + 7) = 80 + 56 = -1 + 2 = 1$.

11. (a) Quants elements té $\mathbb{Z}_{600}$?
    (b) Quants invertibles té $\mathbb{Z}_{600}$?
    (c) Doneu tres elements de $\mathbb{Z}_{600}$ que siguin invertibles i que siguin diferents de 1 i anomeneu-los x, y, z (us serà més senzill si agafeu $x < y < z$).
    (d) Calculeu $200y + 400z$ a $\mathbb{Z}_{600}$.
    (e) Calculeu x^{325} a $\mathbb{Z}_{600}$.
    (f) Doneu l'invers de x utilitzant el teorema d'Euler.
    (g) Comproveu l'apartat anterior.
    (h) Doneu l'invers de y utilitzant la identitat de Bézout.
    (i) Comproveu l'apartat anterior.

Solució:

(a) 600.

(b) $\phi(600) = \phi(2^3 \cdot 3 \cdot 5^2) = \phi(2^3) \cdot \phi(3) \cdot \phi(5^2) = (2^3 - 2^2)(3 - 1)(5^2 - 5) = 4 \cdot 2 \cdot 20 = 160$.

(c) Podem agafar $x = 7, y = 11, z = 13$ o moltes altres opcions.

(d) $200 \cdot 11 + 400 \cdot 13 = 2200 + 5200 = 7400 = 1400 = 200$ o altres resultats depenent de x i y.

(e) Com que $\phi(600) = 160$, aleshores $a^{160} = 1 \mod 600$ si $\mathrm{mcd}(a, 600) = 1$. Per tant, a $\mathbb{Z}_{600}$ tenim $a^{325} = a^{2\cdot 160+5} = (a^{160})^2 a^5 = a^5$. En particular, $7^{325} = 7^5 = 7^2 \cdot 7^2 \cdot 7 = 49 \cdot 49 \cdot 7 = 7$. Aquest resultat es pot obtenir per força bruta. Però també haguéssim pogut procedir així: $(50 - 1)(50 - 1)7 = (2500 - 100 + 1)7 = ((2400 + 100) - 100 + 1)7 = 7$. D'altra banda, $11^{325} = 11^5 = 121 \cdot 121 \cdot 11$. Per força bruta obtenim que és 251. Però també ho haguéssim pogut calcular així: $(120 + 1)(120 + 1)11 = (120^2 + 240 + 1)11 = (1200 \cdot 12 + 240 + 1)11 = 241 \cdot 11 = 2651 = 251$, $13^{325} = 13^5 = 13^2 \cdot 13^2 \cdot 13 = 169 \cdot 169 \cdot 13 = 28561 \cdot 13 = 4561 \cdot 13 = 361 \cdot 13 = (360 + 1)(10 + 3) = 3600 + 10 + 1080 + 3 = 0 + 10 + 480 + 3 = 493$.

(f) Pel teorema d'Euler sabem que l'invers d'un invertible a és a^{159}. L'invers de 7, per exemple, serà $7^{159} = 7^{5\cdot 31+4} = (7^5)^{31} \cdot 7^4$ i ara podem utlitzar el que hem vist a l'apartat anterior, $(7^5)^{31} \cdot 7^4 = 7^{31} \cdot 7^4 = 7^{35} = (7^5)^7 = 7^7 = 7^{5+2} = 7^5 \cdot 7^2 = 7\dot{7}^2 = 7 \cdot 49 = 343$.

Si volguéssim calcular l'invers de 11, per l'apartat anterior sabem que $11^5 = 251 = 240 + 11$. Deduïm que $11^{10} = (240 + 11)^2 = 240^2 + 2 \cdot 240 \cdot 11 + 11^2 = 2400 \cdot 24 + 5280 + 121 = 0 + 480 + 121 = 601 = 1$. L'invers de 11 serà $11^{159} = 11^{10\cdot 15+9} = (11^{10})^{15} \cdot 11^9 = 1^{15} \cdot 11^9 = 11^4 \cdot 11^5$. Pels càlculs intermedis de l'apartat anterior sabem que $11^4 \cdot 11^5 = 241 \cdot 251 = (251 - 10)251 = 251^2 - 2510 = 1 - 110 = 491$.

(g) $343 \cdot 7 = 2401 = 1$ o bé $491 \cdot 11 = 5401 = 1$ o bé altres opcions depenent de l'elecció de y.

(h) Resolem per $y = 11$ i per $y = 13$, però hi ha més opcions. Les divisions successives de 600 entre 11 ens donen la taula següent:

1	0	1	−1	2	
0	1	−54	55	−109	
		54	1	1	
600	11	6	5	1	0

Per tant, $1 = 2 \cdot 600 + (-109) \cdot 11$. Fent mòdul 600 obtenim $1 = -109 \cdot 11$ i, per tant, l'invers de 11 a $\mathbb{Z}_{600}$ és $600 - 109 = 491$.

Les divisions successives de 600 entre 13 ens donen la taula següent:

1	0	1	−6	
0	1	−46	277	
		46	6	
600	13	2	1	0

Per tant, $1 = -6 \cdot 600 + 277 \cdot 13$. Fent mòdul 600 obtenim $1 = 277 \cdot 13$ i, per tant, l'invers de 13 a $\mathbb{Z}_{600}$ és 277.

(i) $491 \cdot 11 = 5401 = 1$ o bé $277 \cdot 13 = 3601 = 1$ o bé altres opcions depenent de l'elecció de y.

12. (a) Doneu, justificadament, si existeix, un polinomi de $\mathbb{Z}_2[x]$ que tingui arrels i que sigui irreductible, o justifiqueu per què no existeix.

(b) Doneu, justificadament, si existeix, un polinomi de $\mathbb{Z}_2[x]$ que tingui arrels i que sigui reductible, o justifiqueu per què no existeix.

(c) Doneu, justificadament, si existeix, un polinomi de $\mathbb{Z}_2[x]$ que no tingui arrels i que sigui irreductible, o justifiqueu per què no existeix.

(d) Doneu, justificadament, si existeix, un polinomi de $\mathbb{Z}_2[x]$ que no tingui arrels i que sigui reductible, o justifiqueu per què no existeix.

(e) En quin cas podem dir que un polinomi és reductible si i només si té arrels? Per què?

Solució:

(a) Només poden ser $x, x+1$. Són irreductibles perquè són lineals i els polinomis lineals són irreductibles. El polinomi x té 0 com arrel i el polinomi $x+1$ té 1 com arrel.

(b) Per exemple, x^2+1. És reductible perquè descompon com a $(x+1)(x+1)$. Té 1 per arrel, ja que si l'avaluem a 1 ens dona 0.

(c) Per exemple, x^2+x+1. No té arrels perquè en avaluar-lo a 0 dona 1 i en avaluar-lo a 1 dona 1. És irreductible perquè té grau 2 i no té arrels.

(d) Per exemple, x^4+x^2+1. És reductible perquè descompon com a $(x^2+x+1)(x^2+x+1)$. No té arrels perquè en avaluar-lo a 0 dona 1 i en avaluar-lo a 1 dona 1.

(e) Podem dir que un polinomi f és reductible si i només si té arrels sempre que tingui grau 2 o 3.
En efecte, suposem que el grau de f és d. Perquè f descompongui, sempre ho farà com a producte de dos polinomis de graus d', d'', respectivament, de manera que $d'+d''=d$. Si $d=2$, això només pot ser si $d'=1, d''=1$. Si $d=3$, això només pot ser si $d'=1, d''=2$ o si $d'=2, d''=1$. Tant si $d=2$ com si $d=3$, el grau d'almenys un dels polinomis en què factoritza f ha de ser 1 i tenir un factor de grau 1 és equivalent a tenir una arrel. Si $d \geq 4$, aleshores podria ser que f no tingués arrels però que es pogués descompondre com a producte de dos polinomis de grau més gran que 1 tots dos. Per exemple, amb $d'=2>1$ i $d''=d-2>1$.

13. A $\mathbb{Z}_2[x]$ calculeu el màxim comú divisor de x^5+x^2+x+1 i x^3+1 i expresseu-lo com a combinació lineal polinomial dels polinomis inicials.

Solució:

Construïm la taula de l'algoritme d'Euclides:

$$
\begin{array}{r|l}
x^5 + x^2 + x + 1 & x^3 + 1 \\ \cline{2-2}
-(x^5 + x^2 \qquad\quad) & x^2 \\ \cline{1-1}
x + 1 &
\end{array}
$$

$$
\begin{array}{r|l}
x^3 \qquad\quad + 1 & x + 1 \\ \cline{2-2}
-(x^3 + x^2 \qquad\quad) & x^2 + x + 1 \\ \cline{1-1}
x^2 \quad + 1 & \\
-(x^2 + x \quad) & \\ \cline{1-1}
x + 1 & \\
-(x + 1) & \\ \cline{1-1}
0 &
\end{array}
$$

1	0	1	
0	1	x^2	
		x^2	
x^5+x^2+x+1	x^3+1	$x+1$	0

Obtenim que $\text{mcd}(x^5+x^2+x+1, x^3+1) = x+1 = (1)(x^5+x^2+x+1) + (x^2)(x^3+1)$.

14. (a) Calculeu el màxim comú divisor dels enters 9 i 7 fent servir la taula de divisions successives d'Euclides i expresseu-lo com a combinació lineal de 9 i 7.

Solució:

1	0	1	−3	
0	1	−1	4	
		1	3	
9	7	2	1	0

Deduïm que $(9)\cdot(-3)+(7)\cdot(4)=1$ i, per tant, $7\cdot 4 \equiv 1 \mod 9$.

(b) Calculeu a $\mathbb{Z}_3[x]$ el màxim comú divisor del polinomi $a = x^2 + 2x + 2$ i el polinomi $b = 2x + 1$ i expresseu-lo com a combinació lineal de a i b.

Solució:

$$\begin{array}{r|l} x^2+2x+2 & 2x+1 \\ \cline{2-2} -(x^2+2x\quad) & 2x \\ \hline 2 & \end{array}$$

1	0	1	
0	1	x	
		$2x$	$x+2$
x^2+2x+2	$2x+1$	2	0

Deduïm que $(x^2 + 2x + 2) + x(2x + 1) = 2$.

(c) Podem deduir si 7 és invertible a $\mathbb{Z}_9$? En cas afirmatiu doneu el seu invers.

Solució:

7 és invertible perquè és coprimer amb 9 i el seu invers és 4.

(d) Podem deduir si $2x + 1$ és invertible a $\mathbb{Z}_3[x]/x^2 + 2x + 2$? En cas afirmatiu doneu el seu invers.

Solució:

$2x+1$ és invertible perquè és coprimer amb x^2+2x+2. De la igualtat $(x^2+2x+2)+x(2x+1) = 2$ deduïm que $2(x^2 + 2x + 2) + 2x(2x + 1) = 1$. En conseqüència, l'invers de $(2x + 1)$ és $2x$.

(e) Podem deduir si $x + 2$ és invertible a $\mathbb{Z}_3[x]/x^2 + 2x + 2$? En cas afirmatiu doneu el seu invers.

Solució:

Observem que $x + 2 = 2(2x + 1)$. Com que $(2x + 1)(2x) = 1$, també $(2(2x + 1))(2(2x)) = 1$, és a dir, $(x + 2)x = 1$. Per tant, l'invers de $(x + 2)$ és x.

(f) Comproveu que tots els inversos que heu trobat són, en efecte, inversos.

Solució:

- $7 \cdot 4 = 28 = 1 \mod 9$
- $(2x + 1)(2x) = x^2 + 2x = -2 = 1 \mod x^2 + 2x + 2$
- $(x + 2)(x) = x^2 + 2x = -2 = 1 \mod x^2 + 2x + 2$

15. Contesteu justificadament els següents apartats:

(a) Llisteu els enters m entre 2 i 10 (ambdós inclosos) pels que $\mathbb{Z}_m$ és un cos.

(b) Llisteu els enters m entre 2 i 10 (ambdós inclosos) pels quals existeix un cos de m elements.

(c) Doneu tres valors de m diferents tals que $\mathbb{Z}_m^*$ tingui 4 elements.

Solució:

(a) 2, 3, 5, 7.

(b) 2, 3, 4, 5, 7, 8, 9.

(c) 5, 10, 8.

16. (a) Digueu tots els cossos primers i tots els polinomis que podem utilitzar per construir el cos finit de 8 elements.

(b) Escolliu una de les opcions de l'apartat anterior i doneu un element primitiu i la corresponent taula potencial-vectorial.

Solució:

(a) El cos primer ha de ser $\mathbb{Z}_2$ i els polinomis han de ser $x^3 + x^2 + 1$ o bé $x^3 + x + 1$, ja que són els únics polinomis de $\mathbb{Z}_2$ irreductibles de grau 3.

(b) En els dos casos $\alpha = [x]$ és un element primitiu.

La taula potencial-vectorial per a $\mathbb{Z}_2/x^3 + x^2 + 1$ és

0	000
α^0	100
α^2	001
α^3	101
α^4	111
α^5	110
α^6	011

La taula potencial-vectorial per a $\mathbb{Z}_2/x^3 + x + 1$ és

0	000
α^0	100
α^2	001
α^3	110
α^4	011
α^5	111
α^6	101

17. (a) Considerem els polinomis $f = x^5 + x^2 + 1$ i $g = x^2 + x + 1$ de $\mathbb{Z}_2[x]$. Quins són el quocient i el residu de dividir f entre g?

(b) Demostreu que f i g són irreductibles a $\mathbb{Z}_2[x]$.

(c) Quants elements té $\mathbb{Z}_2[x]/f$?

(d) Quants elements primitius hi ha a $\mathbb{Z}_2[x]/f$?

Solució:

(a) Fem la divisió de polinomis

$$
\begin{array}{rl|l}
x^5 & \qquad\qquad +x^2+1 & x^2+x+1 \\ \cline{3-3}
-(x^5+x^4+x^3 & \qquad\qquad\quad) & x^3+x^2 \\ \cline{1-2}
x^4+x^3+x^2+1 & & \\
-(x^4+x^3+x^2 & \quad) & \\ \cline{1-2}
1 & &
\end{array}
$$

Obtenim $q = x^3 + x^2$, $r = 1$. Podem comprovar que, en efecte, $(x^2 + x + 1)(x^3 + x^2) + 1 = x^5 + x^4 + x^4 + x^3 + x^3 + x^2 + 1 = x^5 + x^2 + 1$.

(b) El polinomi g és irreductible perquè té grau 2 i no té arrels. Com que el polinomi f té grau 5, per veure que és irreductible hem de mirar que no tingui factors irreductibles de grau 1 (ho sabem perquè no té arrels) ni factors irreductibles de grau 2. Això darrer ho sabem perquè l'únic polinomi irreductible de grau 2 és x^2+x+1 (els altres tindran per força 0 o 1 com arrel) i, del primer apartat, deduïm que g no divideix f.

(c) $2^5 = 32$.

(d) Qualsevol element de $\mathbb{Z}_2[x]/f$ té com a ordre un divisor de $32 - 1 = 31$. Com que 31 és primer, els únics ordres possibles són 1 o 31. Dels 32 elements de $\mathbb{Z}_2[x]/f$, el 0 no té ordre definit i l'1 té ordre 1 (és l'únic element amb aquest ordre). La resta, que són 30, tots tenen ordre 31 i, per tant, són primitius. La resposta a la pregunta és, doncs, que hi ha 30 elements primitius.

18. (a) Doneu un polinomi reductible de grau 2 de $\mathbb{Z}_3[x]$.

(b) Doneu un polinomi irreductible de grau 2 de $\mathbb{Z}_3[x]$.

(c) Quin dels dos polinomis anteriors podem utilitzar per construir un cos? Quants elements tindrà el cos?

(d) Doneu una taula d'equivalències potencial-polinomial-vectorial del cos obtingut a partir d'un element primitiu.

(e) Quins són els ordres possibles dels elements del cos?

(f) Doneu un element de cada ordre possible.

Solució:

(a) Per exemple, x^2, x^2+x, x^2+2.

(b) Només n'hi ha sis de possibles: x^2+1, x^2+x+2, x^2+2x+2, $2x^2+2$, $2x^2+2x+1$, $2x^2+x+1$.

(c) El segon. Tindrà 9 elements.

(d) La taula d'equivalències dependrà de quin polinomi irreductible haguem agafat. Si agafem el primer, resulta que $\alpha=[x]$ no és un element primitiu, ja que $\alpha^4=1$. En aquest cas agafem, per exemple, $\beta=\alpha+1$. Construïm la taula a partir de β i, al mateix temps que la construïm, veiem que β és primitiu.

pot.	pol. en α	vec. resp. α	pol. en β	vec. resp. β
0	0	00	0	00
β^0	1	10	1	10
β^1	$\alpha+1$	11	β	01
β^2	2α	02	$2\beta+1$	12
β^3	$2\alpha+1$	12	$2\beta+2$	22
β^4	2	20	2	20
β^5	$2\alpha+2$	22	2β	02
β^6	α	01	$\beta+2$	21
β^7	$\alpha+2$	21	$\beta+1$	11

Si agafem el polinomi x^2+x+2 i anomenem $\alpha=[x]$, aleshores α és primitiu i ens dona la taula d'equivalències següent:

pot.	pol.	vec.
0	0	00
α^0	1	10
α^1	α	01
α^2	$2\alpha+1$	12
α^3	$2\alpha+2$	22
α^4	2	20
α^5	2α	02
α^6	$\alpha+2$	21
α^7	$\alpha+1$	11

Si agafem el polinomi x^2+2x+2 i anomenem $\alpha=[x]$, aleshores α és primitiu i ens dona la taula d'equivalències següent:

pot.	pol.	vec.
0	0	00
α^0	1	10
α^1	α	01
α^2	$\alpha+1$	11
α^3	$2\alpha+1$	12
α^4	2	20
α^5	2α	02
α^6	$2\alpha+2$	22
α^7	$\alpha+2$	21

Si agafem qualsevol dels altres tres polinomis irreductibles podem construir la taula de manera semblant a les anteriors.

(e) 1, 2, 4, 8.

(f) Si $\alpha=[x]$ és primitiu tenim:

- ordre 1: 1,
- ordre 2: α^4,
- ordre 4: α^2,
- ordre 8: α.

Si α no és primitiu, agafem β primitiu i tenim:

- ordre 1: 1,
- ordre 2: β^4,
- ordre 4: β^2,
- ordre 8: β.

19. Considerem $\mathbb{Z}_3[x]/x^2 + x + 2$

(a) Demostreu que és un cos.

(b) Quants elements té?

(c) És $\alpha = [x]$ un element primitiu? Per què?

(d) Doneu-ne una taula d'equivalències amb les notacions potencial, polinomial i vectorial.

(e) Calculeu $\alpha^2\left(\frac{\alpha^{20}-\alpha^5+\alpha}{\alpha^3-\alpha}\right)$.

Solució:

(a) Cal veure si x^2+x+2 és irreductible i ho és perquè té grau 2 i no té arrels ($f(0) = 2 \neq 0$, $f(1) = 1 \neq 0$ i $f(2) = 2 \neq 0$).

(b) $3^2 = 9$.

(c) Els únics ordres possibles dels elements de $\mathbb{Z}_3[x]/x^2 + x + 2$ són els divisors de $9 - 1 = 8$, és a dir, $\{1, 2, 4, 8\}$. Però α^1 i α^2 són $\neq 1$ i $\alpha^4 = (\alpha^2)^2 = (2\alpha + 1)^2 = 4\alpha^2 + 4\alpha + 1 = \alpha^2 + \alpha + 1 = 2\alpha + 1 + \alpha + 1 = 2 \neq 1$. Per tant, l'ordre de α no és $1, 2$ ni 4 i ha de ser 8.

(d)

pot.	pol.	vect.
0	0	(0,0)
α	α	$(0,1)$
α^2	$2\alpha+1$	$(1,2)$
α^3	$2\alpha+2$	$(2,2)$
α^4	2	$(2,0)$
α^5	2α	$(0,2)$
α^6	$\alpha+2$	$(2,1)$
α^7	$\alpha+1$	$(1,1)$
α^8	1	$(1,0)$

(e) $\alpha^2\left(\frac{\alpha^{20}-\alpha^5+\alpha}{\alpha^3-\alpha}\right) = \alpha^2\left(\frac{\alpha^4-\alpha^5+\alpha}{\alpha^3-\alpha}\right) = \alpha^2\left(\frac{2-2\alpha+\alpha}{2\alpha+2-\alpha}\right) = \alpha^2\left(\frac{2+2\alpha}{\alpha+2}\right) = \alpha^2\left(\frac{\alpha^3}{\alpha^6}\right) = \frac{\alpha^5}{\alpha^6} = \frac{\alpha^{13}}{\alpha^6} = \alpha^7$.

20. Considerem $\mathbb{Z}_3[x]/x^2 + 1$

(a) Demostreu que és un cos.

(b) Quants elements té?

(c) Anomenem α l'element del cos que correspon a la classe de x mòdul $x^2 + 1$. Quin és l'ordre de α?

(d) És $\alpha = [x]$ un element primitiu? Per què?

(e) Trobeu un element primitiu β.

(f) Escriviu α com una potència de β.

(g) Doneu una taula d'equivalències amb les notacions potencial amb potències de β, polinomial amb polinomis en α i vectorial.

(h) Calculeu $\beta^{15}\left(\frac{\beta^2-\beta^3}{\beta^6+\beta}\right)$.

Solució:

(a) És un cos perquè, d'una banda, 3 és primer i, d'altra banda, x^2+1 té grau 2 i no té arrels i, per tant, és irreductible a $\mathbb{Z}_3[x]$.

(b) $3^2 = 9$.

(c) $\alpha^1 \neq 1$, $\alpha^2 = 2 \neq 1$, $\alpha^3 = 2\alpha \neq 1$, $\alpha^4 = (\alpha^2)^2 = 2^2 = 1$. Per tant, l'ordre de α és 4.

(d) No ho és perquè per ser primitiu hauria de tenir ordre $9-1=8$.

(e) Com en l'exercici anterior, els únics ordres possibles són els divisors de 8 i, per tant, β és primitiu si i només si $\beta^4 \neq 1$. Agafem $\beta = \alpha+1$ i veiem que és un element primitiu. En efecte, $\beta^4 = (\beta^2)^2 = (\alpha^2+2\alpha+1)^2 = (2+2\alpha+1)^2 = (2\alpha)^2 = 4\alpha^2 = \alpha^2 = 2 \neq 1$. Haguéssim pogut agafar $\beta = \alpha+2$, $\beta = 2\alpha+1$, $\beta = 2\alpha+2$ i també ens haurien donat elements primitius.

(f) Ho podem fer a partir de la taula de l'apartat següent i obtenim $\alpha = \beta^6$. Si en lloc d'agafar $\beta = \alpha+1$ haguéssim agafat $\beta = 2\alpha+2$, seria el mateix. Si haguéssim agafat $\beta = \alpha+2$ o bé $\beta = 2\alpha+1$, aleshores tindríem $\alpha = \beta^2$.

(g) Depenent de quina β haguem agafat, tindrem alguna de les següents taules:

pot.	pol.	vect.
0	0	$(0,0)$
β	$\alpha+1$	$(1,1)$
β^2	2α	$(0,2)$
β^3	$2\alpha+1$	$(1,2)$
β^4	2	$(2,0)$
β^5	$2\alpha+2$	$(2,2)$
β^6	α	$(0,1)$
β^7	$\alpha+2$	$(2,1)$
β^8	1	$(1,0)$

pot.	pol.	vect.
0	0	$(0,0)$
β	$\alpha+2$	$(2,1)$
β^2	α	$(0,1)$
β^3	$2\alpha+2$	$(2,2)$
β^4	2	$(2,0)$
β^5	$2\alpha+1$	$(1,2)$
β^6	2α	$(0,2)$
β^7	$\alpha+1$	$(1,1)$
β^8	1	$(1,0)$

pot.	pol.	vect.
0	0	$(0,0)$
β	$2\alpha+1$	$(1,2)$
β^2	α	$(0,1)$
β^3	$\alpha+1$	$(1,1)$
β^4	2	$(2,0)$
β^5	$\alpha+2$	$(2,1)$
β^6	2α	$(0,2)$
β^7	$2\alpha+2$	$(2,2)$
β^8	1	$(1,0)$

pot.	pol.	vect.
0	0	$(0,0)$
β	$2\alpha+2$	$(2,2)$
β^2	2α	$(0,2)$
β^3	$\alpha+2$	$(2,1)$
β^4	2	$(2,0)$
β^5	$\alpha+1$	$(1,1)$
β^6	α	$(0,1)$
β^7	$2\alpha+1$	$(1,2)$
β^8	1	$(1,0)$

(h) En tots els casos dona 1. Vegem-ho en el cas $\beta = \alpha+1$: $\beta^{15}\left(\frac{\beta^2-\beta^3}{\beta^6+\beta}\right) = \beta^{-1}\left(\frac{\beta^2-\beta^3}{\beta^6+\beta}\right) = \frac{\beta-\beta^2}{\beta^6+\beta} = \frac{1-\beta}{\beta^5+1} = \frac{2\alpha}{2\alpha} = 1$.

21. Considerem $R = \mathbb{Z}_3[x]/f(x)$.

(a) Doneu un polinomi $f(x)$ de manera que R sigui un cos de més de 3 elements.

(b) Quants elements té?

(c) Anomenem α a l'element del cos que correspon a la classe de x mòdul $f(x)$. Quin és l'ordre de α?

(d) És $\alpha = [x]$ un element primitiu? Per què?

(e) Si α és primitiu, doneu una taula d'equivalències amb les notacions potencial, polinomial i vectorial. Si no ho és, trobeu un element primitiu.

Solució:

(una opció)

(a) Hem de donar un polinomi que sigui irreductible i de grau ≥ 2. Seleccionem x^2+1 que té grau 2 i no té arrels i, per tant, és irreductible a $\mathbb{Z}_3[x]$.

(b) $3^2 = 9$.

(c) $\alpha^1 \neq 1$, $\alpha^2 = 2 \neq 1$, $\alpha^3 = 2\alpha \neq 1$, $\alpha^4 = (\alpha^2)^2 = 2^2 = 1$. Per tant, l'ordre de α és 4.

(d) No ho és perquè per ser primitiu hauria de tenir ordre $9-1=8$.

(e) Com en l'exercici anterior, els únics ordres possibles són els divisors de 8 i, per tant, β és primitiu si i només si $\beta^4 \neq 1$. Agafem $\beta = \alpha+1$ i veiem que és un element primitiu. En efecte, $\beta^4 = (\beta^2)^2 = (\alpha^2+2\alpha+1)^2 = (2+2\alpha+1)^2 = (2\alpha)^2 = 4\alpha^2 = \alpha^2 = 2 \neq 1$. Haguéssim pogut agafar $\beta = \alpha+2$, $\beta = 2\alpha+1$, $\beta = 2\alpha+2$ i també ens haurien donat elements primitius.

(una altra opció)

(a) Hem de donar un polinomi que sigui irreductible i de grau ≥ 2. Seleccionem x^2+x+2, que té grau 2 i no té arrels i, per tant, és irreductible a $\mathbb{Z}_3[x]$.

(b) $3^2 = 9$.

(c) $\alpha^1 \neq 1$, $\alpha^2 = 2\alpha+2 \neq 1$, $\alpha^3 = 2\alpha^2+2\alpha = 2\alpha+2 \neq 1$, $\alpha^4 = 2\alpha^2+2\alpha = 2 \neq 1$. Com que l'ordre ha de ser un divisor de $9-1=8$, com que els divisors de 8 són $1,2,4,8$ i com que ja hem comprovat que α no té ordre $1,2$ ni 4, aleshores α ha de tenir ordre 8.

(d) Sí que ho és, perquè té ordre $9-1=8$.

(e)

pot.	pol.	vec.
0	0	00
α^0	1	10
α^1	α	01
α^2	$2\alpha+1$	12
α^3	$2\alpha+2$	22
α^4	2	20
α^5	2α	02
α^6	$\alpha+2$	21
α^7	$\alpha+1$	11

I tantes opcions com ens puguem imaginar, començant per un polinomi irreductible i de grau ≥ 2...

22. (a) Per què per comprovar que un polinomi de grau més petit o igual que tres n'hi ha prou de veure que no té arrels?

(b) Considerem el conjunt P de polinomis amb coeficients a $\mathbb{Z}_3$ que tenen exactament un monomi de grau senar i coeficient 1 i la resta de monomis de grau parell. Podeu-ne un exemple.

(c) Demostreu que un polinomi $p \in P$ que sigui irreductible ha de complir

i. La suma dels seus coeficients no és múltiple de 3.

ii. La suma dels seus coeficients no és congruent amb 2 mòdul 3.

(d) Doneu una altra condició que ha de complir un polinomi de P que sigui irreductible.

(e) Utilitzeu els apartats anteriors per donar un polinomi que generi $\mathbb{F}_{27}$.

Solució:

(a) Perquè si té grau 2 només pot descompondre en producte de dos polinomis de grau 1 mentre que si té grau 3 només pot descompondre en producte d'un polinomi de grau 1 per un altre de grau 2 o bé en producte de tres polinomis de grau 1. En tots els casos cal un factor de grau 1. Però si no té arrels aleshores no té factors de grau 1 i, per tant, no es pot descompondre i és irreductible.

(b) $x^3 + x^2 + 2 \in P$.

(c) i. La suma dels coeficients de p és $p(1)$. Si $p(1)$ és un múltiple de 3 aleshores s'anul·la a $\mathbb{Z}_3$ i 1 és una arrel de p. Per tant, p no és irreductible.

ii. Tenim que $2^2 = 4 = 1$ a $\mathbb{Z}_3$. Per tant, $2^r = \begin{cases} 1 \text{ si } r \text{ és parell} \\ 2 \text{ si } r \text{ és senar} \end{cases}$

Tenim que $p(2)$ és la suma de coeficients més 1 i, per tant, $p(2)$ no s'anul·la a $\mathbb{Z}_3$ si i només si la suma de coeficients és congruent amb 2 mòdul 3.

(d) El coeficient constant, com que és $p(0)$, no ha de ser nul.

(e) $x^3 + 2x^2 + 1$ o bé $x^3 + x^2 + 2$.

23. (a) Quants polinomis mònics hi ha a $\mathbb{Z}_3[x]$ de grau 2?

Solució:

Hi ha 9 polinomis mònics de grau 2 a $\mathbb{Z}_3[x]$, ja que són tots els polinomis de la forma $x^2 + ax + b$ amb a i b variant cadascun en els tres valors de $\mathbb{Z}_3$.

(b) Quins són els polinomis irreductibles mònics de $\mathbb{Z}_3[x]$ de grau 2? Justifiqueu la resposta.

Solució:

El polinomi $x^2 + ax + b$, per ser irreductible, com que té grau 2, no ha de tenir arrels. Perquè 0 no sigui arrel cal que $0^2 + 0a + b \neq 0$. Això implica $b = 1$ o $b = 2$. Perquè 1 no sigui arrel, cal que $1 + a + b \neq 0$. Perquè que 2 no sigui arrel cal que $4 + 2a + b \neq 0$. Això ens dona tres opcions:

- $b = 1$, $a = 0$
- $b = 2$, $a = 1$
- $b = 2$, $a = 2$

que corresponen als tres polinomis

- $x^2 + 1$
- $x^2 + x + 2$
- $x^2 + 2x + 2$

(c) Escolliu un dels polinomis irreductibles de l'apartat anterior i digues-li f. Quants elements té $\mathbb{Z}_3/(f)$?

Solució:

9.

(d) Quants elements té $\mathbb{Z}_9$?

Solució:

9.

(e) Quants elements invertibles té $\mathbb{Z}_3/(f)$? Doneu un element invertible de $\mathbb{Z}_3/(f)$ que no sigui l'1 i el seu invers.

Solució:

8 invertibles. Per exemple, 2 és invertible i el seu invers és ell mateix.

(f) Quants elements invertibles té $\mathbb{Z}_9$? Doneu un element invertible de $\mathbb{Z}_9$ que no sigui l'1 i el seu invers.

Solució:

$\phi(9) = 9 - 3 = 6$ invertibles. Com hem vist abans, 7 és invertible i el seu invers és 4.

(g) Doneu un element primitiu de $\mathbb{Z}_3/(f)$ i escriviu totes les seves potències diferents en forma polinomial.

Solució:

La solució dependrà de quin polinomi irreductible haguem agafat. Si agafem el primer, resulta que $\alpha = [x]$ no és un element primitiu, ja que $\alpha^4 = 1$. En aquest cas agafem, per exemple, $\beta = \alpha + 1$. Construïm la taula a partir de β i, al mateix temps que la construïm, veiem que β és primitiu.

pot.	pol. en α	pol. en β
0	0	0
β^0	1	1
β^1	$\alpha + 1$	β
β^2	2α	$2\beta + 1$
β^3	$2\alpha + 1$	$2\beta + 2$
β^4	2	2
β^5	$2\alpha + 2$	2β
β^6	α	$\beta + 2$
β^7	$\alpha + 2$	$\beta + 1$

Si agafem el polinomi $x^2 + x + 2$ i anomenem $\alpha = [x]$, aleshores α és primitiu i ens dona la taula d'equivalències següent:

pot.	pol.
0	0
α^0	1
α^1	α
α^2	$2\alpha + 1$
α^3	$2\alpha + 2$
α^4	2
α^5	2α
α^6	$\alpha + 2$
α^7	$\alpha + 1$

Si agafem el polinomi $x^2 + 2x + 2$ i anomenem $\alpha = [x]$, aleshores α és primitiu i ens dona la taula d'equivalències següent:

pot.	pol.
0	0
α^0	1
α^1	α
α^2	$\alpha + 1$
α^3	$2\alpha + 1$
α^4	2
α^5	2α
α^6	$2\alpha + 2$
α^7	$\alpha + 2$

(h) Doneu un element primitiu de $\mathbb{Z}_9$ i escriviu totes les seves potències diferents.

Solució:

Per exemple el 2.

$$\begin{aligned} 2^0 &= 1 \\ 2^1 &= 2 \\ 2^2 &= 4 \\ 2^3 &= 8 \\ 2^4 &= 7 \\ 2^5 &= 5 \\ 2^6 &= 1 \end{aligned}$$

24. (a) Justifiqueu si són irreductibles els següents polinomis a $\mathbb{Z}_2[x]$.

i. $x^4 + 1$

ii. x^4+x+1
iii. x^4+x^2+1
iv. $x^4+x^3+x^2+x+1$

(b) Escriviu cadascun dels polinomis de l'apartat (a) com a producte de polinomis irreductibles.

(c) Doneu el màxim comú divisor de x^4+1 i x^4+x^2+1.

(d) Podeu expressar el màxim comú divisor de x^4+1 i x^4+x^2+1 com a combinació lineal dels mateixos polinomis? En cas afirmatiu, doneu-ne els coeficients i feu la comprovació. En cas negatiu, doneu-ne una justificació.

(e) Quines de les següents estructures són un cos i, en cas de ser-ho, quants elements tenen?
i. $\mathbb{Z}_2[x]/x^4+1$
ii. $\mathbb{Z}_2[x]/x^4+x+1$
iii. $\mathbb{Z}_2[x]/x^4+x^2+1$
iv. $\mathbb{Z}_2[x]/x^4+x^3+x^2+x+1$

(f) En quins dels casos en què tenim un cos, si anomenem α a la classe de x, tenim que α és un element primitiu?

(g) Doneu una taula exponencial-polinòmica-vectorial per un cas en què α sigui primitiu. Els apartats que segueixen els referirem al mateix cas (la mateixa α i la mateixa taula).

(h) Quins són els ordres possibles dels elements del cos?

(i) Per a cadascun dels ordres possibles, doneu un element del cos amb aquell ordre.

Solució:

(a) El primer polinomi s'anul·la en 1 i, per tant, és reductible. El segon polinomi no té arrels. Per ser reductible hauria de ser el quadrat de l'únic polinomi reductible de grau 2, és a dir, hauria de ser $(x^2+x+1)^2=x^4+x^2+1$, però veiem que no ho és. Per tant, és irreductible. El tercer polinomi acabem de veure que és $(x^2+x+1)^2=x^4+x^2+1$, per això és reductible. El quart polinomi és irreductible pel mateix argument que el segon.

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

(c) 1, perquè no tenen factors irreductibles en comú.

(d) Utilitzem l'algoritme d'Euclides.

1	0	1	x^2
0	1	-1	x^2+1
		1	x^2
x^4+x^2+1	x^4+1	x^2	1

Obtenim que $(x^2)(x^4+x^2+1)+(x^2+1)(x^4+1)=1$.
Comprovem el resultat: $(x^2)(x^4+x^2+1)+(x^2+1)(x^4+1)=(x^6+x^4+x^2)+(x^6+x^2)+(x^4+1)=1$.

(e) La segona i la quarta. Tenen $2^4=16$ elements.

(f) Sabem que els únics ordres possibles de α són els divisors de 15, és a dir, $1,3,5,15$. Perquè α sigui primitiu cal que el seu ordre sigui màxim, és a dir, 15.
En el segon cas, α té ordre 15, ja que $1,3$ són més petits que el grau del polinomi generador i $\alpha^5=\alpha\alpha^4=\alpha(\alpha+1)=\alpha^2+\alpha\neq 1$. Per tant, α és primitiu.
En el quart cas, $\alpha^5=\alpha(\alpha^3+\alpha^2+\alpha+1)=\alpha^4+\alpha^3+\alpha^2+\alpha=\alpha^3+\alpha^2+\alpha+1+\alpha^3+\alpha^2+\alpha=1$. Per tant, α té ordre $5<15$ i no és primitiu.

(g)

pot.	pol.	vect.
α^0	1	1000
α^1	α	0100
α^2	α^2	0010
α^3	α^3	0001
α^4	$\alpha + 1$	0011
α^5	$\alpha^2 + \alpha$	0110
α^6	$\alpha^3 + \alpha^2$	0011
α^7	$\alpha^3 + \alpha + 1$	1101
α^8	$\alpha^2 + 1$	1010
α^9	$\alpha^3 + \alpha$	0101
α^{10}	$\alpha^2 + \alpha + 1$	1110
α^{11}	$\alpha^3 + \alpha^2 + \alpha$	0111
α^{12}	$\alpha^3 + \alpha^2 + \alpha + 1$	1111
α^{13}	$\alpha^3 + \alpha^2 + 1$	1011
α^{14}	$\alpha^3 + 1$	1001

(h) Tots els divisors de $16 - 1 = 15$, que són $1, 3, 5, 15$.

(i) 1 té ordre 1, $\alpha^5 = \alpha^2 + \alpha$ té ordre 3, α^3 té ordre 5 i α té ordre 15.

25. (a) Doneu un anell $\mathbb{Z}_m$ i un polinomi de $\mathbb{Z}_m[x]$ amb els qual es pugui construir $\mathbb{F}_9$.

(b) Construïu la taula d'equivalències de les notacions polinòmica-exponencial-vectorial a partir d'un element primitiu.

(c) Hi ha algun altre anell $\mathbb{Z}_m$ amb el qual haguéssim pogut construir $\mathbb{F}_9$? En cas afirmatiu, doneu-ne un altre.

(d) Hi ha algun altre polinomi de $\mathbb{Z}_m[x]$ amb el qual es pugui construir $\mathbb{F}_9$? En cas afirmatiu, doneu-ne un altre.

(e) Quins són els ordres possibles dels elements de $\mathbb{F}_9$?

(f) Doneu un element de cada ordre possible en cadascuna de les tres notacions (polinòmica, exponencial i vectorial).

(g) Si anomenem α a la classe de x, quin valor té $\frac{\alpha^6(\alpha^3+\alpha^4)}{\alpha^7}$? Doneu el resultat en cadascuna de les tres notacions.

Solució:

(a) L'anell ha de ser $\mathbb{Z}_3$ i el polinomi pot ser qualsevol d'aquests: x^2+1, x^2+x+2, x^2+2x+2, $2x^2+2$, $2x^2+2x+1$, $2x^2+x+1$.

(b) La taula d'equivalències dependrà de quin polinomi irreductible haguem agafat. Si agafem el primer, resulta que $\alpha = [x]$ no és un element primitiu, ja que $\alpha^4 = 1$. En aquest cas agafem, per exemple, $\beta = \alpha + 1$. Construïm la taula a partir de β i, al mateix temps que la construïm, veiem que β és primitiu.

pot.	pol. en α	vec. resp. α	pol. en β	vec. resp. β
0	0	00	0	00
β^0	1	10	1	10
β^1	$\alpha + 1$	11	β	01
β^2	2α	02	$2\beta + 1$	12
β^3	$2\alpha + 1$	12	$2\beta + 2$	22
β^4	2	20	2	20
β^5	$2\alpha + 2$	22	2β	02
β^6	α	01	$\beta + 2$	21
β^7	$\alpha + 2$	21	$\beta + 1$	11

Si agafem el polinomi $x^2 + x + 2$ i anomenem $\alpha = [x]$, aleshores α és primitiu i ens dona la taula d'equivalències següent:

pot.	pol.	vec.
0	0	00
α^0	1	10
α^1	α	01
α^2	$2\alpha + 1$	12
α^3	$2\alpha + 2$	22
α^4	2	20
α^5	2α	02
α^6	$\alpha + 2$	21
α^7	$\alpha + 1$	11

Si agafem el polinomi $x^2 + 2x + 2$ i anomenem $\alpha = [x]$, aleshores α és primitiu i ens dona la taula d'equivalències següent:

pot.	pol.	vec.
0	0	00
α^0	1	10
α^1	α	01
α^2	$\alpha + 1$	11
α^3	$2\alpha + 1$	12
α^4	2	20
α^5	2α	02
α^6	$2\alpha + 2$	22
α^7	$\alpha + 2$	21

Si agafem qualsevol dels altres tres polinomis irreductibles podem construir la taula de manera semblant a les anteriors.

(c) No.

(d) Qualsevol dels altres polinomis mencionats al primer apartat.

(e) 1, 2, 4, 8.

(f) Si $\alpha = [x]$ és primitiu tenim:

- ordre 1: 1,
- ordre 2: α^4,
- ordre 4: α^2,
- ordre 8: α.

Les notacions polinomial i vectorial dependran del polinomi escollit i ens vindran donades per la taula. En el segon cas, per exemple, tindríem $1 \equiv 10$, $2 \equiv 20$, $2\alpha + 1 \equiv 12$, $\alpha \equiv 01$, respectivament, mentre que en el tercer cas tindrem $1 \equiv 10$, $2 \equiv 20$, $\alpha + 1 \equiv 11$, $\alpha \equiv 01$, respectivament. Si α no és primitiu, agafem β primitiu i tenim:

- ordre 1: 1,
- ordre 2: β^4,
- ordre 4: β^2,
- ordre 8: β.

Les notacions polinomial i vectorial dependran del polinomi escollit i ens vindran donades per la taula. En el primer cas, per exemple, tindríem $1 \equiv 10_\alpha \equiv 10_\beta$, $2 \equiv 20_\alpha \equiv 20_\beta$, $2\alpha = 2\beta + 1 \equiv 02_\alpha \equiv 12_\beta$, $\alpha + 1 = \beta \equiv 11_\alpha \equiv 01_\beta$, respectivament.

(g) Dependrà del polinomi escollit. Per exemple, si agafem el primer, podem utilitzar que $\alpha^2 = 2$ i que $\alpha^4 = 1$ i el càlcul queda reduït de la manera següent: $\frac{a^6(\alpha^3+\alpha^4)}{\alpha^7} = \frac{2(2\alpha+1)}{2\alpha} = \frac{2\alpha+1}{\alpha} = \frac{\beta^3}{\beta^6} = \beta^{-3} = \beta^5 = 2\alpha + 2 \equiv 22_\alpha = 02_\beta$.

Si agafem el segon, $\frac{a^6(\alpha^3+\alpha^4)}{\alpha^7} = \frac{\alpha^6\alpha^2}{\alpha^7} = \alpha \equiv 01$.

Si agafem el tercer, $\frac{a^6(\alpha^3+\alpha^4)}{\alpha^7} = \frac{\alpha^6\alpha^5}{\alpha^7} = \alpha^4 = 2 \equiv 20$.

26. (a) Doneu un anell $\mathbb{Z}_m$ i un polinomi de $\mathbb{Z}_m[x]$ amb els quals es pugui construir $\mathbb{F}_{16}$.
    (b) Construïu la taula d'equivalències de les notacions polinòmica-exponencial-vectorial a partir d'un element primitiu.
    (c) Hi ha algun altre anell $\mathbb{Z}_m$ amb el qual haguéssim pogut construir $\mathbb{F}_{16}$? En cas afirmatiu, doneu-los tots.
    (d) Hi ha algun altre polinomi de $\mathbb{Z}_m[x]$ amb el qual es pugui construir $\mathbb{F}_{16}$? En cas afirmatiu, doneu-los tots.
    (e) Quins són els ordres possibles dels elements de $\mathbb{F}_{16}$?
    (f) Doneu un element de cada ordre possible en cadascuna de les tres notacions (polinòmica, exponencial i vectorial).
    (g) Si anomenem α a la classe de x, quin valor té $\frac{\alpha^6(\alpha^3+\alpha^4)}{\alpha^7}$? Doneu el resultat en cadascuna de les tres notacions.

Solució:

(a) L'anell ha de ser $\mathbb{Z}_2$ i el polinomi pot ser qualsevol d'aquests: x^4+x+1, x^4+x^3+1, $x^4+x^3+x^2+x+1$.

(b) La taula d'equivalències dependrà de quin polinomi irreductible haguem agafat. Si agafem el primer, tenim la taula d'equivalències següent, on α és la classe de x.

pot.	pol.	vec.
0	0	0000
α^0	1	1000
α^1	α	0100
α^2	α^2	0010
α^3	α^3	0001
α^4	$\alpha+1$	1100
α^5	$\alpha^2+\alpha$	0110
α^6	$\alpha^3+\alpha^2$	0011
α^7	$\alpha^3+\alpha+1$	1101
α^8	α^2+1	1010
α^9	$\alpha^3+\alpha$	0101
α^{10}	$\alpha^2+\alpha+1$	1110
α^{11}	$\alpha^3+\alpha^2+\alpha$	0111
α^{12}	$\alpha^3+\alpha^2+\alpha+1$	1111
α^{13}	$\alpha^3+\alpha^2+1$	1011
α^{14}	α^3+1	1001
α^{15}	1	1000

Si agafem el segon, tenim la taula d'equivalències següent, on α és la classe de x.

pot.	pol.	vec.
0	0	0000
α^0	1	1000
α^1	α	0100
α^2	α^2	0010
α^3	α^3	0001
α^4	α^3+1	1001
α^5	$\alpha^3+\alpha+1$	1101
α^6	$\alpha^3+\alpha^2+\alpha+1$	1111
α^7	$\alpha^2+\alpha+1$	1110
α^8	$\alpha^3\alpha^2+\alpha$	0111
α^9	α^2+1	1010
α^{10}	$\alpha^3+\alpha$	0101
α^{11}	$\alpha^3+\alpha^2+1$	1011
α^{12}	$\alpha+1$	1100
α^{13}	$\alpha^2+\alpha$	0110
α^{14}	$\alpha^3+\alpha^2$	0011
α^{15}	1	1000

Si agafem el tercer, resulta que $\alpha = [x]$ no és un element primitiu. En efecte,

pot.	pol.	vec.
0	0	0000
α^0	1	1000
α^1	α	0100
α^2	α^2	0010
α^3	α^3	0001
α^4	$\alpha^3+\alpha^2+\alpha+1$	1111
α^5	1	1000

En aquest cas agafem, per exemple, $\beta = \alpha+1$. Construïm la taula a partir de β i, al mateix temps que la construïm, veiem que β és primitiu.

pot.	pol. en α	vec. resp. α
0	0	0000
β^0	1	1000
β^1	$\alpha+1$	1100
β^2	α^2+1	1010
β^3	$\alpha^3+\alpha^2+\alpha+1$	1111
β^4	$\alpha^3+\alpha^2+\alpha$	0111
β^5	$\alpha^3+\alpha^2+1$	1011
β^6	α^3	0001
β^7	$\alpha^2+\alpha+1$	1110
β^8	α^3+1	1001
β^9	α^2	0010
β^{10}	$\alpha^3+\alpha^2$	0011
β^{12}	$\alpha^3+\alpha+1$	1101
β^{13}	α	0100
β^{12}	$\alpha^2+\alpha$	0110
β^{14}	$\alpha^3+\alpha$	0101
β^{15}	1	1000

(c) No.

(d) Qualsevol dels altres polinomis mencionats al primer apartat.

(e) 1, 3, 5, 15.

(f) Si $\alpha = [x]$ és primitiu tenim:
- ordre 1: 1,
- ordre 3: α^5,
- ordre 5: α^3,
- ordre 15: α.

Les notacions polinomial i vectorial dependran del polinomi escollit i ens vindran donades per la taula. En el primer cas, per exemple, tindrem $1 \equiv 1000$, $\alpha^5 = \alpha^2 + \alpha \equiv 0110$, $\alpha^3 \equiv 0001$, $\alpha \equiv 0100$, respectivament, mentre que en el segon cas tindrem $1 \equiv 1000$, $\alpha^5 = \alpha^3 + \alpha + 1 \equiv 1101$, $\alpha^3 \equiv 0001$, $\alpha \equiv 0100$, respectivament. Si α no és primitiu, agafem β primitiu i tenim:
- ordre 1: 1,
- ordre 3: β^5,
- ordre 5: β^3,
- ordre 15: β.

Les notacions polinomial i vectorial dependran del polinomi escollit i ens vindran donades per la taula. En el primer cas, per exemple, tindríem $1 \equiv 1000_\alpha$, $\beta^5 = \alpha^3 + \alpha^2 + 1 \equiv 1011_\alpha$, $\beta^3 = \alpha^3 + \alpha^2 + \alpha + 1 \equiv 1111_\alpha$, $\beta = \alpha + 1 \equiv 1100_\alpha$, respectivament.

(g) Dependrà del polinomi escollit.

27. (a) És $\mathbb{Z}_3$ un cos? Per què?

(b) Comproveu que només hi ha tres polinomis mònics (coeficient de grau màxim igual a 1) irreductibles de grau 2 a $\mathbb{Z}_3[x]$ i doneu-los.

(c) Doneu un polinomi mònic $f(x)$ de grau 2 irreductible de $\mathbb{Z}_3[x]$ amb coeficient de grau 1 igual a 1.

(d) Comproveu si $f(x)$ és primitiu.

(e) Anomenem $\mathbb{F}$ al conjunt $\mathbb{Z}_3[x]/f(x)$. Quants elements té $\mathbb{F}$?

(f) És $\mathbb{F}$ un cos? Per què?

(g) Anomenem α a la classe de x dins de $\mathbb{Z}_3[x]/f(x)$. Doneu una taula d'equivalències exponencial-polinomial-vectorial de les potències de α.

Solució:

(a) $\mathbb{Z}_3$ és un cos perquè 3 és primer.

(b) Per ser irreductible ha de tenir coeficient constant no nul. Només hi ha aquests polinomis mònics de grau 2 amb coeficient constant no nul:
- $x^2 + 1$ (grau 2 i no té arrels, per tant, és irreductible)
- $x^2 + x + 1$ (té arrel 1, per tant, no és irreductible)
- $x^2 + 2x + 1$ (té arrel 2, per tant, no és irreductible)
- $x^2 + 2$ (té arrel 1, per tant, no és irreductible)
- $x^2 + x + 2$ (grau 2 i no té arrels, per tant, és irreductible)
- $x^2 + 2x + 2$ (grau 2 i no té arrels, per tant, és irreductible)

Els únics polinomis mònics irreductibles són 3 i són $x^2 + 1$, $x^2 + x + 2$, $x^2 + 2x + 2$.

(c) L'únic polinomi mònic irreductible amb coeficient lineal igual a 1 és $x^2 + x + 2$.

(d) És primitiu perquè totes les potències de la classe de x en el quocient $\mathbb{Z}_3[x]/f(x)$ de grau més petit que 8 són diferents, com podem comprovar en la taula de l'apartat (g).

(e) 9.

(f) És un cos perquè 3 és primer i $x^2 + x + 2$ és irreductible.

(g)

pot.	*pol.*	*vect.*
0	0	00
α^0	1	10
α^1	α	01
α^2	$2\alpha+1$	12
α^3	$2\alpha+2$	22
α^4	2	20
α^5	2α	02
α^6	$\alpha+2$	21
α^7	$\alpha+1$	11
α^8	1	

28. Sigui $f(x) = x^6 + x^3 + 1 \in \mathbb{Z}_2[x]$.
    (a) Avalueu f en tots els elements de $\mathbb{Z}_2$ i doneu els resultats obtinguts.
    (b) Té arrels $f(x)$? Si en té, quines són?
    (c) N'hi ha prou amb l'apartat anterior per deteriminar si $f(x)$ és irreductible? Per què?
    (d) Anomenem $F = \mathbb{Z}_2[x]/f(x)$.
        - És F un cos?
        - Per què?
        - Quines comprovacions heu fet?
    (e) Quants elements té F?
    (f) Anomenem a a la classe de x dins de F. Doneu les primeres potències de a fins que alguna potència sigui repetida.
    (g) Quin és l'ordre de a?
    (h) És a un element primitiu de F? Per què?
    (i) Calculeu els següents valors i doneu-los com una potència de a o bé zero.
        - $a^5 - a^{11}$
        - $a^3 + a^{18}$
        - $\frac{a^5-a^{11}}{a^3+a^{18}} + a^{14}$

Solució:

(a) $f(0) = 1$, $f(1) = 1$.

(b) No en té.

(c) No, perquè el grau de f és més gran que 3.

(d)
- Sí.
- Perquè 2 és primer i f és irreductible.
- Hem comprovat (1) 2 és primer; (2) f no té arrels; (3) f no és divisible pels polinomis irreductibles de grau 2 i 3.

(e) $2^6 = 64$.

(f) $a^0 = 1$, $a^1 = a$, $a^2 = a^2$, $a^3 = a^3$, $a^4 = a^4$, $a^5 = a^5$, $a^6 = a^3 + 1$, $a^7 = a^4 + a$, $a^8 = a^5 + a^2$, $a^9 = 1$.

(g) El seu ordre és 9.

(h) No és primitiu perquè el seu ordre és més petit que $64 - 1 = 63$.

(i) Calculeu els següents valors i doneu-los com una potència de a o bé zero.
- $a^5 - a^{11} = a^5 + a^2 = a^8$
- $a^3 + a^{18} = a^3 + 1 = a^6$
- $\frac{a^5-a^{11}}{a^3+a^{18}} + a^{14} = \frac{a^8}{a^6} + a^5 = a^2 + a^5 = a^8$

2 Codis lineals i cíclics

1. Dins de $\mathbb{F}_2^3$ considerem el conjunt de paraules $C = \{(000), (111), (101), (010)\}$.
   (a) Demostreu que C és un codi lineal.
   (b) Doneu una matriu generadora de C.
   (c) Comproveu que totes les paraules de C estan generades per G.
   (d) Doneu una matriu de control de C.
   (e) Justifiqueu quina és la distància mínima de C.
   (f) Comproveu que totes les paraules del codi quan les multipliquem per la matriu de control donen 0.
   (g) Doneu el codi dual $C^{\perp}$.
   (h) Comproveu que les paraules del codi dual quan les multipliquem per la matriu G donen 0.

   Solució:

   (a) Podem comprovar que és un espai vectorial perquè les combinacions lineals de dos vectors qualssevol de C és dins de C. En efecte,

$$\begin{array}{ccccccc}
(000) & + & (000) & = & (000) & \in & C \\
(000) & + & (111) & = & (111) & \in & C \\
(000) & + & (101) & = & (101) & \in & C \\
(000) & + & (010) & = & (010) & \in & C \\
(111) & + & (111) & = & (000) & \in & C \\
(111) & + & (101) & = & (010) & \in & C \\
(111) & + & (010) & = & (101) & \in & C \\
(101) & + & (101) & = & (000) & \in & C \\
(101) & + & (010) & = & (111) & \in & C \\
(010) & + & (010) & = & (000) & \in & C
\end{array}$$

   (b) Per exemple, $G = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}$.

   (c) Vegem com la matriu G genera tot C:

$$\begin{array}{ll}
\begin{pmatrix} 0 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix} & = \begin{pmatrix} 0 & 0 & 0 \end{pmatrix} \\
\begin{pmatrix} 1 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix} & = \begin{pmatrix} 1 & 1 & 1 \end{pmatrix} \\
\begin{pmatrix} 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix} & = \begin{pmatrix} 1 & 0 & 1 \end{pmatrix} \\
\begin{pmatrix} 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix} & = \begin{pmatrix} 0 & 1 & 0 \end{pmatrix}
\end{array}$$

   (d) Com que G té la forma $(I|P)$, podem construir H com $(-P^T|I)$. Ens queda $H = (101)$.

   (e) $d = 1$. Es pot veure per la matriu de control o perquè hi ha una paraula de pes 1 o perquè podem trobar dues paraules a distància 1.

   (f) Podem comprovar que totes les paraules de C quan les multipliquem per H ens donen 0. En efecte,

$$\begin{pmatrix} 1 & 0 & 1 \end{pmatrix}\begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix} = 0$$
$$\begin{pmatrix} 1 & 0 & 1 \end{pmatrix}\begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix} = 0$$
$$\begin{pmatrix} 1 & 0 & 1 \end{pmatrix}\begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix} = 0$$
$$\begin{pmatrix} 1 & 0 & 1 \end{pmatrix}\begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} = 0$$

(g) El codi dual és el que està generat per H. En el nostre cas és $\{0H, 1H\} = \{(000), (101)\}$.

(h)

$$\begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}\begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix}$$
$$\begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}\begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix}$$

2. Considerem el codi ternari C generat per la matriu

$$\begin{pmatrix} 1 & 1 & 1 & 0 \\ 2 & 0 & 1 & 1 \end{pmatrix}$$

(a) Quantes paraules té aquest codi?

(b) Doneu totes les paraules del codi.

(c) Doneu la distància mínima del codi. **Justifiqueu la resposta**.

(d) Quina dimensió té el codi dual? **Justifiqueu la resposta**.

(e) Doneu dues paraules (no múltiples una de l'altra) del codi dual. **Justifiqueu la resposta**.

(f) Quina relació hi ha entre C i $C^{\perp}$?

(g) Trobeu una matriu de control del codi.

(h) Corregiu el missatge rebut 212112012222.

Solució:

(a) La dimensió del codi és el nombre de files de la matriu generadora que és 2. Aleshores el codi té 9 paraules perquè té dimensió 2 i és sobre $\mathbb{Z}_3$.

(b) Les paraules s'obtenen multiplicant la matriu generadora per tots els possibles vectors de dues coordenades de $\mathbb{Z}_3$:

$$(00)\begin{pmatrix} 1 & 1 & 1 & 0 \\ 2 & 0 & 1 & 1 \end{pmatrix} = (0000) \quad (10)\begin{pmatrix} 1 & 1 & 1 & 0 \\ 2 & 0 & 1 & 1 \end{pmatrix} = (1110) \quad (20)\begin{pmatrix} 1 & 1 & 1 & 0 \\ 2 & 0 & 1 & 1 \end{pmatrix} = (2220)$$
$$(01)\begin{pmatrix} 1 & 1 & 1 & 0 \\ 2 & 0 & 1 & 1 \end{pmatrix} = (2011) \quad (11)\begin{pmatrix} 1 & 1 & 1 & 0 \\ 2 & 0 & 1 & 1 \end{pmatrix} = (0121) \quad (21)\begin{pmatrix} 1 & 1 & 1 & 0 \\ 2 & 0 & 1 & 1 \end{pmatrix} = (1201)$$
$$(02)\begin{pmatrix} 1 & 1 & 1 & 0 \\ 2 & 0 & 1 & 1 \end{pmatrix} = (1022) \quad (12)\begin{pmatrix} 1 & 1 & 1 & 0 \\ 2 & 0 & 1 & 1 \end{pmatrix} = (2102) \quad (22)\begin{pmatrix} 1 & 1 & 1 & 0 \\ 2 & 0 & 1 & 1 \end{pmatrix} = (0212)$$

(c) La distància mínima és 3 perquè totes les paraules, excepte la nul·la, tenen pes 3.

(d) El codi dual, com que està generat per la matriu de control, té com a dimensió dimensió el nombre de files de la matriu de control que és $n - k = 2$.

(e) Observem que les dues files de la matriu generadora quan les multipliquem per la matriu generadora ens donen 0. Per tant, podem donar les paraules 1110 i 2011.

(f) C i $C^{\perp}$ són iguals, ja que $C^{\perp}$ té dimensió 2 i, per tant, està generat per la mateixa matriu generadora de C.

(g) Com que C i $C^{\perp}$ són iguals, la mateixa matriu generadora és matriu de control.

(h) Podem corregir per síndrome o per observació de les paraules del codi. Com que la distància mínima és 3, només es pot corregir un error. Per cada bloc, si trobem una paraula del codi a distància 1 (o 0), aquesta és la paraula corregida. Així doncs, la seqüència corregida ens queda 0121 1201 2220.

3. A $\mathbb{Z}_5$ considerem el codi C_1 que té matriu de control

$$\begin{pmatrix} 3 & 1 & 3 & 2 & 1 \\ 4 & 1 & 0 & 4 & 1 \\ 3 & 2 & 2 & 0 & 3 \end{pmatrix}$$

(a) Doneu una matriu de control de C_1 sistemàtica per la dreta.

(b) Doneu una matriu generadora de C_1.

(c) Quina és la dimensió de C_1?

(d) Quina és la longitud de C_1?

(e) Quina és la distància mínima de C_1?

(f) Quants esborralls es poden corregir?

(g) Quants errors es poden corregir?

(h) Corregiu els esborralls de la paraula $(324??)$ i doneu la paraula corregida.

(i) Rebem la paraula (43031). Escolliu una matriu de control de les anteriors i doneu la síndrome de la paraula rebuda.

(j) Quants errors hi ha i en quines posicions es troben?

(k) Quins són els valors dels errors?

(l) Doneu la paraula corregida.

Solució:

(a) Transformem la matriu donada en una d'equivalent amb una identitat a la dreta:

$$\begin{pmatrix} 3 & 1 & 3 & 2 & 1 \\ 4 & 1 & 0 & 4 & 1 \\ 3 & 2 & 2 & 0 & 3 \end{pmatrix} \underset{\substack{f1' = 2f1 \\ f3' = f3 + f2}}{\sim} \begin{pmatrix} 1 & 2 & 1 & 4 & 2 \\ 4 & 1 & 0 & 4 & 1 \\ 1 & 3 & 0 & 2 & 4 \end{pmatrix}$$

$$\underset{\substack{f1' = f1 - f2 \\ f2' = 4f2 \\ f3' = f3 + 2f2}}{\sim} \begin{pmatrix} 2 & 1 & 1 & 0 & 1 \\ 1 & 4 & 0 & 1 & 4 \\ 4 & 0 & 0 & 0 & 1 \end{pmatrix}$$

$$\underset{\substack{f1' = f1 - f3 \\ f2' = f2 + f3}}{\sim} \begin{pmatrix} 3 & 1 & 1 & 0 & 0 \\ 0 & 4 & 0 & 1 & 0 \\ 4 & 0 & 0 & 0 & 1 \end{pmatrix}$$

(b) Com que en l'apartat anterior hem obtingut una matriu de control sistemàtica de la forma $(P|I)$, ara podem trobar la generadora de la forma $(I| - P^T)$.

$$\begin{pmatrix} 1 & 0 & 2 & 0 & 1 \\ 0 & 1 & 4 & 1 & 0 \end{pmatrix}$$

(c) La dimensió del codi és el nombre de files de la matriu generadora, que és 2.

(d) La longitud del codi és el nombre de columnes de la matriu generadora, que és 5.

(e) Per calcular la distància mínima comprovem que no pot ser 1 perquè no hi ha cap columna nul·la en H ni pot ser 2 perquè no hi ha cap parella de columnes linealment dependents. Sí que hi ha tres columnes linealment dependents, per exemple la primera, la tercera i la cinquena. Per això la distància mínima és $d = 3$.

(f) Es podran corregir $d - 1 = 2$ esborralls.

(g) Es podran corregir $\lfloor \frac{d-1}{2} \rfloor = 1$ errors.

(h) Per corregir la paraula amb esborralls resolem el sistema

$$\begin{pmatrix} 3 & 1 & 1 & 0 & 0 \\ 0 & 4 & 0 & 1 & 0 \\ 4 & 0 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 3 \\ 2 \\ 4 \\ x \\ y \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix},$$

que té solució $x = 2$ i $y = 3$. Per tant, la paraula corregida és (32423).

(i) La síndrome de (43031) és, si fem servir la matriu de l'enunciat,

$$\begin{pmatrix} 3 & 1 & 3 & 2 & 1 \\ 4 & 1 & 0 & 4 & 1 \\ 3 & 2 & 2 & 0 & 3 \end{pmatrix} \begin{pmatrix} 4 \\ 3 \\ 0 \\ 3 \\ 1 \end{pmatrix} = \begin{pmatrix} 2 \\ 2 \\ 1 \end{pmatrix},$$

o bé, si fem servir la matriu sistemàtica,

$$\begin{pmatrix} 3 & 1 & 1 & 0 & 0 \\ 0 & 4 & 0 & 1 & 0 \\ 4 & 0 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 4 \\ 3 \\ 0 \\ 3 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 2 \end{pmatrix}.$$

(j) En tots dos casos veiem que la síndrome és dues vegades la cinquena columna de H. Per tant, hi ha un error a la cinquena posició.

(k) El valor de l'error és 2.

(l) La paraula corregida és $(43031) - (00002) = (43034)$.

4. (a) Quants símbols diferents hi ha a $\mathbb{F}_{125}$?

   (b) Quins són els dígits d'un codi sobre $\mathbb{F}_{125}$?

   (c) Quants dígits té cada símbol?

5. (a) Doneu justificadament un polinomi en x que generi $\mathbb{F}_4$.

   (b) Doneu una taula exponencial-vectorial de $\mathbb{F}_4$.

   (c) Anomenem α a la classe de x dins de $\mathbb{F}_4$. Considerem el codi C amb matriu generadora

$$G = \begin{pmatrix} 1 & \alpha & \alpha & 1 \\ 0 & \alpha^2 & 0 & \alpha^2 \end{pmatrix}.$$

   Codifiqueu la cadena de bits 011001001111 i doneu el resultat també amb bits.

   (d) Doneu una matriu de control del codi.

   (e) Quina és la distància mínima del codi C?

(f) Quants errors es poden corregir en cada paraula rebuda? I quants esborralls? Quants errors es poden detectar?

(g) Detecteu si hi ha errors en la cadena codificada de bits

$$011111010011001000000000.$$

(h) En quina posició ha de ser un error per poder-lo corregir?

Solució:

(a) Els polinomis irreductibles de grau 2 de $\mathbb{Z}_2[x]$ seran aquells que no s'anul·lin a 0 (coef. constant 1) ni a 1 (nombre senar de termes no nuls). L'únic polinomi amb aquestes característiques és $x^2 + x + 1$.

(b)

0	00
1	10
α	01
α^2	11

(c) La cadena de bits representa la cadena de símbols $\alpha 1 \alpha 0 \alpha^2 \alpha^2$. Multipliquem cada parell de símbols per la matriu generadora:

$$\alpha 0 \alpha^2 1 \quad \alpha \alpha^2 \alpha^2 \alpha \quad \alpha^2 \alpha^2 11.$$

El resultat en bits serà

$$01001110 \;\; 01111101 \;\; 11111010.$$

(d) La matriu generadora sistemàtica serà

$$\begin{pmatrix} 1 & 0 & \alpha & \alpha^2 \\ 0 & 1 & 0 & 1 \end{pmatrix}.$$

Per tant, com a matriu de control podem agafar

$$\begin{pmatrix} \alpha & 0 & 1 & 0 \\ \alpha^2 & 1 & 0 & 1 \end{pmatrix}.$$

(e) Com que hi ha dues columnes iguals i no hi ha cap columna nul·la, la distància mínima és 2.

(f) No es pot corregir cap error, es pot corregir un esborrall i es pot detectar un error.

(g) De les tres paraules codificades només té error la paraula del mig (multiplicada per la matriu de control dona $\neq 0$).

6. (a) Comproveu que el polinomi $x^2 + 2x + 2$ és irreductible i primitiu a $\mathbb{Z}_3[x]$.

(b) Doneu una taula exponencial-vectorial de $\mathbb{Z}_3[x]/x^2 + 2x + 2$ respecte l'element $\alpha = [x]$.

(c) Considerem el codi C amb matriu generadora

$$G = \begin{pmatrix} 1 & \alpha & \alpha^2 & \alpha^3 \\ 0 & \alpha^4 & 0 & 1 \end{pmatrix}.$$

Codifiqueu la cadena de trits 01211022. Doneu el resultat també com a cadena de trits.

(d) Doneu una matriu de control del codi.

(e) Quina és la distància mínima de C?

(f) Quants errors es poden corregir en cada paraula rebuda? I quants esborralls? Quants errors es poden detectar?

(g) Corregiu els esborralls de la cadena de trits 0112??22. Doneu el resultat en trits.

Solució:

(a) El polinomi és irreductible perquè té grau 2 i no té arrels ($f(0) = 2$, $f(1) = 2$ i $f(2) = 2$). Si fem totes les potències de $\alpha = [x]$ veiem que són diferents fins que arribem a $\alpha^8 = 1$. Per això el polinomi és primitiu.

(b)

exp.	*vect.*
0	00
1	10
α	01
α^2	11
α^3	12
α^4	20
α^5	02
α^6	22
α^7	21

(c) Com que els elements de $\mathbb{Z}_3[x]/x^2 + 2x + 2$ es representen per dos trits cadascun, per poder passar la cadena de trits a cadena de símbols haurem d'agrupar els trits de 2 en 2. Així, la cadena de trits 01211022 la separem com $(01)(21)(10)(22)$. A cada parella de trits li fem correspondre un símbol seguint la taula de l'apartat anterior. Obtenim la cadena de símbols $\alpha\alpha^7 1\alpha^6$. Ara, per poder codificar la cadena de símbols, la separem en blocs de $k = 2$ símbols: $(\alpha\alpha^7)(1\alpha^6)$. Multipliquem cada bloc per la matriu generadora:

$$\begin{pmatrix} \alpha & \alpha^7 \end{pmatrix} \begin{pmatrix} 1 & \alpha & \alpha^2 & \alpha^3 \\ 0 & \alpha^4 & 0 & 1 \end{pmatrix} = \begin{pmatrix} \alpha & 2 & \alpha^3 & \alpha^2 \end{pmatrix}$$

$$\begin{pmatrix} 1 & \alpha^6 \end{pmatrix} \begin{pmatrix} 1 & \alpha & \alpha^2 & \alpha^3 \\ 0 & \alpha^4 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & \alpha^3 & \alpha^2 & \alpha \end{pmatrix}$$

i obtenim la cadena de símbols

$$\alpha, 2, \alpha^3, \alpha^2 \quad 1, \alpha^3, \alpha^2 \alpha,$$

que correspon a la cadena de trits

$$01201211 \quad 10121101.$$

(d) La matriu generadora és equivalent a

$$\begin{pmatrix} 1 & \alpha & \alpha^2 & \alpha^3 \\ 0 & 1 & 0 & 2 \end{pmatrix},$$

que és equivalent a

$$\begin{pmatrix} 1 & 0 & \alpha^2 & 1 \\ 0 & 1 & 0 & 2 \end{pmatrix}.$$

Per tant, com a matriu de control podem agafar

$$H = \begin{pmatrix} \alpha^6 & 0 & 1 & 0 \\ 2 & 1 & 0 & 1 \end{pmatrix}.$$

(e) Com que hi ha dues columnes linealment dependents i no hi ha cap columna nul·la, la distància mínima és 2.

(f) No es pot corregir cap error, es pot corregir un esborrall i es pot detectar un error.

(g) La cadena de trits representa el vector $\alpha\alpha^3 x\alpha^6$. Perquè aquest vector sigui del codi, cal que en multiplicar-lo per H ens doni el vector nul.

$$H \cdot \begin{pmatrix} \alpha \\ \alpha^3 \\ x \\ \alpha^6 \end{pmatrix} = \begin{pmatrix} \alpha^7 + x \\ 0 \end{pmatrix}.$$

Deduïm que

$$x + \alpha^7 = 0.$$

Per tant, $x = -\alpha^7 = \alpha^3$. La paraula codi corregida és $\alpha\alpha^3\alpha^3\alpha^6$, que correspon a la cadena de trits

$$01121222.$$

7. (a) Comproveu que el polinomi $x^4 - 1$ té 4 arrels diferents a $\mathbb{Z}_5$.
   (b) Doneu el polinomi generador d'un codi C primitiu cíclic sobre $\mathbb{Z}_5$ de dimensió 2 (l'apartat anterior us pot ajudar).
   (c) Quina longitud té el codi?
   (d) Doneu el polinomi de control del codi.
   (e) Doneu una matriu generadora del codi.
   (f) Doneu una matriu de control del codi.
   (g) Quina és la distància mínima de C?
   (h) Quants errors podem detectar amb aquest codi?
   (i) Codifiqueu de manera sistemàtica en les darreres posicions la informació 2014. Utilitzeu tantes paraules com sigui necessari.
   (j) Comproveu que les paraules obtingudes en l'apartat anterior pertanyen al codi per tres procediments diferents:
      - Mitjançant el polinomi generador.
      - Mitjançant el polinomi de control.
      - Mitjançant la matriu de control.

Solució:

(a) Veiem que $1, 2, 3, 4$ són arrels i són totes diferents. Per tant, $x^4 - 1 = (x-1)(x-2)(x-3)(x-4)$.

(b) Haurà de ser $n = 4$ i, per tant, el polinomi generador haurà de ser un divisor de grau 2 de $x^4 - 1$. Per l'apartat anterior, pot ser qualsevol de
   - $(x-1)(x-2) = x^2 + 2x + 2$
   - $(x-1)(x-3) = x^2 + x + 3$
   - $(x-1)(x-4) = x^2 + 4$
   - $(x-2)(x-3) = x^2 + 1$
   - $(x-2)(x-4) = x^2 + 4x + 3$
   - $(x-3)(x-4) = x^2 + 3x + 2$.

   Com a exemple de resolució agafem $g(x) = x^2 + 2x + 2$.

(c) $n = q - 1 = 4$.

(d) $h(x) = \frac{x^4-1}{g(x)} = \frac{(x-1)(x-2)(x-3)(x-4)}{(x-1)(x-2)} = (x-3)(x-4) = x^2 + 3x + 2$.

(e) Com a matriu generadora podem agafar

$$G = \begin{pmatrix} 2 & 2 & 1 & 0 \\ 0 & 2 & 2 & 1 \end{pmatrix}.$$

(f) Com a matriu de control podem agafar la matriu generadora del codi generat pel polinomi recíproc de $h(x)$:

$$H = \begin{pmatrix} 1 & 3 & 2 & 0 \\ 0 & 1 & 3 & 2 \end{pmatrix}.$$

(g) El mínim nombre de columnes linealment dependents de H és 3 i, per tant, aquesta és la distància mínima.

(h) $\lfloor \frac{d-1}{2} \rfloor = 1$.

(i) Separem en dos blocs:

- (20): $i_1(x) = 2$, $i_1(x)x^{n-k} = 2x^2$, $R(x) = x + 1$, $i_1(x)x^{n-k} - R(x) = 2x^2 + 4x + 4$ i obtenim la paraula codi $(4, 4, 2, 0)$.
- (14): $i_2(x) = 1 + 4x$, $i_2(x)x^{n-k} = x^2 + 4x^3$, $R(x) = x + 4$, $i_2(x)x^{n-k} - R(x) = 4x^3 + x^2 + 4x + 1$ i obtenim la paraula codi $(1, 4, 1, 4)$.

(j)
- Dividim els polinomis corresponents a les paraules pel polinomi generador i veiem que ens dona residu 0. En efecte, en el primer cas, $(2x^2 + 4x + 4)/(x^2 + 2x + 2) = 2$ i la divisió és exacta. En el segon cas, $(4x^3 + x^2 + 4x + 1)/(x^2 + 2x + 2) = 4x + 3$ i la divisió és exacta.
- Multipliquem els polinomis corresponents a les paraules pel polinomi de control i ens dona un múltiple de $x^4 - 1$. En efecte, en el primer cas, $(2x^2 + 4x + 4)h(x) = 2x^4 + 3 = 2(x^4 - 1)$, mentre que, en el segon, $(4x^3 + x^2 + 4x + 1)h(x) = 4x^5 + 3x^4 + x + 2) = (4x + 3)(x^4 - 1)$.
- $\begin{pmatrix} 1 & 3 & 2 & 0 \\ 0 & 1 & 3 & 2 \end{pmatrix} \begin{pmatrix} 4 \\ 4 \\ 2 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix}$
- $\begin{pmatrix} 1 & 3 & 2 & 0 \\ 0 & 1 & 3 & 2 \end{pmatrix} \begin{pmatrix} 1 \\ 4 \\ 1 \\ 4 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix}$

8. Considerem el codi $\mathcal{C}$ sobre $\mathbb{Z}_3$ donat per les solucions del sistema

$$\begin{cases} x_1 + 2x_3 + x_4 + x_5 + 2x_6 = 0 \\ x_1 + 2x_2 + x_3 + 2x_4 + 2x_6 = 0 \end{cases}$$

(a) Doneu una matriu G generadora de $\mathcal{C}$.

(b) Doneu una matriu H de control de $\mathcal{C}$.

(c) Com és el producte GH^T? I el producte HG^T? Comproveu-ho.

(d) Doneu la longitud i la dimensió de $\mathcal{C}$.

(e) Doneu la distància mínima de $\mathcal{C}$.

(f) Podem corregir algun esborrall? En cas afirmatiu

i. Digueu quants.

ii. Poseu un exemple detallat de correcció d'esborralls.

En cas negatiu

i. Justifiqueu per què no.

ii. Poseu un exemple detallat en què no es corregeixi bé cap esborrall.

(g) Rebem la paraula 221220

i. Quina és la seva síndrome?

ii. És del codi? En cas negatiu, si es pot corregir, expliqueu quina seria la paraula del codi corregida; si no es pot corregir, doneu més d'una paraula que es trobin a distància mínima.

(h) Rebem la paraula 110102

i. Quina és la seva síndrome?

ii. És del codi? En cas negatiu, si es pot corregir, expliqueu quina seria la paraula del codi corregida; si no es pot corregir, doneu més d'una paraula que es trobin a distància mínima.

(i) Rebem la paraula 022202

i. Quina és la seva síndrome?

ii. És del codi? En cas negatiu, si es pot corregir, expliqueu quina seria la paraula del codi corregida; si no es pot corregir, doneu més d'una paraula que es trobin a distància mínima.

(j) Rebem la paraula 210120

i. Quina és la seva síndrome?

ii. És del codi? En cas negatiu, si es pot corregir, expliqueu quina seria la paraula del codi corregida; si no es pot corregir, doneu més d'una paraula que es trobin a distància mínima.

Solució:

(a) Una matriu de control ve donada pel sistema d'equacions i és

$$H = \begin{pmatrix} 1 & 0 & 2 & 1 & 1 & 2 \\ 1 & 2 & 1 & 2 & 0 & 2 \end{pmatrix}$$

En busquem una d'equivalent que sigui sistemàtica:

$$\begin{pmatrix} 1 & 0 & 2 & 1 & 1 & 2 \\ 1 & 2 & 1 & 2 & 0 & 2 \end{pmatrix} \sim \begin{pmatrix} 1 & 0 & 2 & 1 & 1 & 2 \\ 0 & 2 & 2 & 1 & 2 & 0 \end{pmatrix} \sim \begin{pmatrix} 1 & 0 & 2 & 1 & 1 & 2 \\ 0 & 1 & 1 & 2 & 1 & 0 \end{pmatrix}$$

Deduïm que una matriu generadora és

$$G = \begin{pmatrix} 1 & 2 & 1 & 0 & 0 & 0 \\ 2 & 1 & 0 & 1 & 0 & 0 \\ 2 & 2 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

(b) Una matriu de control l'hem donada en l'apartat anterior i és

$$H = \begin{pmatrix} 1 & 0 & 2 & 1 & 1 & 2 \\ 1 & 2 & 1 & 2 & 0 & 2 \end{pmatrix}$$

(c) El producte GH^T és la matriu nul·la de dimensions 4×2:

$$\begin{pmatrix} 1 & 2 & 1 & 0 & 0 & 0 \\ 2 & 1 & 0 & 1 & 0 & 0 \\ 2 & 2 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 2 \\ 2 & 1 \\ 1 & 2 \\ 1 & 0 \\ 2 & 2 \end{pmatrix} = \begin{pmatrix} 3 & 6 \\ 3 & 6 \\ 3 & 6 \\ 3 & 3 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \\ 0 & 0 \\ 0 & 0 \end{pmatrix}$$

El producte HG^T és la matriu nul·la de dimensions 2×4:

$$\begin{pmatrix} 1 & 0 & 2 & 1 & 1 & 2 \\ 1 & 2 & 1 & 2 & 0 & 2 \end{pmatrix} \begin{pmatrix} 1 & 2 & 2 & 1 \\ 2 & 1 & 2 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 50 & 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 3 & 3 & 3 & 3 \\ 6 & 6 & 6 & 3 \end{pmatrix} = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

(d) $n = 6$, $k = n - 2 = 4$.

(e) $d = 2$ perquè hi ha dues columnes de H que són linealment dependents.

(f) Es pot corregir un esborrall. Per exemple, suposem que rebem la paraula 10000?. Resolem el sistema $H \cdot \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ x \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix}$ equivalent a $2x + 1 = 0$. Deduïm que $x = 1$ i, per tant, la paraula corregida és 100001.

(g) La síndrome és $\begin{pmatrix} 2 \\ 2 \end{pmatrix}$. No es pot corregir perquè l'error tant podria ser 200000 com 000001. A distància mínima (igual a 1) hi trobem 021220 i 221222.

(h) La síndrome és $\begin{pmatrix} 0 \\ 0 \end{pmatrix}$. És del codi.

(i) La síndrome és $\begin{pmatrix} 1 \\ 2 \end{pmatrix}$. No es pot corregir perquè l'error tant podria ser 002000 com 000100. A distància mínima (igual a 1) hi trobem 020202 i 022102.

(j) La síndrome és $\begin{pmatrix} 2 \\ 0 \end{pmatrix}$. L'error és únic perquè només pot ser 00020. Per tant, la paraula corregida serà 210100.

9. (a) Doneu la matriu de control d'un codi binari de dimensió 3 capaç de corregir un esborrall en una paraula codificada.
   (b) Poseu un exemple de paraula del codi i poseu-li un esborrall.
   (c) Expliqueu el procés per corregir l'esborrall de l'apartat anterior.
   (d) Amb el codi que heu construït, es podrien corregir dos esborralls?
   (e) Si en l'apartat anterior heu respost que sí, poseu un exemple de paraula del codi amb dos esborralls i expliqueu el procés per corregir-los. Si en l'apartat anterior heu respost que no, poseu un exemple de paraula amb dos esborralls que no es puguin corregir.

Solució:

(a) Perquè sigui un codi binari cal que la matriu sigui de zeros i uns. Perquè una matriu sigui una matriu de control, cal que totes les seves files siguin linealment independents. Per tenir dimensió 3 cal que el nombre de files de la matriu de control sigui $n - 3$, on n és el nombre de columnes. I, finalment, perquè puguem corregir un esborrall, cal que la distància mínima sigui ≥ 2. Per això n'hi ha prou que no hi hagi cap columna nul·la.

Com a exemple haguéssim pogut donar la matriu

$$\begin{pmatrix} 1 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 \end{pmatrix}$$

(b) Com a matriu generadora podem agafar

$$\begin{pmatrix} 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 & 1 \end{pmatrix}$$

Com a paraula codi, aleshores podem agafar qualsevol fila de la matriu generadora. Per exemple, la primera: 11000. Li podem afegir un esborrall a la primera posició i obtenir ?1000.

(c) Perquè una paraula sigui del codi, en multiplicar-la per la matriu de control ens ha de donar zero. Això ens determina el següent sistema d'equacions:

$$\begin{pmatrix} 1 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 \end{pmatrix} \begin{pmatrix} x \\ 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix} \Longrightarrow \begin{pmatrix} x+1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix} \Longrightarrow x = 1$$

(d) No, perquè la distància mínima és 2 perquè hi ha dues columnes linealment dependents (o també perquè la matriu generadora té paraules de pes 2). Si haguéssim tingut distància mínima ≥ 3, aleshores sí, però no és el cas de l'exemple que hem triat.

(e) La paraula $(??000)$ no es pot corregir de manera única, perquè tant (11000) com (00000) són paraules del codi.

10. (a) Doneu justificadament una matriu de control d'un codi binari de dimensió 4 capaç de corregir un error en una paraula codificada.
(b) Doneu-ne una matriu generadora.
(c) Poseu un exemple de paraula no nul·la del codi i poseu-li un error.
(d) Expliqueu el procés per corregir l'error de l'apartat anterior.
(e) Amb el codi que heu construït, es podrien corregir sempre dos esborralls?
(f) Si en l'apartat anterior heu respost que sí, poseu un exemple de paraula del codi amb dos eborralls i expliqueu el procés per corregir-los. Si en l'apartat anterior heu respost que no, poseu un exemple de paraula amb dos esborralls que no es puguin corregir.
(g) Amb el codi que heu construït, es podrien corregir sempre dos errors?
(h) Si en l'apartat anterior heu respost que sí, poseu un exemple de paraula del codi amb dos errors i expliqueu el procés per corregir-los. Si en l'apartat anterior heu respost que no, poseu un exemple de paraula amb dos errors que no es puguin corregir.

Solució:

(a) Perquè es tracti d'un codi binari cal que la matriu sigui de zeros i uns. Perquè una matriu sigui una matriu de control, cal que totes les seves files siguin linealment independents. Per tenir dimensió 4 cal que el nombre de files de la matriu de control sigui $n-4$, on n és el nombre de columnes. I, finalment, perquè puguem corregir un error, cal que la distància mínima sigui ≥ 3. Per això n'hi ha prou que no hi hagi cap parell de columnes linealment dependents, que en el cas binari es redueix al fet que no hi hagi dues columnes iguals.

Com a exemple haguéssim pogut donar la matriu

$$\begin{pmatrix} 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{pmatrix}.$$

(b) Com que és una matriu sistemàtica, una matriu generadora seria

$$\begin{pmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 \end{pmatrix}.$$

(c) Com a paraula codi, aleshores podem agafar qualsevol fila de la matriu generadora. Per exemple, la primera: 1101000. Li podem afegir un error a la primera posició i obtenim 0101000.

(d) Com que el codi té distància mínima 3, només podem corregir un error, i això ho podem fer per la síndrome:

$$\begin{pmatrix} 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{pmatrix} \begin{pmatrix} 0 \\ 1 \\ 0 \\ 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}.$$

Com que la síndrome és un múltiple de la primera columna de la matriu de control, deduïm que l'únic error s'ha produït a la primera posició. Com que el codi és binari l'error per força és 1. Deduïm que la paraula enviada és $0101000 + 1000000 = 1101000$.

(e) Sí, perquè la distància mínima és 3.

(f) Com a exemple agafem la mateixa paraula d'abans on hem posat esborralls en les dues darreres posicions: 11010??. A l'hora de corregir-la, substituïm els esborralls per "x" i "y" i imposem que en multiplicar per la matriu de control el resultat sigui zero:

$$\begin{pmatrix} 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{pmatrix} \begin{pmatrix} 1 \\ 1 \\ 0 \\ 1 \\ 0 \\ x \\ y \end{pmatrix} = \begin{pmatrix} x+y \\ y \\ x+y \end{pmatrix}.$$

Deduïm que $x = y = 0$, per tant, la paraula enviada era $11010xy = 1101000$.

(g) No, perquè la distància mínima és 3 perquè hi ha tres columnes linealment dependents (o també perquè la matriu generadora té paraules de pes 3). Si haguéssim tingut distància mínima ≥ 5, aleshores sí, però no és el cas de l'exemple que hem triat.

(h) Suposem que s'envia 1101000 (la mateixa paraula que abans) i es produeixen dos errors en la primera i segona posició, respectivament. Aleshores es rep la paraula 0001000, que és més a prop de 0000000 que no pas de la paraula original.

11. Considerem el conjunt de paraules $\{0000, 0101, 1010, 1111\} \subseteq \mathbb{Z}_2$.

(a) Demostreu que és un codi lineal.

(b) Quina dimensió té?

(c) Doneu-ne una matriu generadora.

(d) Demostreu que és un codi cíclic.

(e) Doneu-ne el polinomi generador.

Solució:

(a) És un subespai vectorial perquè totes les combinacions lineals de dues de les quatre paraules pertanyen al codi:

$$\begin{array}{ccccc} 0000 & + & 0000 & = & 0000 \\ 0000 & + & 0101 & = & 0101 \\ 0000 & + & 1010 & = & 1010 \\ 0101 & + & 0101 & = & 0000 \\ 0101 & + & 1010 & = & 1111 \\ 0101 & + & 1111 & = & 1010 \\ 1010 & + & 1010 & = & 0000 \\ 1010 & + & 1111 & = & 0101 \\ 1111 & + & 1111 & = & 0000 \end{array}$$

Per tant, és un codi lineal.

(b) La dimensió és 2 perquè és el màxim nombre de paraules linealment independents.

(c) Haguéssim pogut agafar qualsevol de les tres matrius següents:

$$\begin{pmatrix} 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 \end{pmatrix},$$

o qualsevol de les anteriors intercanviant les dues files.

(d) És un codi cíclic perquè qualsevol desplaçament circular de qualsevol de les paraules dona una altra paraula del codi. En efecte,

- tots els desplaçaments circulars de 0000 donen la mateixa paraula 0000,
- tots els desplaçaments circulars de 0101 donen o bé la mateixa paraula 0101 o bé la paraula 1010,

- tots els desplaçaments circulars de 1010 donen o bé la mateixa paraula 1010 o bé la paraula 0101,
- tots els desplaçaments circulars de 1111 donen la mateixa paraula 1111.

(e) Els polinomis que representen les 4 paraules del codi són 0, $x+x^3$, $1+x^2$, $1+x+x^2+x^3$, dels quals el de grau mínim sense comptar el 0 és x^2+1. Per tant, aquest és el polinomi generador del codi.

12. (a) Doneu l'únic polinomi f de $\mathbb{Z}_2[x]$ tal que $\mathbb{Z}_2[x]/f$ és el cos de 4 elements. Justifiqueu per què, amb el polinomi que heu escollit, $\mathbb{Z}_2[x]/f$ és un cos.

(b) Anomenem α a la classe de x dins el cos generat en l'apartat anterior. Considerem el conjunt de vectors

$$C=\{(0,0,0),(1,\alpha,\alpha^2),(\alpha,\alpha^2,1),(\alpha^2,1,\alpha)\}.$$

Demostreu que es tracta d'un codi lineal.

(c) Quina és la longitud del codi?

(d) Doneu-ne una matriu generadora.

(e) Quina és la dimensió del codi?

(f) Doneu-ne una matriu de control.

(g) Quina és la distància mínima del codi? I la capacitat correctora?

(h) Es tracta d'un codi cíclic?

(i) En cas afirmatiu, quin és el polinomi generador? En cas negatiu, quins vectors li hem d'afegir perquè sigui un codi cíclic?

Solució:

(a) $f(x)=x^2+x+1$. Obtenim un cos perquè és irreductible (té grau 2 i no té arrels) i el cos és de $2^2=4$ elements. La seva taula d'equivalències és

exp.	*vect.*
0	00
1	10
α	01
α^2	11

(b) Anomenem $v_1=(0,0,0), v_2=(1,\alpha,\alpha^2), v_3=(\alpha,\alpha^2,1), v_4=(\alpha^2,1,\alpha)$. És un codi lineal perquè totes les sumes de dos vectors cauen dins de C:

$$\begin{array}{cccc} v_1+v_1=v_1 & v_1+v_2=v_2 & v_1+v_3=v_3 & v_1+v_4=v_4 \\ & v_2+v_2=v_1 & v_2+v_3=v_4 & v_2+v_4=v_3 \\ & & v_3+v_3=v_1 & v_3+v_4=v_2 \\ & & & v_4+v_4=v_1 \end{array}$$

i perquè qualsevol vector multiplicat per un escalar també cau dins de C:

$$\begin{array}{cccc} 0v_1=v_1 & 1v_1=v_1 & \alpha v_1=v_1 & \alpha^2 v_1=v_1 \\ 0v_2=v_1 & 1v_2=v_2 & \alpha v_2=v_3 & \alpha^2 v_2=v_4 \\ 0v_3=v_1 & 1v_3=v_3 & \alpha v_3=v_4 & \alpha^2 v_3=v_2 \\ 0v_4=v_1 & 1v_4=v_4 & \alpha v_4=v_2 & \alpha^2 v_4=v_3 \end{array}.$$

(c) La longitud del codi és 3 perquè és el nombre de components dels seus vetors.

(d) A l'apartat (b) hem vist que els múltiples de v_2 són tot C (podem dir el mateix dels múltiples de v_3, i dels de v_5). Això ens diu que v_2 genera tot C (o també v_3 o v_4) i, per tant, $\{v_2\}$ és una base de C com a subespai vectorial. Per tant, la matriu que té una única fila corresponent a v_2 és una matriu generadora de C. Així doncs, podem agafar $G=\begin{pmatrix} 1 & \alpha & \alpha^2 \end{pmatrix}$.

(e) La dimensió és 1 perquè hem vist que hi ha un sol vector que genera tot el codi. També podem dir que és 1 perquè és el nombre de files de G.

(f) La matriu $G = \begin{pmatrix} 1 & \alpha & \alpha^2 \end{pmatrix}$ té una identitat a l'esquerra, de dimensions 1×1. En efecte, $G = \begin{pmatrix} I \mid P \end{pmatrix}$ amb $I = \begin{pmatrix} 1 \end{pmatrix}$ i $P = \begin{pmatrix} \alpha & \alpha^2 \end{pmatrix}$. Per tant, podem agafar com a matriu de control la matriu

$$H = \begin{pmatrix} -P^T \mid I \end{pmatrix} = \begin{pmatrix} \alpha & 1 & 0 \\ \alpha^2 & 0 & 1 \end{pmatrix}$$

(g) La distància mínima és $d = 3$ perquè és el mínim dels pesos de C. Capacitat correctora $= \lfloor \frac{d-1}{2} \rfloor = 1$.

(h) Sí que es tracta d'un codi cíclic, ja que tots els desplaçaments circulars de v_1 són ell mateix i tots els desplaçaments circulars de v_2, v_3, v_4 són algun de v_2, v_3, v_4.

(i) És $\alpha + \alpha^2 x + x^2$, ja que és l'únic polinomi mònic de grau mínim d'entre els que representen paraules no nul·les del codi.

13. Considerem el codi *binari* $C_2 \subseteq \mathbb{F}_2^6$ generat per la matriu

$$G = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 \end{pmatrix}$$

(a) Quantes paraules té? Enumereu-les totes.

Solució:

Té 4 paraules, que són $c_1 = (000000)$, $c_2 = (111111)$, $c_3 = (101010)$, $c_4 = (010101)$.

(b) Quina longitud té?

Solució:

Té longitud 6.

(c) Quina dimensió té? Justifiqueu la resposta.

Solució:

Té dimensió 2 perquè està generat per dues paraules linealment independents.

(d) Demostreu que es tracta d'un codi cíclic.

Solució:

Es tracta d'un codi lineal per ser definit com l'espai vectorial generat per les files de G i és cíclic, ja que tots els desplaçaments circulars de les paraules de C_2 són paraules de C_2. En efecte, els desplaçaments circulars de c_1 i de c_2 els deixen invariants, mentre que els desplaçaments circulars de c_3 i c_4 són o bé c_3 o bé c_4.

(e) Quin és el seu polinomi generador? Justifiqueu la resposta.

Solució:

Dels polinomis que representen les paraules de C_2, el que és mònic i té grau mínim i, per tant, és el polinomi generador, és $g(x) = x^4 + x^2 + 1$.

(f) Quin és el seu polinomi de control?

Solució:

El polinomi de control és $h(x) = \frac{x^6-1}{x^4+x^2+1} = \frac{x^6+1}{x^4+x^2+1} = x^2 + 1$.

(g) Doneu una matriu de control de C_2.

Solució:

$$H = \begin{pmatrix} 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 \end{pmatrix}$$

(h) Quina és la distància mínima de C_2? Justifiqueu la resposta.

Solució:

No hi ha cap columna de H nul·la. Per tant, $d \geq 2$. No hi ha dues columnes de H proporcionals. Per tant, $d \geq 3$. Hi ha tres columnes de H linealment dependents. Per exemple, la primera, la tercera i la cinquena. Per tant, $d = 3$.

(i) Quants errors es poden corregir en una paraula de C_2? Justifiqueu la resposta.

Solució:

Com que la distància mínima és $d = 3$, es pot corregir $\lfloor \frac{d-1}{2} \rfloor = \lfloor \frac{3-1}{2} \rfloor = 1$ error.

(j) Quina és la síndrome de la paraula (100110)?

Solució:

$$H \cdot \begin{pmatrix} 1 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 1 \\ 1 \\ 1 \end{pmatrix}$$

(k) Si té errors expliqueu els passos per corregir-los i doneu la paraula corregida. Si no té errors demostreu que no en té.

Solució:

La manera d'obtenir la síndrome com a combinació lineal de columnes de H emprant el mínim nombre possible de columnes és com la suma de les columnes 3a i 4a. Com que no hi ha cap altra combinació de dues columnes que doni la síndrome, podem deduir que només s'han produït dos errors ens les posicions 3a i 4a i que laparaula enviada era (101010).

(l) Poseu un exemple de paraula amb dos errors que no es corregeixi de manera correcta.

Solució:

Com que les columnes primera i cinquena sumen la columna tercera, si es produeix un error a la posició primera i un altre a la cinquena, la síndrome serà la mateixa que si només s'hagués produït un sol error a la tercera posició i, per tant, per màxima versemblança, corregirem pensant que només s'ha produït un error a la tercera posició. Per exemple, si a la paraula (000000) li afegim dos errors a les posicions primera i cinquena obtenim la paraula (100010). La síndrome d'aquesta paraula serà (1010) que és igual a la tercera columna. Per tant, deduïm que la paraula enviada era $(100010) - (001000) = (101010)$.

14. Considerem el codi *ternari* $C_3 \subseteq \mathbb{F}_3^6$ generat per la matriu

$$G = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 \end{pmatrix}$$

(a) Quantes paraules té? Enumereu-les totes.

Solució:

Té 9 paraules, que són $c_1 = (000000), c_2 = (111111), c_3 = (101010), c_4 = (010101), c_5 = (222222), c_6 = (202020), c_7 = (020202), c_8 = (212121), c_9 = (121212)$.

(b) Quina longitud té?

Solució:

Té longitud 6.

(c) Quina dimensió té? Justifiqueu la resposta.

Solució:

Té dimensió 2 perquè està generat per dues paraules linealment independents.

(d) Es tracta d'un codi cíclic? Justifiqueu la resposta.

Solució:

Es tracta d'un codi lineal per ser definit com l'espai vectorial generat per les files de G i és cíclic, ja que tots els desplaçaments circulars de les paraules de C_2 són paraules de C_2. En efecte, els desplaçaments circulars de c_1, de c_2 i de c_5 els deixen invariants, els desplaçaments circulars de c_3 i c_4 són o bé c_3 o bé c_4, els desplaçaments circulars de c_6 i c_7 són o bé c_6 o bé c_7 i els desplaçaments circulars de c_8 i c_9 són o bé c_8 o bé c_9.

(e) Si es tracta d'un codi cíclic, doneu el seu polinomi generador i justifiqueu la resposta. Si no és cíclic, doneu una paraula que no tingui els desplaçaments circulars dins el codi.

Solució:

Dels polinomis que representen les paraules de C_3, el que és mònic i té grau mínim i, per tant, és el polinomi generador, és $g(x) = x^4 + x^2 + 1$.

(f) Si es tracta d'un codi cíclic, doneu el seu polinomi de control i justifiqueu la resposta. Si no és cíclic, doneu una altra paraula que no tingui els desplaçaments circulars dins el codi.

Solució:

El polinomi de control és $h(x) = \frac{x^6-1}{x^4+x^2+1} = \frac{x^6+2}{x^4+x^2+1} = x^2 + 2$.

(g) Doneu una matriu de control de C_3.

Solució:

$$H = \begin{pmatrix} 2 & 0 & 1 & 0 & 0 & 0 \\ 0 & 2 & 0 & 1 & 0 & 0 \\ 0 & 0 & 2 & 0 & 1 & 0 \\ 0 & 0 & 0 & 2 & 0 & 1 \end{pmatrix}$$

(h) Quina és la distància mínima de C_3? Justifiqueu la resposta.

Solució:

No hi ha cap columna de H nul·la. Per tant, $d \geq 2$. No hi ha dues columnes de H proporcionals. Per tant, $d \geq 3$. Hi ha tres columnes de H linealment dependents. Per exemple, la primera, la tercera i la cinquena. Per tant, $d = 3$.

(i) Quants errors es poden corregir en una paraula de C_3? Justifiqueu la resposta.

Solució:

Com que la distància mínima és $d = 3$, es pot corregir $\lfloor \frac{d-1}{2} \rfloor = \lfloor \frac{3-1}{2} \rfloor = 1$ error.

(j) Quina és la síndrome de la paraula (212021)?

Solució:

$$H \cdot \begin{pmatrix} 2 \\ 1 \\ 2 \\ 0 \\ 2 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 2 \\ 0 \\ 1 \end{pmatrix}$$

(k) Si té errors, expliqueu els passos per corregir-los i doneu la paraula corregida. Si no té errors demostreu que no en té.

Solució:

Observem que la síndrome és dues vegades la quarta columna de H. Deduïm que hi ha hagut un error amb valor 2 a la posició quarta i la paraula enviada era $(212021) - (000200) = (212121)$.

(l) Doneu una paraula no nu·la del codi amb dos esborralls i corregiu-los explicant tots els passos.

Solució:

Podem agafar, per exemple, la paraula c_7 i li afegim dos esborralls a les darreres posicions i obtenim $(0202??)$. Per corregir els esborralls els convertim en incògnites x i y, és a dir, considerem

$(0202xy)$. Multipliquem aquesta paraula amb incògnites per la matriu de control i imposem que el resultat sigui el vector nul. Això ens dona el sistema d'equacions següent:

$$\begin{aligned} 0 &= 0 \\ 0 &= 0 \\ x &= 0 \\ 1+y &= 0 \end{aligned}$$

D'on deduïm que $x = 0$, $y = 2$ i, per tant, la paraula enviada era (020202).

15. Considerem el conjunt de vectors amb coeficients a $\mathbb{Z}_5$ següent:

$$C = \{(0,0,0,0),(1,2,4,3),(2,4,3,1),(3,1,2,4),(4,3,1,2)\}.$$

(a) Doneu la taula de la suma i del producte de $\mathbb{Z}_5$.

(b) Quantes possibles sumes hi ha entre dos vectors de C? Calculeu-les totes.

(c) Quants possibles productes d'un escalar de $\mathbb{Z}_5$ per un vector de C hi ha? Calculeu-los tots.

(d) És C un codi lineal?

(e) Quina és la longitud del codi?

(f) Doneu-ne una matriu generadora.

(g) Quina és la dimensió del codi?

(h) Doneu-ne una matriu de control.

(i) Quin sistema lineal d'equacions ens dona com a solució totes les paraules del codi?

(j) Agafeu una paraula no nul·la qualsevol de C i comproveu que és solució del sistema anterior.

(k) Quina és la distància mínima del codi? I la capacitat correctora?

(l) Considerem el vector $(3,1,2,4)$.
   (i) Doneu-ne la síndrome.
   (ii) Es pot corregir de manera unívoca?
      - En cas afirmatiu, expliqueu els passos seguits per corregir mitjançant la síndrome, així com el corresponent vector corregit.
      - En cas negatiu, doneu la llista de les paraules de C que es troben a distància de Hamming mínima.

(m) Considerem el vector $(2,4,4,3)$.
   (i) Doneu-ne la síndrome.
   (ii) Es pot corregir de manera unívoca?
      - En cas afirmatiu, expliqueu els passos seguits per corregir mitjançant la síndrome, així com el corresponent vector corregit.
      - En cas negatiu, doneu la llista de les paraules de C que es troben a distància de Hamming mínima.

(n) Considerem el vector $(2,3,1,2)$.
   (i) Doneu-ne la síndrome.
   (ii) Es pot corregir de manera unívoca?
      - En cas afirmatiu, expliqueu els passos seguits per corregir mitjançant la síndrome, així com el corresponent vector corregit.
      - En cas negatiu, doneu la llista de les paraules de C que es troben a distància de Hamming mínima.

(o) És C un codi cíclic?

(p) En cas afirmatiu, quin és el polinomi generador mònic? En cas negatiu, quins vectors li hem d'afegir perquè sigui un codi cíclic?

(q) En cas afirmatiu, quins són el polinomi de control i el polinomi generador mònic del codi dual? En cas negatiu, quins són tots els vectors del dual?

Solució:

(a)

+	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

×	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

(b) Diem $v_1 = (0,0,0,0)$, $v_2 = (1,2,4,3)$, $v_3 = (2,4,3,1)$, $v_4 = (3,1,2,4)$, $v_5 = (4,3,1,2)$. Hi ha 15 possibles sumes entre els vectors de C. Són les següents:

$$\begin{array}{ccccc}
v_1+v_1=v_1 & v_1+v_2=v_2 & v_1+v_3=v_3 & v_1+v_4=v_4 & v_1+v_5=v_5 \\
 & v_2+v_2=v_3 & v_2+v_3=v_4 & v_2+v_4=v_5 & v_2+v_5=v_1 \\
 & & v_3+v_3=v_5 & v_3+v_4=v_1 & v_3+v_5=v_2 \\
 & & & v_4+v_4=v_2 & v_4+v_5=v_3 \\
 & & & & v_5+v_5=v_4
\end{array}$$

(c) Hi ha 25 possibles productes d'un escalar de $\mathbb{Z}_5$ per un vector de C. Són els següents:

$$\begin{array}{ccccc}
0v_1=v_1 & 1v_1=v_1 & 2v_1=v_1 & 3v_1=v_1 & 4v_1=v_1 \\
0v_2=v_1 & 1v_2=v_2 & 2v_2=v_3 & 3v_2=v_4 & 4v_2=v_5 \\
0v_3=v_1 & 1v_3=v_3 & 2v_3=v_5 & 3v_3=v_2 & 4v_3=v_4 \\
0v_4=v_1 & 1v_4=v_4 & 2v_4=v_2 & 3v_4=v_5 & 4v_4=v_3 \\
0v_5=v_1 & 1v_5=v_5 & 2v_5=v_4 & 3v_5=v_3 & 4v_5=v_2
\end{array}$$

(d) És un codi lineal perquè totes les sumes de dos vectors pertany a C i perquè qualsevol vector multiplicat per un escalar també pertany a C.

(e) La longitud del codi és 4 perquè és el nombre de components dels seus vetors.

(f) A l'apartat 3 hem vist que els múltiples de v_2 són tot C (podem dir el mateix dels múltiples de v_3, dels de v_4 i dels de v_5). Això ens diu que v_2 genera tot C (o també v_3, v_4 o v_5) i, per tant, $\{v_2\}$ és una base de C com a subespai vectorial. Per tant, la matriu que té una única fila corresponent a v_2 és una matriu generadora de C. Així doncs, podem agafar $G = \begin{pmatrix} 1 & 2 & 4 & 3 \end{pmatrix}$.

(g) La dimensió és 1 perquè hem vist que hi ha un sol vector que genera tot el codi. També podem dir que és 1 perquè és el nombre de files de G.

(h) La matriu $G = \begin{pmatrix} 1 & 2 & 4 & 3 \end{pmatrix}$ té una identitat a l'esquerra, de dimensions 1×1. En efecte, $G = \begin{pmatrix} I \mid P \end{pmatrix}$ amb $I = \begin{pmatrix} 1 \end{pmatrix}$ i $P = \begin{pmatrix} 2 & 4 & 3 \end{pmatrix}$. Per tant, podem agafar com a matriu de control la matriu

$$H = \begin{pmatrix} -P^T \mid I \end{pmatrix} = \begin{pmatrix} 3 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 2 & 0 & 0 & 1 \end{pmatrix}.$$

(i) Un vector $(x_0, x_1, x_2, x_3) \in \mathbb{Z}_5$ pertany al codi si i només si
$\left\{\begin{array}{rcl} 3x_0 + x_1 & = & 0 \\ x_0 + x_2 & = & 0 \\ 2x_0 + x_3 & = & 0 \end{array}\right.$ o, equivalentment, $\left\{\begin{array}{rcl} x_1 & = & 2x_0 \\ x_2 & = & 4x_0 \\ x_3 & = & 3x_0 \end{array}\right.$

(j) Si agafem v_2, tenim que $x_0 = 1$ i es verifiquen les tres equacions: $x_1 = 2 = 2x_0$, $x_2 = 4 = 4x_0$, $x_2 = 3 = 3x_0$.
Si agafem v_3, tenim que $x_0 = 2$ i es verifiquen les tres equacions: $x_1 = 4 = 2x_0$, $x_2 = 3 = 4x_0$, $x_2 = 1 = 3x_0$.
Si agafem v_4, tenim que $x_0 = 3$ i es verifiquen les tres equacions: $x_1 = 1 = 2x_0$, $x_2 = 2 = 4x_0$, $x_2 = 4 = 3x_0$.
Si agafem v_5, tenim que $x_0 = 4$ i es verifiquen les tres equacions: $x_1 = 3 = 2x_0$, $x_2 = 1 = 4x_0$, $x_2 = 2 = 3x_0$.

(k) $d = 4$ perquè és el mínim dels pesos de les paraules no nul·les de C. Capacitat correctora $=\lfloor \frac{d-1}{2} \rfloor = 1$.

(l) $\begin{pmatrix} 3 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 2 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 3 \\ 1 \\ 2 \\ 4 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}$.
Com que la síndrome és nul·la, és una paraula del codi i ja no cal corregir.

(m) $\begin{pmatrix} 3 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 2 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 2 \\ 4 \\ 4 \\ 3 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \\ 2 \end{pmatrix}$
No es pot corregir de manera unívoca, perquè, si anomenem h_1, h_2, h_3, h_4, respectivament, a les columnes de H, aleshores la síndrome es pot escriure amb el mínim nombre de columnes possible, o bé com $h_1 - 3h_2$, o bé com $h_3 + 2h_4$.
Veiem que la distància de Hamming de $(2, 4, 4, 3)$ a les paraules del codi és
- $d((2, 4, 4, 3), v_1) = 4$
- $d((2, 4, 4, 3), v_2) = 2$
- $d((2, 4, 4, 3), v_3) = 2$
- $d((2, 4, 4, 3), v_4) = 4$
- $d((2, 4, 4, 3), v_5) = 4$

La llista de les dues paraules a distància de Hamming mínima de $(2, 4, 4, 3)$ és, doncs, $\{v_2, v_3\}$.

(n) $\begin{pmatrix} 3 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 2 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 2 \\ 3 \\ 1 \\ 2 \end{pmatrix} = \begin{pmatrix} 4 \\ 3 \\ 1 \end{pmatrix}$
Veiem que la síndrome és $3h_1$. Això vol dir que hi ha un error a la primera posició amb valor 3. Si el restem de la paraula rebuda obtenim $(2, 3, 1, 2) - (3, 0, 0, 0) = (4, 3, 1, 2) = v_5 \in C$.

(o) Sí que es tracta d'un codi cíclic, ja que tots els desplaçaments circulars de v_1 són ell mateix i tots els desplaçaments circulars de v_2, v_3, v_4, v_5 són, respectivament, v_3, v_5, v_2, v_4.

(p) $x^3 + 3x^2 + 4x + 2$.

(q) El polinomi de control és $h = (x^5 - 1)/(x^3 + 3x^2 + 4x + 2) = x + 2$.
Polinomi mònic vol dir que el coeficient del terme de grau més gran és 1. El polinomi generador del codi dual és el recíproc del polinomi de control. Això vol dir el de control però invertint els coeficients de grau més petit a grau més gran. Així, el recíproc de $x + 2$ (coeficients $2, 1$) és $2x + 1$ (coeficients $1, 2$). Però $2x + 1$ no és mònic. Per passar-lo a mònic l'hem de "dividir" entre 2, és a dir, multiplicar per l'invers de 2, que és 3. Per tant, el polinomi generador mònic del dual és $3(2x + 1) = x + 3$.

16. A $\mathbb{Z}_7[x]$ considerem el polinomi $g(x) = x^4 + 3x^3 + x + 3$ i el codi primitiu C_2 generat per g.
   (a) Expliqueu per què g genera un codi cíclic.
   (b) Doneu el polinomi de control de C_2.
   (c) Doneu una matriu generadora de C_2.
   (d) Doneu una matriu generadora de C_2 sistemàtica per l'esquerra.
   (e) Doneu una matriu generadora de C_2 sistemàtica per la dreta.
   (f) Doneu el polinomi generador (mònic) del codi dual de C_2.
   (g) Doneu la matriu de control de C_2 que s'obté a partir del polinomi de control.
   (h) Volem enviar el bloc d'informació 21. Doneu el polinomi corresponent a la informació que es vol enviar.
   (i) Per enviar-lo utilitzarem la codificació sistemàtica dels codis cíclics.
      - Doneu el dividend de la divisió necessària per a la codificació sistemàtica.
      - Doneu el divisor de la divisió necessària per a la codificació sistemàtica.
      - Doneu el quocient de la divisió necessària per a la codificació sistemàtica.
      - Doneu el residu de la divisió necessària per a la codificació sistemàtica.
   (j) Doneu el polinomi corresponent a la codificació sistemàtica del bloc 21.
   (k) Doneu el vector corresponent a la codificació sistemàtica del bloc 21.

Solució:

(a) Com que ens diuen que es tracta d'un codi primitiu, sabem que la seva longitud serà $q - 1 = 7 - 1 = 6$. Si dividim $x^6 - 1$ entre g ens dona quocient $x^2 + 4x + 2$ i residu 0. Com que el residu és 0, g és divisor de $x^n - 1$ i, per tant, és el polinomi generador d'un codi cíclic de longitud 6 a $\mathbb{F}_7$.

(b) El polinomi de control és el quocient de la divisió anterior, que és $h(x) = x^2 + 4x + 2$.

(c) A partir dels coeficients de g construïm la matriu generadora:

$$\begin{pmatrix} 3 & 1 & 0 & 3 & 1 & 0 \\ 0 & 3 & 1 & 0 & 3 & 1 \end{pmatrix}$$

(d) Per trobar la matriu generadora sistemàtica per la dreta fem transformacions de files:

$$\begin{pmatrix} 3 & 1 & 0 & 3 & 1 & 0 \\ 0 & 3 & 1 & 0 & 3 & 1 \end{pmatrix} \underset{\substack{f1' = 5f1 \\ f2' = 5f2}}{\sim} \begin{pmatrix} 1 & 5 & 0 & 1 & 5 & 0 \\ 0 & 1 & 5 & 0 & 1 & 5 \end{pmatrix}$$

$$\underset{f1' = f1 + 2f2}{\sim} \begin{pmatrix} 1 & 0 & 3 & 1 & 0 & 3 \\ 0 & 1 & 5 & 0 & 1 & 5 \end{pmatrix}$$

(e) Com que el codi és cíclic, la matriu sistemàtica per l'esquerra la podem obtenir, simplement, per un desplaçament circular de les seves columnes:

$$\begin{pmatrix} 3 & 1 & 0 & 3 & 1 & 0 \\ 5 & 0 & 1 & 5 & 0 & 1 \end{pmatrix}$$

(f) El polinomi generador (mònic) del dual l'obtenim a partir del recíproc del polinomi de control i multiplicant-lo per una constant perquè ens quedi mònic. En efecte, $h^*(x) = 2x^2 + 4x + 1$. Per obtenir un generador mònic l'haurem de multiplicar per l'invers de 2, que és 4 (trobem fàcilment que $2 \cdot 4 = 1$ a $\mathbb{Z}_7$). Obtenim que el polinomi generador del dual serà $4h^*(x) = x^2 + 2x + 4$.

(g) La matriu de control que obtenim a partir del polinomi de control és

$$\begin{pmatrix} 1 & 4 & 2 & 0 & 0 & 0 \\ 0 & 1 & 4 & 2 & 0 & 0 \\ 0 & 0 & 1 & 4 & 2 & 0 \\ 0 & 0 & 0 & 1 & 4 & 2 \end{pmatrix}.$$

(h) Codifiquem la informació com $i(x) = x + 2$.

(i) Per fer la codificació sistemàtica hem de fer la divisió de polinomis de dividend $x^5 + 2x^4$ i divisor $g(x) = x^4 + 3x^3 + x + 3$. El quocient ens dona $x + 6$ i el residu $3x^3 + 6x^2 + 5x + 3$.

(j) Deduïm que el polinomi corresponent a la codificacio sistemàtica de la informació és $x^5 + 2x^4 + 4x^3 + x^2 + 2x + 4$, que correspon a la paraula codi (421421).

17. (a) Considerem el codi lineal $C \subseteq \mathbb{Z}_7^6$ generat pels vectors $(6, 4, 6, 1, 0, 0)$, $(0, 6, 4, 6, 1, 0)$ i $(0, 0, 6, 4, 6, 1)$ amb components de $\mathbb{Z}_7$. Quines són la seva longitud i la seva dimensió?

(b) Doneu-ne una matriu generadora.

(c) Comproveu que es tracta d'un codi cíclic.

(d) Doneu-ne una matriu de control.

(e) Doneu-ne una altra matriu de control per un procediment diferent.

(f) Quina és la distància mínima de C? Justifiqueu-ho.

(g) Doneu una paraula del codi de pes 4, una de pes 5 i una de pes 6.

(h) Agafeu la paraula de pes 5 i anomeneu-la c. Doneu totes les paraules que obtenim quan fem desplaçaments circulars de c.

(i) Agafeu un dels desplaçaments circulars de c i comproveu que pertany a C mitjançant una matriu de control.

(j) Agafeu un altre dels desplaçaments circulars de c, diferent de l'anterior, i comproveu que pertany a C mitjançant o bé el polinomi generador o bé el polinomi de control.

(k) Agafeu un altre dels desplaçaments circulars de c, diferent dels anteriors, i produïu-li dos esborralls.

(l) Expliqueu i feu tots els passos necessaris per corregir els esborralls.

(m) Agafeu un altre dels desplaçaments circulars de c, diferent dels anteriors i produïu-li un error.

(n) Expliqueu i feu tots els passos necessaris per corregir l'error.

Solució:

(a) $n = 6$, $k = 3$.

(b)

$$G = \begin{pmatrix} 6 & 4 & 6 & 1 & 0 & 0 \\ 0 & 6 & 4 & 6 & 1 & 0 \\ 0 & 0 & 6 & 4 & 6 & 1 \end{pmatrix}$$

(c) Si fos un codi cíclic, deduïm per la forma de la matriu que el seu polinomi generador hauria de ser $x^3 + 6x^2 + 4x + 6$. En efecte, el polinomi mònic de grau més petit que podem obtenir com a combinació lineal dels polinomis corresponents a les files de G és precisament aquest.

Comprovem si aquest polinomi divideix $x^n - 1 = x^6 + 6$.

$$\begin{array}{rrrrrrrl|l}
x^6 & & & & & & +6 & & x^3+6x^2+4x+6 \\
\hline
-(x^6 & +6x^5 & +4x^4 & +6x^3 & & & &) & x^3+x^2+4x+1 \\
\hline
 & x^5 & +3x^4 & +x^3 & & & +6 & & \\
 -(& x^5 & +6x^4 & +4x^3 & +6x^2 & & &) & \\
\hline
 & & 4x^4 & +4x^3 & +x^2 & & +6 & & \\
 & -(& 4x^4 & +3x^3 & +2x^2 & +3x & &) & \\
\hline
 & & & x^3 & +6x^2 & +4x & +6 & & \\
 & & -(& x^3 & +6x^2 & +4x & +6 &) & \\
\hline
 & & & & & & 0 & &
\end{array}$$

Com que el dividieix, deduïm que es tracta del polinomi generador d'un codi cíclic. La matriu generadora del codi cíclic generat per aquest polinomi és la de l'enunciat i per això deduïm que la matriu genera un codi cíclic.

(d) Com que es tracta d'un codi cíclic amb polinomi de control $\frac{x^6-1}{x^3+6x^2+4x+6} = x^3 + x^2 + 4x + 1$, deduïm que una matriu de control és

$$H_1 = \begin{pmatrix} 1 & 1 & 4 & 1 & 0 & 0 \\ 0 & 1 & 1 & 4 & 1 & 0 \\ 0 & 0 & 1 & 1 & 4 & 1 \end{pmatrix}$$

(e) Busquem una matriu G' sistemàtica, $G' \sim G$.

$$\begin{pmatrix} 6 & 4 & 6 & 1 & 0 & 0 \\ 0 & 6 & 4 & 6 & 1 & 0 \\ 0 & 0 & 6 & 4 & 6 & 1 \end{pmatrix} \sim_{f_2=f_2-6f_1=f_1+f_2} \begin{pmatrix} 6 & 4 & 6 & 1 & 0 & 0 \\ 6 & 3 & 3 & 0 & 1 & 0 \\ 0 & 0 & 6 & 4 & 6 & 1 \end{pmatrix}$$

$$\sim_{f_3=f_3-4f_1-6f_2=3f_1+f_2+f_3} \begin{pmatrix} 6 & 4 & 6 & 1 & 0 & 0 \\ 6 & 3 & 3 & 0 & 1 & 0 \\ 3 & 1 & 6 & 0 & 0 & 1 \end{pmatrix} = G'$$

Deduïm que una matriu de control sistemàtica serà

$$H_2 = \begin{pmatrix} 1 & 0 & 0 & 1 & 1 & 4 \\ 0 & 1 & 0 & 3 & 4 & 6 \\ 0 & 0 & 1 & 1 & 4 & 1 \end{pmatrix}$$

(f) La distància mínima és 4 perquè és el mínim nombre de columnes linealment dependents de H_1 o de H_2. Tots els grups de tres columnes o menys són linealment independents.

(g) La primera fila de G és 646100 i té pes 4. La suma de les tres files de G és 632401 i té pes 5. La suma de les tres files de G' és 111111 i té pes 6.

(h) $c = 632401$. Els seus desplaçaments circulars són:

- 324016
- 240163
- 401632
- 016324
- 163240
- 632401, que torna a ser c.

(i) Agafem el desplaçament circular 324016. Podem comprovar-ho amb H_1 o H_2. Ho farem amb H_2 :

$$\begin{pmatrix} 1 & 0 & 0 & 1 & 1 & 4 \\ 0 & 1 & 0 & 3 & 4 & 6 \\ 0 & 0 & 1 & 1 & 4 & 1 \end{pmatrix} \begin{pmatrix} 3 \\ 2 \\ 4 \\ 0 \\ 1 \\ 6 \end{pmatrix} = \begin{pmatrix} 28 \\ 42 \\ 14 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}.$$

(j) Agafem el desplaçament circular 240163. Mitjançant el polinomi generador:

$$\begin{array}{rl|l}
 & 3x^5 + 6x^4 + x^3 + 4x + 2 & x^3 + 6x^2 + 4x + 6 \\ \cline{3-3}
-(& 3x^5 + 4x^4 + 5x^3 + 4x^2) & 3x^2 + 2x + 5 \\ \cline{1-2}
 & 2x^4 + 3x^3 + 3x^2 + 4x + 2 & \\
-(& 2x^4 + 5x^3 + x^2 + 5x) & \\ \cline{1-2}
 & 5x^3 + 2x^2 + 6x + 2 & \\
-(& 5x^3 + 2x^2 + 6x + 2) & \\ \cline{1-2}
 & 0 &
\end{array}$$

O bé mitjançant el polinomi de control:

$$\begin{aligned}(3x^5+6x^4+x^3+4x+2)\cdot(x^3+x^2+4x+1) &= 3x^8+(3+6)x^7+(5+6+1)x^6+(3+3+1)x^5+(6+4+4)x^4+\\ &\quad +(1+4+2)x^3+(2+2)x^2+(4+1)x+2\\ &= 3x^8+2x^7+5x^6+4x^2+5x+2\\ &= (3x^2+2x+5)x^6-(3x^2+2x+5)\\ &= (x^6-1)(3x^2+2x+5)\\ &= 0 \mod (x^6-1)\end{aligned}$$

(k) Agafem el desplaçament circular 401632. Li posem dos esborralls, per exemple, en les dues darreres posicions: 4016??.

(l) Les convertim en incògnites x, y i resolem el sistema

$$\begin{pmatrix}1&0&0&1&1&4\\0&1&0&3&4&6\\0&0&1&1&4&1\end{pmatrix}\begin{pmatrix}4\\0\\1\\6\\x\\y\end{pmatrix}=\begin{pmatrix}x+4y+3\\4x+6y+4\\4x+y\end{pmatrix}=\begin{pmatrix}0\\0\\0\end{pmatrix}.$$

De la darrera equació deduïm que $y=3x$, substituint a la primera obtenim $6x+3=0$, d'on $x=3$ i, per tant, $y=3x=2$. Obtenim la paraula original, prèvia als esborralls: 401632.

(m) Agafem el desplaçament circular 016324. Li posem un error, per exemple, en la darrera posició: 016320.

(n) Multipliquem la paraula per la matriu de control per calcular la síndrome:

$$\begin{pmatrix}1&0&0&1&1&4\\0&1&0&3&4&6\\0&0&1&1&4&1\end{pmatrix}\begin{pmatrix}0\\1\\6\\3\\2\\0\end{pmatrix}=\begin{pmatrix}5\\4\\3\end{pmatrix}$$

Mirem si és múltiple d'alguna de les columnes de H_2 i resulta que $\begin{pmatrix}5\\4\\3\end{pmatrix}=3\begin{pmatrix}4\\6\\1\end{pmatrix}$, és a dir, és 3 vegades la darrera columna. Això vol dir que hi ha un error de valor 3 a la darrera posició que li hem de restar a la paraula rebuda. Per tant, la paraula corregida serà $016320-000003=016324$.

18. (a) Doneu l'únic polinomi f de $\mathbb{Z}_2[x]$ tal que $\mathbb{Z}_2[x]/f$ és el cos de 4 elements. Justifiqueu-ne l'elecció. Anomenem α a la classe de x dins el cos generat en l'apartat anterior. Considerem el codi $\mathcal{C}$ sobre $\mathbb{F}_4$ donat per les solucions a $\mathbb{F}_4^3$ del sistema $\begin{cases} x_1+x_2+x_3=0,\\ x_1+\alpha x_2+\alpha^2x_3=0.\end{cases}$

(b) Quina és la longitud del codi?

(c) Rebem la següent seqüència de símbols on hi ha hagut uns quants esborralls: $??\alpha?\alpha^2?1??$ Podeu corregir-los?

(d) Doneu-ne una matriu generadora.

(e) Quina és la dimensió del codi?

(f) Doneu-ne una matriu de control.

(g) Quina és la distància mínima del codi? I la capacitat correctora?

(h) Doneu una paraula del codi en símbols.

(i) Afegiu-li un error i calculeu-ne la síndrome.

(j) Expliqueu com es dedueix a partir de la síndrome
- on és l'error,
- quin és el valor de l'error.

(k) Es tracta d'un codi cíclic. Quin és el polinomi generador mònic (és a dir, amb coeficient de grau màxim igual a 1)?

(l) Volem enviar la següent seqüència de bits: 10110100. A quina seqüència de símbols correspon?

(m) Codifiqueu-la de manera sistemàtica mitjançant polinomis. Doneu el resultat en
- símbols,
- bits.

Solució:

(a) $f(x) = x^2 + x + 1$. Obtenim un cos perquè és irreductible (té grau 2 i no té arrels) i el cos és de $2^2 = 4$ elements. La seva taula d'equivalències és

exp.	*vect.*
0	00
1	10
α	01
α^2	11

(b) 3.

(c) Separem en tres blocs de 3 símbols cada un: $x_1 x_2 \alpha$, $y_1 \alpha^2 y_3$, $1 z_2 z_3$. En resulten els sistemes d'equacions

i. $\begin{cases} x_1 + x_2 + \alpha = 0, \\ x_1 + \alpha x_2 + 1 = 0. \end{cases}$

Deduïm que $x_2 + \alpha = \alpha x_2 + 1$, és a dir, $x_2 = 1$, i deduïm que $x_1 = \alpha^2$. Per tant, la primera paraula corregida és $\alpha^2 1 \alpha$.

ii. $\begin{cases} y_1 + \alpha^2 + y_3 = 0, \\ y_1 + 1 + \alpha^2 y_3 = 0. \end{cases}$

Deduïm que $\alpha^2 + y_3 = 1 + \alpha^2 y_3$, és a dir, $y_3 = 1$, i deduïm que $y_1 = \alpha$. Per tant, la segona paraula corregida és $\alpha\alpha^2 1$.

iii. $\begin{cases} 1 + z_2 + z_3 = 0, \\ 1 + \alpha z_2 + \alpha^2 z_3 = 0. \end{cases}$

El sistema és equivalent a $\begin{cases} \alpha + \alpha z_2 + \alpha z_3 = 0, \\ 1 + \alpha z_2 + \alpha^2 z_3 = 0. \end{cases}$

Deduïm que $\alpha + \alpha z_3 = 1 + \alpha^2 z_3$, és a dir, $z_3 = \alpha^2$, i deduïm que $z_2 = \alpha$. Per tant, la segona paraula corregida és $1\alpha\alpha^2$.

(d) Per les equacions deduïm que una matriu de control és

$$H = \begin{pmatrix} 1 & 1 & 1 \\ 1 & \alpha & \alpha^2 \end{pmatrix}.$$

En busquem una d'equivalent que sigui sistemàtica: $\begin{pmatrix} 1 & 1 & 1 \\ 1 & \alpha & \alpha^2 \end{pmatrix} \sim_{f_2 += f_1} \begin{pmatrix} 1 & 1 & 1 \\ 0 & \alpha^2 & \alpha \end{pmatrix} \sim_{f_2 *= \alpha}$ $\begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & \alpha^2 \end{pmatrix} \sim_{f_1 += f_2} \begin{pmatrix} 1 & 0 & \alpha \\ 0 & 1 & \alpha^2 \end{pmatrix}$.

D'aquí deduïm que una matriu generadora pot ser

$$G = \begin{pmatrix} \alpha & \alpha^2 & 1 \end{pmatrix}.$$

(e) 1.

(f) Com ja hem vist abans, podem agafar

$$H = \begin{pmatrix} 1 & 1 & 1 \\ 1 & \alpha & \alpha^2 \end{pmatrix}.$$

(g) $d = 3$ perquè és el mínim nombre de columnes linealment dependents de la matriu H. Capacitat correctora $= \lfloor \frac{d-1}{2} \rfloor = 1$.

(h) Agafem la paraula que trobem com a única fila de la matriu generadora: $\alpha\alpha^2 1$

(i) Alterem, per exemple, la segona posició afegint, per exemple, l'error α i obtenim $\alpha 11$

$$H = \begin{pmatrix} 1 & 1 & 1 \\ 1 & \alpha & \alpha^2 \end{pmatrix} \begin{pmatrix} \alpha \\ 1 \\ 1 \end{pmatrix} = \begin{pmatrix} \alpha \\ \alpha^2 \end{pmatrix}.$$

(j) Com que la síndrome és α vegades la segona columna de H, això vol dir que tenim un error a la segona posició i de valor α.

(k) A partir de la matriu generadora podem deduir que el polinomi generador mònic és $g = \alpha + \alpha^2 x + x^2$.

(l) 10110100 correspon a $1\alpha^2\alpha 0$.

(m) Separem en blocs de k en k, és a dir, d'un en un.

i. $i_1 = 1$, $i_1 x^{n-k} = x^2$ i el residu de dividir x^2 entre $x^2 + \alpha^2 x + \alpha$ és $\alpha^2 x + \alpha$. La primer paraula codificada serà, doncs, en símbols,

$$\alpha\alpha^2 1.$$

ii. $i_2 = \alpha^2$, $i_2 x^{n-k} = \alpha^2 x^2$ i el residu de dividir $\alpha^2 x^2$ entre $x^2 + \alpha^2 x + \alpha$ és $\alpha x + 1$. La segona paraula codificada serà, doncs, en símbols,

$$1\alpha\alpha^2.$$

iii. $i_3 = \alpha$, $i_3 x^{n-k} = \alpha x^2$ i el residu de dividir αx^2 entre $x^2 + \alpha^2 x + \alpha$ és $x + \alpha^2$. La tercera paraula codificada serà, doncs, en símbols,

$$\alpha^2 1\alpha.$$

iv. $i_4 = 0$, $i_4 x^{n-k} = 0$ i el residu de dividir 0 entre $x^2 + \alpha^2 x + \alpha$ és 0. La quarta paraula codificada serà, doncs, en símbols,

$$000.$$

Si ara passem les quatre paraules a bits, obtenim 011110 100111 111001 000000.

19. (a) Demostreu que $g = x^4 + 4x^3 + 6x + 3$ genera un codi cíclic primitiu sobre $\mathbb{F}_7 = \mathbb{Z}_7$.

(b) Quina longitud i quina dimensió té aquest codi?

(c) Doneu-ne una matriu generadora.

(d) Es pot deduir la distància mínima a partir de la matriu generadora?

(e) Corregiu la següent paraula amb esborralls: $(???235)$.

(f) Comproveu si la paraula obtinguda en l'apartat anterior pertany al codi mitjançant el polinomi de control.

(g) Codifiqueu de forma sistemàtica la informació (11) mitjançant el polinomi generador.

Solució:

(a) Cal demostrar que g divideix $x^6 - 1$. I, en efecte, $(x^6 - 1)/g = x^2 + 3x + 2$.

(b) $n = 6$, $k = 2$.

(c) $G = \begin{pmatrix} 3 & 6 & 0 & 4 & 1 & 0 \\ 0 & 3 & 6 & 0 & 4 & 1 \end{pmatrix}.$

(d) Les paraules del codi seran combinacions lineals de les dues files de G. Observem que totes dues files tenen pes 4 i que qualsevol combinació lineal d'ambdues tindrà com a mínim 4 components no nul·les.

(e) (542235).

(f) $(5+4x+2x^2+2x^3+3x^4+5x^5)(x^2+3x+2) = 5x^7+4x^6+2x+3$. Si ara dividim $5x^7+4x^6+2x+3$ entre x^6-1 ens dona quocient $5x+4$ i residu 0.

(g) El residu de dividir $i(x)x^{n-k} = x^4+x^5$ entre g és $R(x) = 5x^3+x^2+x+2$. Aleshores $x(x)x^{n-k}-R(x)$ correspon a la paraula codi 566211.

20. (a) Comproveu que el polinomi x^2+x+2 és irreductible i primitiu a $\mathbb{Z}_3[x]$.

(b) Doneu una taula exponencial-vectorial de $\mathbb{Z}_3[x]/x^2+x+2$ respecte $\alpha = [x]$.

(c) Considerem el codi C amb matriu generadora

$$G = \begin{pmatrix} 1 & \alpha^3 & \alpha & \alpha^6 \\ 0 & 1 & 0 & \alpha^2 \end{pmatrix}.$$

Codifiqueu la cadena de trits 01200210. Doneu el resultat també com a cadena de trits.

(d) Doneu una matriu de control del codi.

(e) Es tracta d'un codi cíclic?

(f) Quina és la distància mínima de C?

(g) Quants errors es poden corregir en cada paraula rebuda? I quants esborralls? Quants errors es poden detectar?

(h) Corregiu els esborralls de la cadena de trits 20??0211. Doneu el resultat en trits.

Solució:

(a) El polinomi és irreductible perquè té grau 2 i no té arrels ($f(0) = 2$, $f(1) = 1$ i $f(2) = 2$). Si fem totes les potències de $\alpha = [x]$ veiem que són diferents fins que arribem a $\alpha^8 = 1$. Per això el polinomi és primitiu.

(b)

exp.	*vect.*
0	00
1	10
α	01
α^2	12
α^3	22
α^4	20
α^5	02
α^6	21
α^7	11

(c) La cadena de trits representa la cadena de símbols $\alpha\alpha^4\alpha^5 1$. Multipliquem cada parell de símbols per la matriu generadora:

$$\alpha 1 \alpha^2 \alpha^5 \quad \alpha^5 2 \alpha^6 \alpha =$$

$$01101202 \quad 02202101.$$

(d) La matriu generadora sistemàtica serà:

$$\begin{pmatrix} 1 & 0 & \alpha & \alpha^3 \\ 0 & 1 & 0 & \alpha^2 \end{pmatrix}.$$

Per tant, com a matriu de control podem agafar

$$H = \begin{pmatrix} \alpha^5 & 0 & 1 & 0 \\ \alpha^7 & \alpha^6 & 0 & 1 \end{pmatrix}.$$

(e) Per la matriu generadora veiem que els polinomis que representen paraules del codi tenen grau, com a mínim, 2. Per la segona fila veiem que $\alpha^2 x^2 + 1$ és un d'aquests polinomis de grau mínim. Si el multipliquem per α^6 obtenim el polinomi mònic $x^2 + \alpha^6$. Perquè fos un codi cíclic caldria que $x^2+\alpha^6$ fos un divisor de x^4-1. Però, fent la divisió euclidiana, obtenim $x^4-1 = (x^2+\alpha^6)(x^2+\alpha^2)+1$. Per tant, $x^2 + \alpha^6$ no és un divisor de $x^4 - 1$ i el codi no és cíclic.

(f) Com que hi ha dues columnes linealment dependents i no hi ha cap columna nul·la, la distància mínima és 2.

(g) No es pot corregir cap error, es pot corregir un esborrall i es pot detectar un error.

(h) La cadena de trits representa el vector $\alpha^4 x \alpha^5 \alpha^7$. Perquè aquest vector sigui del codi, cal que en multiplicar-lo per H ens doni el vector nul.

$$H \cdot \begin{pmatrix} \alpha^4 \\ x \\ \alpha^5 \\ \alpha^7 \end{pmatrix} = \begin{pmatrix} \alpha + \alpha^5 \\ \alpha^{11} + \alpha^6 x + \alpha^7 \end{pmatrix} = \begin{pmatrix} 0 \\ \alpha^6 x \end{pmatrix}.$$

Deduïm que
$$x = 0.$$

La paraula codi corregida és $\alpha^4 0 \alpha^5 \alpha^7$, que correspon a la cadena de trits

$$20000211.$$

21. Considerem el polinomi de $\mathbb{Z}_2[x]$
$$g(x) = 1 + x^3 + x^6.$$

(a) Quin és el codi cíclic C de longitud mínima que pot generar g? Quina longitud té?

(b) Quina dimensió té C?

(c) Doneu una matriu generadora de C.

(d) Doneu una matriu de control de C.

(e) Quina és la distància mínima del codi? Per què?

(f) En una transmissió on s'ha codificat mitjançant C rebem la seqüència de bits següent: 101101110001101. Extraieu-ne la primera paraula rebuda.

(g) Quina síndrome té?

(h) Pot ser que no s'hagi produït cap error? Per què?

(i) Pot ser que s'hagi produït un sol error? Per què?

(j) Pot ser que s'hagin produït dos errors? Per què?

Solució:

(a) Veiem amb les divisions següents que $g(x)$ no és divisor de $x^6 - 1$, ni de $x^7 - 1$, ni de $x^8 - 1$. En canvi sí que ho és de $x^9 - 1$. Per això genera un codi cíclic de longitud $n = 9$ i no en genera cap de més petit.

$$\begin{array}{rrrl|l} x^6 & & +1 & & x^6 + x^3 + 1 \\ \cline{5-5} -(x^6 & +x^3 & +1) & & 1 \\ \cline{1-3} & x^3 & & & \end{array}$$

$$\begin{array}{rrrrl|l} x^7 & & & +1 & & x^6 + x^3 + 1 \\ \cline{6-6} -(x^7 & +x^4 & +x &) & & x \\ \cline{1-4} & x^4 & +x & +1 & & \end{array}$$

$$\begin{array}{rl}
\begin{array}{r}
x^8 \qquad\qquad +1 \\
-(x^8 + x^5 + x^2 \quad) \\
\hline
x^5 + x^2 + 1
\end{array}
&
\begin{array}{|l}
x^6 + x^3 + 1 \\
\hline
x^2
\end{array}
\end{array}$$

$$\begin{array}{rl}
\begin{array}{r}
x^9 \qquad\qquad\quad +1 \\
-(x^9 + x^6 + x^3 \quad) \\
\hline
x^6 + x^3 + 1 \\
-(x^6 + x^3 + 1) \\
\hline
0
\end{array}
&
\begin{array}{|l}
x^6 + x^3 + 1 \\
\hline
x^3 + 1
\end{array}
\end{array}$$

(b) Té dimensió $n - \text{grau}(g) = 9 - 6 = 3$.

(c)

$$\begin{pmatrix} 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 \end{pmatrix}$$

(d) Podríem calcular la matriu de control a partir del polinomi de control, però optem per fer-ho aprofitant el fet que la matriu generadora és sistemàtica amb una identitat a l'esquerra.

$$\begin{pmatrix} 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

(e) La distància mínima de C és 3 perquè dins la matriu de control no hi ha columnes nul·les ni dues columnes que siguin linealment dependents (en aquest cas iguals). En canvi sí que n'hi ha tres que són linealment dependents. Per exemple, la primera, la quarta i la setena.

(f) La primera paraula rebuda és 101101110 perquè la longitud del codi és 9.

(g) Aquesta paraula té síndrome

$$\begin{pmatrix} 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 \\ 0 \\ 1 \\ 1 \\ 0 \\ 1 \\ 1 \\ 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \end{pmatrix}$$

(h) No, perquè aleshores la síndrome hauria de ser nul·la.

(i) No, perquè aleshores la síndrome hauria de ser múltiple d'alguna columna de la matriu de control i no ho és.

(j) Sí, perquè la síndrome és la suma de les dues darreres columnes i es pot haver produït, per tant, error en les dues darreres components de la paraula. En aquest cas, la paraula codi corregida seria 101101101. Veiem que aquesta paraula pertany al codi perquè és la suma de la primera i la tercera files de la matriu generadora.

Si només s'han produït dos errors han de ser en les dues darreres posicions, perquè no hi ha cap altra combinació de dues columnes de la matriu de control que sumi la síndrome.

22. Escriviu totes les paraules del codi cíclic binari de longitud 3 generat per $1 + x + x^2$.

23. (a) Comproveu que el polinomi x^3+x+1 és irreductible i primitiu a $\mathbb{Z}_2[x]$.
    (b) Doneu una taula exponencial-vectorial de $\mathbb{Z}_2[x]/x^3+x+1$ respecte $\alpha=[x]$.
    (c) Digueu justificadament quin dels següents polinomis genera un codi binari cíclic de longitud 7.
    - x,
    - $x^7+\alpha x+1$,
    - $x^4+\alpha^3x^3+x^2+\alpha x+\alpha^3$.

    (d) Quina és la dimensió del codi generat? Per què?
    (e) Doneu el polinomi de control del codi.
    (f) Doneu una matriu generadora del codi.
    (g) Doneu una matriu de control del codi.
    (h) Rebem la següent cadena de bits 011111000111100100000. Justifiqueu si correspon a una paraula del codi per tres procediments diferents:
    - Mitjançant el polinomi generador.
    - Mitjançant el polinomi de control.
    - Mitjançant la matriu de control.

    (i) Codifiqueu de manera sistemàtica en les darreres posicions la informació $\alpha\alpha^2\alpha^3$.
    (j) Quina cadena de bits passaria pel canal?

Solució:

(a) És irreductible perquè té grau 3 i no té arrels (si substituïm la x per 0 i per 1 ens dona 1). És primitiu perquè totes les potències de $[x]=\alpha$ amb exponents de 0 a 6 són diferents. Es pot veure en la taula de l'apartat següent.

(b)

pot.	vec.
0	0
α^0	(100)
α	(010)
α^2	(001)
α^3	(110)
α^4	(011)
α^5	(111)
α^6	(101)

(c) Només el tercer perquè és l'únic que és divisor de x^7-1. En efecte, x^7-1 entre x ens donarà residu 1, mentre que x^7-1 entre $x^7+\alpha x+1$ ens donarà residu αx. En canvi, si dividim x^7-1 entre $x^4+\alpha^3x^3+x^2+\alpha x+\alpha^3$ ens dona quocient $x^3+\alpha^3x^2+\alpha^2x+\alpha^4$ i residu 0.

(d) Com que el grau del polinomi generador és $n-k=7-k=4$, la dimensió és 3.

(e) $h(x)=x^3+\alpha^3x^2+\alpha^2x+\alpha^4$.

(f) $G=\begin{pmatrix} \alpha^3 & \alpha & 1 & \alpha^3 & 1 & 0 & 0 \\ 0 & \alpha^3 & \alpha & 1 & \alpha^3 & 1 & 0 \\ 0 & 0 & \alpha^3 & \alpha & 1 & \alpha^3 & 1 \end{pmatrix}.$

(g) $H=\begin{pmatrix} 1 & \alpha^3 & \alpha^2 & \alpha^4 & 0 & 0 & 0 \\ 0 & 1 & \alpha^3 & \alpha^2 & \alpha^4 & 0 & 0 \\ 0 & 0 & 1 & \alpha^3 & \alpha^2 & \alpha^4 & 0 \\ 0 & 0 & 0 & 1 & \alpha^3 & \alpha^2 & \alpha^4 \end{pmatrix}.$

(h) La cadena de bits correspon a la cadena de símbols $\alpha^4\alpha^5 0\alpha^5 110$ i al polinomi $u(x)=x^5+x^4+\alpha^5x^3+\alpha^5x+\alpha^4$.
- Si dividim $u(x)$ entre $g(x)$ ens dona quocient $x+\alpha$ i residu 0.
- Si multipliquem $u(x)$ per $h(x)$ ens dona $x^8+\alpha x^7+x+\alpha$ que és 0 mòdul x^7-1.

- $$H \cdot \begin{pmatrix} \alpha^4 \\ \alpha^5 \\ 0 \\ \alpha^5 \\ 1 \\ 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 & \alpha^3 & \alpha^2 & \alpha^4 & 0 & 0 & 0 \\ 0 & 1 & \alpha^3 & \alpha^2 & \alpha^4 & 0 & 0 \\ 0 & 0 & 1 & \alpha^3 & \alpha^2 & \alpha^4 & 0 \\ 0 & 0 & 0 & 1 & \alpha^3 & \alpha^2 & \alpha^4 \end{pmatrix} \cdot \begin{pmatrix} \alpha^4 \\ \alpha^5 \\ 0 \\ \alpha^5 \\ 1 \\ 1 \\ 0 \end{pmatrix} = \begin{pmatrix} \alpha^4+\alpha+\alpha^2 \\ \alpha^5+\alpha^4+1 \\ \alpha+\alpha^2+\alpha^4 \\ \alpha^5+\alpha^3+\alpha^2 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}$$

(i) $(\alpha x^4+\alpha^2x^5+\alpha^3x^6)-R((\alpha x^4+\alpha^2x^5+\alpha^3x^6, g(x)) = \alpha^3x^6+\alpha^2x^5+\alpha x^4+x^3+\alpha^6x^2+\alpha^5x+\alpha^4$, que correspon a la cadena de símbols $\alpha^4\alpha^5\alpha^6 1\alpha\alpha^2\alpha^3$.

(j) 010111101100010001110.

24. (a) Comproveu que $1, 2, 3, 4 \in \mathbb{Z}_5$ són quatre arrels del polinomi x^4-1 i utilitzeu aquestes arrels per expressar x^4-1 com a producte de polinomis de grau 1.

(b) Agafeu un polinomi de $\mathbb{Z}_5[x]$ divisor de x^4-1 i de grau 2 i anomeneu-lo $g(x)$ (l'apartat anterior us pot ajudar).

(c) Quina dimensió té el codi C de longitud 4 generat per $g(x)$?

(d) Doneu el polinomi de control del codi.

(e) Doneu una matriu de control del codi.

(f) Codifiqueu de manera sistemàtica en les darreres posicions la informació 24.

(g) Comproveu que la paraula obtinguda en l'apartat anterior pertany al codi per tres procediments diferents:
- Mitjançant el polinomi generador,
- Mitjançant el polinomi de control,
- Mitjançant la matriu de control.

Solució:

(a) $1, 2, 3, 4$ són arrels de x^4-1 perquè $1^4 = 1, 2^4 = 1, 3^4 = 1$ i $4^4 = 1$ a $\mathbb{Z}_5$. Sabem que a és arrel d'un polinomi $p(x)$ si i només si $x-a$ divideix $p(x)$. Això vol dir, en el nostre cas, que $(x-1)(x-2)(x-3)(x-4)$ divideix x^4-1. Mirant els graus deduïm que $x^4-1 = (x-1)(x-2)(x-3)(x-4)$.

(b) Podríem agafar qualsevol dels següents:
- $(x-1)(x-2) = x^2+2x+2$
- $(x-1)(x-3) = x^2+x+3$
- $(x-1)(x-4) = x^2+4$
- $(x-2)(x-3) = x^2+1$
- $(x-2)(x-4) = x^2+4x+3$
- $(x-3)(x-4) = x^2+3x+2$

Com a exemple de resolució agafem $g(x) = x^2+2x+2$.

(c) $\text{Grau}(g) = 2 = n-k = 4-k$. Per tant, $k = 2$.

(d) $h(x) = \frac{x^4-1}{g(x)} = \frac{(x-1)(x-2)(x-3)(x-4)}{(x-1)(x-2)} = (x-3)(x-4) = x^2+3x+2$.

(e) Com a matriu de control podem agafar la matriu generadora del codi generat pel polinomi recíproc de $h(x)$:

$$H = \begin{pmatrix} 1 & 3 & 2 & 0 \\ 0 & 1 & 3 & 2 \end{pmatrix}.$$

(f) El polinomi d'informació que representa el vector d'informació $i = (24)$ és $i(x) = 2+4x$. La seva codificació sistemàtica en les darreres posicions serà $c(x) = i(x)x^{n-k} - (i(x)x^{n-k} \mod g(x)) = 2x^2+4x^4-(4x+2) = 4x^3+2x^2+x+3$, que correspon al vector $c = (3124)$.

(g)
- Fem la divisió de $4x^3+2x^2+x+3$ entre $g(x)$ i ens dona residu 0 (i quocient $4x+4$).
- Multipliquem $4x^3+2x^2+x+3$ per $h(x)$ i ens dona $4x^5+4x^4+x+1$, que dividit entre x^4-1 ens dona residu 0 (i quocient $4x+4$).

- $$\begin{pmatrix} 1 & 3 & 2 & 0 \\ 0 & 1 & 3 & 2 \end{pmatrix} \begin{pmatrix} 3 \\ 1 \\ 2 \\ 4 \end{pmatrix} = \begin{pmatrix} 3+3+4 \\ 1+6+8 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix}.$$

25. Sigui C el conjunt de paraules binàries de longitud 4 i pes parell.
    (a) Demostreu que C és un codi lineal.
    (b) Quina és la distància mínima de C?
    (c) Quants errors pot corregir C?
    (d) I quants esborralls?
    (e) Si es rep la paraula 10?1 podríeu dir justificadament quin símbol correspon a l'esborrall?
    (f) Demostreu que C és un codi cíclic.
    (g) Doneu-ne el polinomi generador.

    Solució:

    (a) Totes les paraules de C són $\{v_0 = 0000, v_1 = 1100, v_2 = 1010, v_3 = 1001, v_4 = 0110, v_5 = 0101, v_6 = 0011, v_7 = 1111\}$. Si en sumem dues qualssevol, sempre n'obtenim una altra del conjunt.
    (b) El mínim dels pesos de les paraules no nul·les és 2. Per tant, la distància mínima és 2.
    (c) No pot corregir cap error.
    (d) Pot corregir un esborrall.
    (e) Ha de ser 0 perquè, si no, la paraula tindria pes senar.
    (f) Els desplaçaments circulars de v_0 són ell mateix, els desplaçaments circulars de v_1, v_4, v_6, v_3 són algun altre vector de v_1, v_4, v_6, v_3. Els desplaçaments circulars de v_2, v_5 són algun altre vector de v_2, v_5. Els desplaçaments circulars de v_7 són ell mateix.
    (g) El polinomi generador és el polinomi mònic de grau mínim que representa alguna paraula del codi. En aquest cas és $x + 1$.

3 Matrius de Vandermonde i codis algebraics

1. (a) Demostreu que $\mathbb{Z}_3[x]/x^2 + x + 2$ és un cos.
   (b) Doneu una taula d'equivalències exponencial-polinomial-vectorial per a $\mathbb{Z}_3/(x^2+x+2)$ a partir de l'element α que representa la classe de x.
   (c) Quina és la matriu de Vandermonde $V_3(1, \alpha^2, \alpha^5)$?
   (d) Calculeu el determinant de $V_3(1, \alpha^2, \alpha^5)$.
   (e) Calculeu el producte $(\alpha^2 - 1)(\alpha^5 - 1)(\alpha^5 - \alpha^2)$.
   (f) Comproveu que
   $$\det(V_3(1, \alpha^2, \alpha^5))) = (\alpha^2 - 1)(\alpha^5 - 1)(\alpha^5 - \alpha^2).$$

   Solució:

   (a) És un cos perquè 3 és un primer i el polinomi $x^2 + x + 2$ és irreductible perquè té grau < 4 i no té arrels a $\mathbb{Z}_3$. En efecte, si l'avaluem a 0, 1 i 2, respectivament, dona $2 \neq 0$, $4 = 1 \neq 0$, $8 = 2 \neq 0$.
   (b)

pot.	*pol.*	*vect.*
0	0	00
α^0	1	10
α^1	α	01
α^2	$2\alpha + 1$	12
α^3	$2\alpha + 2$	22
α^4	2	20
α^5	2α	02
α^6	$\alpha + 2$	21
α^7	$\alpha + 1$	11
α^8	1	

   (c)
   $$V_4(1, \alpha^2, \alpha^5) = \begin{pmatrix} 1 & 1 & 1 \\ 1 & \alpha^2 & \alpha^5 \\ 1 & \alpha^4 & \alpha^2 \end{pmatrix}.$$
   (d) $\det(V_4(1, \alpha^2, \alpha^5)) = \alpha^4 + \alpha^5 + \alpha^4 - (\alpha^2 + \alpha + \alpha^2) = 20 + 02 + 20 + 21 + 02 + 21 = 20 = \alpha^4$.
   (e) $(\alpha^2 - 1)(\alpha^5 - 1)(\alpha^5 - \alpha^2) = \alpha^5\alpha^3\alpha^4 = \alpha^4$.
   (f) Hem vist que els dos valors valen α^4. Per tant, es dona la igualtat.

2. (a) El polinomi $x^3 + 2x^2 + x + 1$ és irreductible i primitiu sobre $\mathbb{Z}_3$. Quants elements té el cos $\mathbb{F} = \mathbb{Z}_3/(x^3 + 2x^2 + x + 1)$?
   (b) A continuació donem les primeres files d'una taula d'equivalències de les potències de $\alpha = [x]$. Completeu-la.

α^1	α
α^2	α^2
α^3	$\alpha^2+2\alpha+2$
α^4	$\alpha+2$
α^5	$\alpha^2+2\alpha$
α^6	$2\alpha+2$
α^7	$2\alpha^2+2\alpha$
α^8	$\alpha^2+\alpha+1$
α^9	$2\alpha^2+2$
α^{10}	$2\alpha^2+1$
α^{11}	$2\alpha^2+2\alpha+1$
α^{12}	$\alpha^2+2\alpha+1$
α^{13}	2
α^{14}	2α
α^{15}	$2\alpha^2$
α^{16}	$2\alpha^2+\alpha+1$
α^{17}	$2\alpha+1$
α^{18}	$2\alpha^2+\alpha$
α^{19}	$\alpha+1$
α^{20}	$\alpha^2+\alpha$
α^{21}	$2\alpha^2+2\alpha+2$
α^{22}	α^2+1

(c) Un codi C de Reed-Solomon primitiu i en sentit estricte definit sobre $\mathbb{F}$ té polinomi generador

$$g = x^4 + Ax^3 + \alpha^7 x^2 + \alpha^8 x + B,$$

on A, B són elements de $\mathbb{F}$. Quins són els valors de A i B?

(d) Quina és la dimensió de C? Quina és la distància mínima?

(e) Quants símbols té una paraula del codi? I quants trits?

(f) Doneu una paraula no nul·la del codi en símbols i en trits.

Solució:

(a) $3^3 = 27$.

(b)

α^{23}	α^2+2
α^{24}	$\alpha^2+\alpha+2$
α^{25}	$2\alpha^2+\alpha+2$
α^{26}	1

(c) Com que g té grau 4, haurà de ser $g = (x-\alpha)(x-\alpha^2)(x-\alpha^3)(x-\alpha^4)$. A és el coeficient de grau 3 que serà $A = -\alpha-\alpha^2-\alpha^3-\alpha^4 = \alpha^2+2\alpha+2 = \alpha^3$. B és el coeficient constant que serà $(-\alpha)(-\alpha^2)(-\alpha^3)(-\alpha^4) = 2\alpha^2+1 = \alpha^{10}$.

(d) Sabem que el grau de $g(=4)$ és $n-k = (q-1)-k = 26-k$. Deduïm que $k = 22$. D'altra banda, com que es tracta d'un codi Reed-Solomon, $d = n-k+1 = 26-22+1 = 5$.

(e) Una paraula codi té 26 símbols o, equivalentment, $26 \cdot 3 = 78$ trits.

(f) Podem agafar, per exemple, la paraula corresponent al polinomi generador: $g = x^4+\alpha^3x^3+\alpha^7x^2+\alpha^8x+\alpha^{10}$, que en símbols és

$$(\alpha^{10}, \alpha^8, \alpha^7, \alpha^3, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0)$$

i en trits és

(102 111 122 221 100 000 000 000 000 000 000 000 000 000 000
000 000 000 000 000 000 000 000 000 000).

3. (a) Comproveu que el polinomi x^4+x+1 sobre $\mathbb{Z}_2$
   i. És irreductible.
   ii. És primitiu.

   (b) Quants elements té el cos $\mathbb{F}$ que obtenim fent mòdul x^4+x+1 a $\mathbb{Z}_2[x]$? Per què?

   (c) Doneu-ne una taula potencial-vectorial.

   (d) Doneu el polinomi generador d'un codi C de Reed-Solomon sobre $\mathbb{F}$ primitiu en sentit estricte capaç de corregir dos esborralls.

   (e) Doneu els paràmetres (longitud, dimensió i distància mínima) de C.

   (f) Demostreu que la paraula $(\alpha^3\alpha^5 1000\alpha^3\alpha^5 1000\alpha^3\alpha^5 1)$ pertany al codi.

   (g) Amb quina cadena de bits la passaríem pel canal?

   (h) Corregiu els esborralls de la següent cadena de bits rebuda per un canal que afegeix només esborralls si s'ha emprat C per codificar la informació:

$$???????00000000000000000000000000000000000000000000000000001.$$

Solució:

(a) i. Com que avaluat a 0 i a 1 dona diferent de zero, no té arrels. Per tant, no té factors de grau 1. Tampoc és un múltiple de l'únic irreductible de grau 2. Per tant, és irreductible.
   ii. Si fem totes les potències de $\alpha=[x]$ veiem que no obtenim 1 fins a arribar a l'exponent 15. Vegeu l'apartat amb la taula d'equivalències potencial vectorial.

(b) El cos té 16 elements, ja que el polinomi està definit sobre $\mathbb{Z}_p$ amb $p=2$ i el grau del polinomi és $m=4$. Per tant, el cos obtingut té $p^m=16$ elements. És a dir, $\mathbb{F}=\mathbb{F}_{16}$.

(c) La taula d'equivalència vectorial-potencial és:

vect.	(1000)	(0100)	(0010)	(0001)	(1100)	(0110)	(0011)
pot.	α^0	α	α^2	α^3	α^4	α^5	α^6

(1101)	(1010)	(0101)	(1110)	(0111)	(1111)	(1011)	(1001)
α^7	α^8	α^9	α^{10}	α^{11}	α^{12}	α^{13}	α^{14}

(d) Per corregir dos esborralls cal una distància mínima més gran o igual que 3. Agafem com a polinomi generador $g(x)=(x-\alpha)(x-\alpha^2)=x^2+\alpha^5x+\alpha^3$.

(e) Longitud= $n=15$, dimensió= $k=n-\text{grau}(g)=15-2=13$. Com que és un codi RS, $d=n-k+1=15-13+1=3$.

(f) La paraula donada és la forma vectorial del polinomi $g+x^6g+x^{12}g=(1+x^6+x^{12})g$. Com que és un múltiple del polinomi generador és del codi.

(g) 0001 0110 1000 0000 0000 0000 0001 0110 1000 0000 0000 0000 0001 0110 1000.

(h) La paraula correspon al vector de símbols $??000000000000\alpha^3$. Per tant, el polinomi corresponent a la paraula rebuda és $u(x)=\alpha^3x^{14}$. Tenim les síndromes $u(\alpha)=\alpha^{3+14}=\alpha^2$, $u(\alpha^2)=\alpha^{3+2\cdot 14}=\alpha$ i hem de resoldre el sistema $\begin{pmatrix}1 & \alpha\\ 1 & \alpha^2\end{pmatrix}\begin{pmatrix}e_0\\ e_1\end{pmatrix}=\begin{pmatrix}\alpha^2\\ \alpha\end{pmatrix}$, que té solució $e_0=\alpha^5$ i $e_1=1$. Per tant, la paraula corregida és $00000000000000\alpha^3-\alpha^5 10000000000000=\alpha^5 1000000000000\alpha^3$. Observem que correspon al polinomi $x^{14}g$ i que haguéssim pogut deduir el resultat per la forma de la paraula rebuda.

4. (a) Comproveu que el polinomi $x^2 + x + 2$ és irreductible i primitiu a $\mathbb{Z}_3[x]$.
   (b) Doneu una taula exponencial-vectorial de $\mathbb{Z}_3[x]/x^2 + x + 2$, utilitzant $\alpha = [x]$.
   (c) Utilitzant aquest cos, construïm un codi C de Reed-Solomon primitiu en sentit estricte capaç de corregir tres esborralls en una mateixa paraula. Quina distància de disseny hem d'agafar?
   (d) Doneu el polinomi generador de C.
   (e) Quina és la dimensió de C?
   (f) Corregiu totes les paraules de la seqüència 0122012??2000000.
   (g) Quin polinomi generador tindrà el codi dual de C?

   Solució:

   (a) El polinomi és irreductible perquè té grau 2 i no té arrels ($f(0) = 2$, $f(1) = 1$ i $f(2) = 2$).
   (b)

0	00
1	10
α	01
α^2	12
α^3	22
α^4	20
α^5	02
α^6	21
α^7	11

   (c) Hem d'agafar distància prevista 4.
   (d) $g(x) = (x - \alpha)(x - \alpha^2)(x - \alpha^3) = x^3 + \alpha x^2 + \alpha^7 x + \alpha^2$.
   (e) La dimensió serà $n - \text{grau}(g) = 5$.
   (f) Tenim la paraula amb esborralls $(\alpha\alpha^3\alpha??000)$. El polinomi corresponent és $u(x) = \alpha x^2 + \alpha^3 x + \alpha$. Calculem $u(\alpha) = \alpha^3 + \alpha^4 + \alpha = 1$, $u(\alpha^2) = \alpha^5 + \alpha^5 + \alpha = \alpha^5$ i resolem el sistema $\begin{pmatrix} \alpha^3 & \alpha^4 \\ \alpha^6 & 1 \end{pmatrix}\begin{pmatrix} e_3 \\ e_4 \end{pmatrix} = \begin{pmatrix} 1 \\ \alpha^5 \end{pmatrix}$, d'on deduïm que $e_3 = \alpha^2$ i $e_4 = \alpha^3$. Per tant, la paraula corregida és $(\alpha, \alpha^3, \alpha, \alpha^6, \alpha^7, 0, 0, 0)$ corresponent a (0122012111000000).
   (g) El polinomi de control és $(x^8 - 1)/g = x^5 + \alpha^5 x^4 + \alpha x^3 + \alpha^3 x^2 + \alpha^3 x + \alpha^2$. El seu recíproc serà el generador del codi dual i és exactament $h* = \alpha^2 x^5 + \alpha^3 x^4 + \alpha^3 x^3 + \alpha x^2 + \alpha^5 x + 1$.

5. (a) Doneu justificadament un polinomi en x que generi $\mathbb{F}_4$ i doneu una taula exponencial-vectorial de $\mathbb{F}_4$.
   (b) Construïu un codi C de Reed-Solomon primitiu en sentit estricte sobre $\mathbb{F}_4$ capaç de corregir un esborrall, tot donant-ne el polinomi generador g.
   (c) Quin valor tenen la longitud i la dimensió de C?
   (d) Codifiqueu de manera sistemàtica utilitzant $g(x)$ la informació corresponent al polinomi x. Doneu el resultat en bits.
   (e) Doneu una matriu generadora de C.
   (f) Doneu una matriu de control de C.
   (g) Corregiu els esborralls de totes les paraules de la seqüència codificada de bits

   $$0011????0100.$$

   Doneu el resultat en bits.
   (h) Comproveu que la seqüència obtinguda pertany al codi.
   (i) Quin polinomi generador tindrà el codi dual de C?

   Solució:

(a) Els polinomis irreductibles de grau 2 de $\mathbb{Z}_2[x]$ seran aquells que no s'anul·lin a 0 (coef. constant 1) ni a 1 (nombre senar de termes no nuls). L'únic polinomi amb aquestes característiques és $x^2 + x + 1$.

0	00
1	10
α	01
α^2	11

(b) Hem d'agafar distància prevista 2 i polinomi generador $x - \alpha$.

(c) $n = 3$ i $k = 2$.

(d) $x \cdot x^{n-k} - (x \cdot x^{n-k} \mod g) = x^2 + \alpha^2$. Correspon a la paraula $\alpha^2 01 \equiv 110010$.

(e)
$$\begin{pmatrix} \alpha & 1 & 0 \\ 0 & \alpha & 1 \end{pmatrix}.$$

(f)
$$(1\alpha\alpha^2).$$

(g) Tenim dues paraules amb un esborrall cadascuna:

- $(0\alpha^2?)$: Agafem $u(x) = \alpha^2 x$ i resolem el sistema $\alpha^2 e_2 = u(\alpha) = \alpha^3 = 1$. Deduïm que $e_2 = \alpha$. Per tant, la primera paraula corregida és $(0\alpha^2\alpha) \equiv 001101$.
- $(?\alpha 0)$: Agafem $u(x) = \alpha x$ i resolem el sistema $\alpha^0 e_0 = u(\alpha) = \alpha^2$. Deduïm que $e_0 = \alpha^2$. Per tant, la segona paraula corregida és $(\alpha^2\alpha 0) \equiv 110100$.

(h) Veiem que la segona paraula és la mateixa que la primera paraula desplaçada. Com que és un codi cíclic, n'hi ha prou en comprovar que una de les dues pertany al codi. I, en efecte, la segona paraula correspon al polinomi generador multiplicat per α.

(i) El polinomi de control és $h(x) = (x^3 - 1)/(x - \alpha) = x^2 + \alpha x + \alpha^2$. El seu recíproc és $\alpha^2 x^2 + \alpha x + 1$. Si el que volem és un generador mònic, hem d'agafar $x^2 + \alpha^2 x + \alpha$.

6. (a) El polinomi $x^2 + x + 1$ és irreductible i primitiu sobre $\mathbb{Z}_2$. A continuació, donem la taula d'equivalències de $\mathbb{F}_4 = \mathbb{Z}_2/(x^2 + x + 1)$, on α és la classe de x:

0	00
1	10
α	01
α^2	11

Construïu un codi C de Reed-Solomon primitiu en sentit estricte sobre $\mathbb{F}_4$ capaç de corregir un esborrall i doneu-ne el polinomi generador g.

(b) Doneu una matriu generadora de C.

(c) Doneu una matriu de control de C.

(d) Codifiqueu de manera sistemàtica utilitzant $g(x)$ el bloc d'informació corresponent als bits 1001 i doneu el resultat en bits. A la paraula codi generada l'anomenem c.

(e) Comproveu que c pertany al codi.

(f) Afegiu un esborrall en una posició de la paraula c i doneu la paraula amb error obtinguda.

(g) Corregiu aquesta paraula explicant tots els passos.

Solució:

(a) Hem d'agafar distància prevista 2 i polinomi generador $x - \alpha$.

(b)
$$\begin{pmatrix} \alpha & 1 & 0 \\ 0 & \alpha & 1 \end{pmatrix}.$$

(c)
$$(1\alpha\alpha^2).$$

(d) $(1+\alpha x)\cdot x^{n-k} - ((1+\alpha x)\cdot x^{n-k} \mod g) = (1+\alpha x)\cdot x - ((1+\alpha x)\cdot x \mod g) = x+\alpha x^2 + (x+\alpha x^2 \mod x+\alpha) = x+\alpha x^2+\alpha^2$. Correspon a la paraula $\alpha^2 1\alpha \equiv 111001$.

(e) c pertany al codi perquè $\alpha x^2 + x + \alpha^2$ és divisible per g. En concret, $\alpha x^2 + x + \alpha^2 = (\alpha x + \alpha)g$.

(f) Podem agafar diferents opcions. Per exemple,
$?11001 \equiv ?1\alpha$
o bé
$11?001 \equiv \alpha^2?\alpha$
o bé
$11100? \equiv \alpha^2 1?$

(g) En el primer cas tenim $u = x + \alpha x^2$ i hem de resoldre el sistema $\alpha^0 e_0 = u(\alpha) = \alpha + 1 = \alpha^2$. Per tant, $e_0 = \alpha^2$ i obtenim la paraula corregida $(\alpha^2 1\alpha) \equiv 111001$.
En el segon cas tenim $u = \alpha^2 + \alpha x^2$ i hem de resoldre el sistema $\alpha e_1 = u(\alpha) = \alpha^2 + 1 = \alpha$. Per tant, $e_1 = 1$ i obtenim la paraula corregida $(\alpha^2 1\alpha) \equiv 111001$.
En el tercer cas tenim $u = \alpha^2 + x$ i hem de resoldre el sistema $\alpha^2 e_2 = u(\alpha) = \alpha^2 + \alpha = 1$. Ara $e_2 = \alpha$ i obtenim la paraula corregida $(\alpha^2 1\alpha) \equiv 111001$.

7. (a) Digueu tots els cossos primers i tots els polinomis que podem utilitzar per construir el cos finit de 8 elements.
(b) Escolliu una de les opcions de l'apartat anterior i doneu un element primitiu i la corresponent taula potencial-vectorial.
(c) Doneu el polinomi generador d'un codi Reed-Solomon primitiu en sentit estricte capaç de corregir dos esborralls.
(d) Quina longitud i quina dimensió té el codi?
(e) Doneu una paraula no nul·la del codi.
(f) Afegiu-li dos esborralls i corregiu la paraula obtinguda.

Solució:

(a) El cos primer ha de ser $\mathbb{Z}_2$ i els polinomis han de ser $x^3 + x^2 + 1$ o bé $x^3 + x + 1$, ja que són els únics polinomis de $\mathbb{Z}_2$ irreductibles de grau 3.

(b) En els dos casos $\alpha = [x]$ és un element primitiu.
La taula potencial-vectorial per a $\mathbb{Z}_2/x^3 + x^2 + 1$ és

0	000
α^0	100
α^1	010
α^2	001
α^3	101
α^4	111
α^5	110
α^6	011

La taula potencial-vectorial per a $\mathbb{Z}_2/x^3 + x + 1$ és

0	000
α^0	100
α^1	010
α^2	001
α^3	110
α^4	011
α^5	111
α^6	101

(c) Considerarem la segona cosntrucció de $\mathbb{F}_8$. Per corregir dos esborralls cal una distància mínima ≥ 3. Agafem $d = 3$. El polinomi generador serà $g(x) = (x - \alpha)(x - \alpha^2) = x^2 + \alpha^4 x + \alpha^3$.

(d) La longitud és $8 - 1 = 7$. La dimensió és $7 - \text{grau}(g) = 7 - 2 = 5$.

(e) Com a paraula no nul·la del codi podem agafar $(0\alpha^3\alpha^4 1000)$, que correspon al polinomi $x \cdot g$.

(f) Posem esborralls a les posicions primera i segona. Obtenim $(??\alpha^4 1000)$. El polinomi corresponent a la paraula rebuda, si substituïm els esborralls per zero, és $u(x) = \alpha^4 x^2 + x^3$.

Resolem el sistema $\begin{pmatrix} 1 & \alpha \\ 1 & \alpha^2 \end{pmatrix} \begin{pmatrix} e_0 \\ e_1 \end{pmatrix} = \begin{pmatrix} u(\alpha) \\ u(\alpha^2) \end{pmatrix} = \begin{pmatrix} \alpha^4 \\ \alpha^5 \end{pmatrix}$ i obtenim que $e_0 = 0$ i $e_1 = \alpha^3$.

Per tant, la paraula enviada ha de ser $(00\alpha^4 1000) - (0\alpha^3 00000) = (0\alpha^3\alpha^4 1000)$.

8. (a) És $\mathbb{Z}_3$ un cos? Per què?

(b) Comproveu que només hi ha tres polinomis mònics (coeficient de grau màxim igual a 1) irreductibles de grau 2 a $\mathbb{Z}_3[x]$ i doneu-los.

(c) Doneu un polinomi mònic $f(x)$ de grau 2 irreductible de $\mathbb{Z}_3[x]$ amb coeficient de grau 1 igual a 1.

(d) Comproveu si $f(x)$ és primitiu.

(e) Anomenem $\mathbb{F}$ al conjunt $\mathbb{Z}_3[x]/f(x)$. Quants elements té $\mathbb{F}$?

(f) És $\mathbb{F}$ un cos? Per què?

(g) Anomenem α a la classe de x dins de $\mathbb{Z}_3[x]/f(x)$. Doneu una taula d'equivalències exponencial-polinomial-vectorial de les potències de α.

(h) Volem construir un codi C de Reed-Solomon primitiu sobre $\mathbb{F}$ capaç de corregir tres errors, basat en l'element primitiu α. Quina longitud i quina dimensió hem d'agafar?

(i) Doneu una matriu generadora de C.

(j) Quantes files i quantes columnes té una matriu de control de C?

(k) Doneu les dues primeres files d'una matriu de control.

(l) Codifiqueu la cadena de símbols $\alpha\ \alpha^2\ \alpha^3\ \alpha^4$ i doneu el resultat en símbols.

(m) Codifiqueu la cadena de símbols $\alpha\ \alpha^2\ \alpha^3\ \alpha^4$ i doneu el resultat en dígits.

(n) Agafeu una paraula de C de les obtingudes en l'apartat (l) i afegiu-li tres esborralls.

(o) Expliqueu els passos de l'algoritme per determinar els valors dels esborralls.

(p) Expliciteu els càlculs de l'algoritme.

Solució:

(a) $\mathbb{Z}_3$ és un cos perquè 3 és primer.

(b) Per ser irreductible ha de tenir coeficient constant no nul. Només hi ha aquests polinomis mònics de grau 2 amb coeficient constant no nul:

- $x^2 + 1$ (grau 2 i no té arrels, per tant, és irreductible)
- $x^2 + x + 1$ (té arrel 1, per tant, no és irreductible)
- $x^2 + 2x + 1$ (té arrel 2, per tant, no és irreductible)
- $x^2 + 2$ (té arrel 1, per tant, no és irreductible)
- $x^2 + x + 2$ (grau 2 i no té arrels, per tant, és irreductible)
- $x^2 + 2x + 2$ (grau 2 i no té arrels, per tant, és irreductible)

Els únics polinomis mònics irreductibles són 3 i són $x^2 + 1$, $x^2 + x + 2$, $x^2 + 2x + 2$.

(c) L'únic polinomi mònic irreductible amb coeficient lineal igual a 1 és $x^2 + x + 2$.

(d) És primitiu perquè totes les potències de la classe de x en el quocient $\mathbb{Z}_3[x]/f(x)$ de grau més petit que 8 són diferents, com podem comprovar en la taula de l'apartat (g).

(e) 9.

(f) És un cos perquè 3 és primer i $x^2 + x + 2$ és irreductible.

(g)

pot.	*pol.*	*vect.*
0	0	00
α^0	1	10
α^1	α	01
α^2	$2\alpha+1$	12
α^3	$2\alpha+2$	22
α^4	2	20
α^5	2α	02
α^6	$\alpha+2$	21
α^7	$\alpha+1$	11
α^8	1	

(h) Per poder corregir tres errors hem d'agafar $d=7$. Aleshores la longitud i la dimensió són

$$n = q-1 = 8,$$

$$k = n-d+1 = 8-7+1 = 2.$$

(i)

$$G = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & \alpha & \alpha^2 & \alpha^3 & \alpha^4 & \alpha^5 & \alpha^6 & \alpha^7 \end{pmatrix}.$$

(j) La matriu H té 6 files i 10 columnes.

(k) Les tres primeres files són les següents.

$$\begin{pmatrix} 1 & \alpha & \alpha^\alpha & \alpha^3 & \alpha^4 & \alpha^5 & \alpha^6 & \alpha^7 \\ 1 & \alpha^2 & \alpha^4 & \alpha^6 & 1 & \alpha^2 & \alpha^4 & \alpha^6 \\ 1 & \alpha^3 & \alpha^6 & \alpha & \alpha^4 & \alpha^7 & \alpha^2 & \alpha^5 \end{pmatrix}.$$

(l) Separem els símbols de k en k, és a dir, de 2 en 2, i els multipliquem per la matriu generadora.

$$\begin{aligned} \begin{pmatrix} \alpha & \alpha^2 \end{pmatrix} G &= \begin{pmatrix} \alpha & \alpha^2 \end{pmatrix} \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & \alpha & \alpha^2 & \alpha^3 & \alpha^4 & \alpha^5 & \alpha^6 & \alpha^7 \end{pmatrix} \\ &= \begin{pmatrix} \alpha+2\alpha+1 & \alpha+2\alpha+2 & \alpha+2 & \alpha+2\alpha & \alpha+\alpha+2 & \alpha+\alpha+1 & \alpha+1 & \alpha+\alpha \end{pmatrix} \\ &= \begin{pmatrix} 1 & 2 & \alpha^6 & 0 & \alpha^3 & \alpha^2 & \alpha^7 & \alpha^5 \end{pmatrix}, \end{aligned}$$

$$\begin{aligned} \begin{pmatrix} \alpha^3 & \alpha^4 \end{pmatrix} G &= \alpha^2 \begin{pmatrix} \alpha & \alpha^2 \end{pmatrix} G \\ &= \begin{pmatrix} \alpha^2 & \alpha^6 & 1 & 0 & \alpha^5 & \alpha^4 & \alpha^9 & \alpha^7 \end{pmatrix}, \end{aligned}$$

La informació codificada en símbols serà, doncs, $12\alpha^6 0\alpha^3\alpha^2\alpha^7\alpha^5\alpha^2\alpha^6 10\alpha^5\alpha^4\alpha\alpha^7$.

(m) La informació codificada en dígits serà 10 20 21 00 22 12 11 02 12 21 10 00 02 20 01 11.

(n) Per exemple, agafem la paraula $12\alpha^6 0\alpha^3\alpha^2\alpha^7\alpha^5$ i li afegim tres esborralls al final. Obtenim $12\alpha^6 0\alpha^3???$

(o) Anomenem u al polinomi $1+2x+\alpha^6x^2+\alpha^3x^4$ i l'avaluem en les primeres potències de α. Obtenim

$$\begin{aligned} u(\alpha) &= 1+2\alpha+\alpha^8+\alpha^7 = 1+\alpha^5+1+\alpha^7 = 0 \\ u(\alpha^2) &= 1+2\alpha^2+\alpha^{10}+\alpha^{11} = 1+\alpha^6+\alpha^2+\alpha^3 = \alpha^5 \\ u(\alpha^3) &= 1+2\alpha^3+\alpha^{12}+\alpha^{15} = 1+\alpha^7+\alpha^4+\alpha^7 = \alpha^3 \end{aligned}$$

Haurem de resoldre el sistema

$$\begin{pmatrix} \alpha^5 & \alpha^6 & \alpha^7 \\ (\alpha^5)^2 & (\alpha^6)^2 & (\alpha^7)^2 \\ (\alpha^5)^3 & (\alpha^6)^3 & (\alpha^7)^3 \end{pmatrix} \begin{pmatrix} e_5 \\ e_6 \\ e_7 \end{pmatrix} = \begin{pmatrix} u(\alpha) \\ u(\alpha^2) \\ u(\alpha^3) \end{pmatrix},$$

és a dir,

$$\begin{pmatrix} \alpha^5 & \alpha^6 & \alpha^7 \\ \alpha^2 & \alpha^4 & \alpha^6 \\ \alpha^7 & \alpha^2 & \alpha^5 \end{pmatrix} \begin{pmatrix} e_5 \\ e_6 \\ e_7 \end{pmatrix} = \begin{pmatrix} 0 \\ \alpha^5 \\ \alpha^3 \end{pmatrix}.$$

(p) La matriu inversa de la matriu del sistema és

$$\frac{1}{\alpha^6+\alpha^3+\alpha^3-\alpha^2-\alpha^5-\alpha^5} \begin{pmatrix} (\alpha-1) & -(\alpha^3-\alpha) & (\alpha^4-\alpha^3) \\ -(\alpha^7-\alpha^5) & (\alpha^2-\alpha^6) & -(\alpha^3-\alpha) \\ (\alpha^4-\alpha^3) & -(\alpha^7-\alpha^5) & (\alpha-1) \end{pmatrix} = \alpha^5 \begin{pmatrix} \alpha^6 & \alpha^2 & \alpha \\ \alpha^6 & \alpha^6 & \alpha^2 \\ \alpha & \alpha^6 & \alpha^6 \end{pmatrix}$$
$$= \begin{pmatrix} \alpha^3 & \alpha^7 & \alpha^6 \\ \alpha^3 & \alpha^3 & \alpha^7 \\ \alpha^6 & \alpha^3 & \alpha^3 \end{pmatrix}.$$

Per tant, el valor dels esborralls és

$$\begin{pmatrix} \alpha^3 & \alpha^7 & \alpha^6 \\ \alpha^3 & \alpha^3 & \alpha^7 \\ \alpha^6 & \alpha^3 & \alpha^3 \end{pmatrix} \begin{pmatrix} 0 \\ \alpha^5 \\ \alpha^3 \end{pmatrix} = \begin{pmatrix} \alpha^4+\alpha \\ 1+\alpha^2 \\ 1+\alpha^6 \end{pmatrix} = \begin{pmatrix} \alpha^6 \\ \alpha^3 \\ \alpha \end{pmatrix}.$$

Deduïm que la paraula corregida és $12\alpha^6 0\alpha^3 000 - 00000\alpha^6\alpha^3\alpha = 12\alpha^6 0\alpha^3\alpha^2\alpha^7\alpha^5$.

9. (a) Construcció d'un cos finit.
   - Comproveu que el polinomi $x^3 + x + 1$ és irreductible i primitiu sobre $\mathbb{Z}_2$.
     Solució:
     És irreductible perquè és de grau 2 i no té arrels. És primitiu perquè $\alpha = [x]$ té ordre 7 (vegeu la taula de l'apartat següent).
   - Construïu $\mathbb{F}_8$ utilitzant aquest polinomi i doneu-ne una taula exponencial-vectorial.
     Solució:

0	α^0	α^1	α^2	α^3	α^4	α^5	α^6
000	100	010	001	110	011	111	101

(b) Definiu el codi RS primitiu i en sentit estricte, amb longitud 7, capaç de detectar dos errors.
   - Doneu-ne el polinomi generador.
     Solució:
     $g = (x-\alpha)(x-\alpha^2) = x^2 + \alpha^4 x + \alpha^3$.
   - Doneu-ne el polinomi de control.
     Solució:
     $h = (x^7-1)/g(x) = x^5 + \alpha^4 x^4 + x^3 + \alpha^5 x^2 + \alpha^5 x + \alpha^4$.
   - Doneu-ne la longitud i la dimensió.
     Solució:
     $n = 7$, $k = 5$.
   - Doneu-ne una matriu generadora.
     Solució:

$$G = \begin{pmatrix} \alpha^3 & \alpha^4 & 1 & 0 & 0 & 0 & 0 \\ 0 & \alpha^3 & \alpha^4 & 1 & 0 & 0 & 0 \\ 0 & 0 & \alpha^3 & \alpha^4 & 1 & 0 & 0 \\ 0 & 0 & 0 & \alpha^3 & \alpha^4 & 1 & 0 \\ 0 & 0 & 0 & 0 & \alpha^3 & \alpha^4 & 1 \end{pmatrix}$$

- Doneu-ne una matriu de control.
  Solució:

$$H = \begin{pmatrix} 1 & \alpha^4 & 1 & \alpha^5 & \alpha^5 & \alpha^4 & 0 \\ 0 & 1 & \alpha^4 & 1 & \alpha^5 & \alpha^5 & \alpha^4 \end{pmatrix}$$

- Quants errors podem garantir que podrà corregir?
  Solució:
  Podrà corregir un error.

(c) Codifiqueu de manera sistemàtica utilitzant el polinomi generador el primer bloc d'informació de la seqüència $01\alpha01\alpha01\alpha01\alpha\ldots$

Solució:

Agafem $i(x) = x+\alpha x^2+x^4$. La codificació sistemàtica serà $c(x) = i(x)x^{n-k} - (i(x)x^{n-k} \mod g(x)) = x^6 + \alpha x^4 + x^3 + \alpha x + \alpha^6$, que correspon a la paraula $(\alpha^6, \alpha, 0, 1, \alpha, 0, 1)$.

(d) En quines posicions és sistemàtica la codificació anterior?

Solució:

En les darreres.

(e) Corregiu els errors de la primera paraula de la seqüència
$\alpha^3 0\alpha^4\alpha^5 1\alpha 1\alpha^3 10\alpha^5\alpha^4\ldots$

Solució:

Com que la distància mínima és 3, només corregim un error.

El polinomi corresponent a la primera paraula rebuda és $u(x) = \alpha^3 + \alpha^4 x^2 + \alpha^5 x^3 + x^4 + \alpha x^5 + x^6$.
Les síndromes són $u(\alpha) = \alpha$, $u(\alpha^2) = \alpha^2$.

Tenim rang() $\neq$ rang $\begin{pmatrix} \alpha \\ \alpha^2 \end{pmatrix}$ i, en canvi, $\text{rang}(\alpha) = \text{rang}\begin{pmatrix} \alpha & \alpha^2 \end{pmatrix} = 1$. Per tant, $t = 1$. Resolem el sistema $\alpha l_0 = -\alpha^2$ i obtenim $l_0 = \alpha$ i, per tant, el localitzador d'errors és $\lambda = x + \alpha$.

Com que λ s'anul·la a α, deduïm que hi ha un error a la segona posició i el seu valor el calculem resolent el sistema $\alpha e_1 = u(\alpha) = \alpha$, que ens dona $e_1 = 1$.

Per tant, la paraula corregida és $\alpha^3 0\alpha^4\alpha^5 1\alpha 1 - 0100000 = \alpha^3 1\alpha^4\alpha^5 1\alpha 1$.

10. (a) És $\mathbb{Z}_7$ un cos? Per què?

(b) Comproveu que $a = 5$ és un element primitiu de $\mathbb{Z}_7$.

(c) Volem construir un codi C de Reed-Solomon primitiu sobre $\mathbb{Z}_7$ capaç de corregir dos errors, basat en l'element primitiu $a = 5$. Quina longitud i quina dimensió hem d'agafar?

(d) Doneu el polinomi generador del codi.

(e) Doneu dues matrius generadores de C, per procediments diferents: una fent servir el polinomi generador i l'altra fent servir l'element primitiu $a = 5$.

(f) Doneu la matriu de control de C fent servir l'element primitiu $a = 5$.

(g) Escolliu una de les matrius generadores de l'apartat 5 i codifiqueu la informació 110256 en funció de la matriu generadora escollida.

(h) Quina síndrome té la paraula 421632?

(i) Determineu si la paraula 421632 té error i, en cas de tenir-ne, corregiu-la.

(j) Quina síndrome té la paraula 342650?

(k) Determineu si la paraula 342650 té error i, en cas de tenir-ne, corregiu-la.

(l) Quina síndrome té la paraula 025625?

(m) Determineu si la paraula 025625 té error i, en cas de tenir-ne, corregiu-la.

(n) Escolliu una de les matrius generadores que heu trobat en l'apartat 5. Per cadascuna de les tres paraules corregides en els apartats anteriors, quina informació s'ha codificat, si per codificar s'ha emprat la matriu generadora que heu escollit?

Solució:

(a) $\mathbb{Z}_7$ és un cos perquè 7 és primer.

(b) En efecte, les seves potències són

5^0	1
5^1	5
5^2	4
5^3	6
5^4	2
5^5	3
5^6	1

(c) Per poder corregir dos errors hem d'agafar $d = 5$. Aleshores la longitud i la dimensió són

$$n = q - 1 = 6,$$

$$k = n - d + 1 = 2.$$

(d) El polinomi generador és $(x-5)(x-4)(x-6)(x-2) = x^4 + (-5-4-6-2)x^3 + (5\cdot 4 + 5\cdot 6 + 5\cdot 2 + 4\cdot 6 + 4\cdot 2 + 6\dot{2})x^2 + (-5\cdot 4\cdot 6 - 5\cdot 4\cdot 2 - 5\cdot 6\cdot 2 - 4\cdot 6\cdot 2)x + 5\cdot 4\cdot 6\cdot 2 = x^4 + 4x^3 + 6x^2 + 5x + 2$.

(e) Utilitzant el polinomi generador, obtenim

$$G' = \begin{pmatrix} 2 & 5 & 6 & 4 & 1 & 0 \\ 0 & 2 & 5 & 6 & 4 & 1 \end{pmatrix}.$$

Fent servir l'element primitiu $a = 5$,

$$G = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 5 & 4 & 6 & 2 & 3 \end{pmatrix}.$$

(f)

$$H = \begin{pmatrix} 1 & 5 & 4 & 6 & 2 & 3 \\ 1 & 4 & 2 & 1 & 4 & 2 \\ 1 & 6 & 1 & 6 & 1 & 6 \\ 1 & 2 & 4 & 1 & 2 & 4 \end{pmatrix}.$$

(g) Escollim la segona matriu generadora (G). Separem la informació en blocs de k símbols i multipliquem cada bloc per G.

$$\begin{pmatrix} 1 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 5 & 4 & 6 & 2 & 3 \end{pmatrix} = \begin{pmatrix} 2 & 6 & 5 & 0 & 3 & 4 \end{pmatrix},$$

$$\begin{pmatrix} 0 & 2 \end{pmatrix} \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 5 & 4 & 6 & 2 & 3 \end{pmatrix} = \begin{pmatrix} 2 & 3 & 1 & 5 & 4 & 6 \end{pmatrix},$$

$$\begin{pmatrix} 5 & 6 \end{pmatrix} \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 5 & 4 & 6 & 2 & 3 \end{pmatrix} = \begin{pmatrix} 4 & 0 & 1 & 6 & 3 & 2 \end{pmatrix}.$$

La informació codificada serà, doncs, 265034231546401632.

Si haguéssim escollit la primera matriu generadora (G'), la informació codificada seria: 204351043512324016.

(h) Anomenem u indistintament al vector 421632 i al polinomi $4+2x+x^2+6x^3+3x^4+2x^5$. Les síndromes de u són

$$\begin{pmatrix} u(a) \\ u(a^2) \\ u(a^3) \\ u(a^4) \end{pmatrix} = \begin{pmatrix} 1 & 5 & 4 & 6 & 2 & 3 \\ 1 & 4 & 2 & 1 & 4 & 2 \\ 1 & 6 & 1 & 6 & 1 & 6 \\ 1 & 2 & 4 & 1 & 2 & 4 \end{pmatrix} \begin{pmatrix} 4 \\ 2 \\ 1 \\ 6 \\ 3 \\ 2 \end{pmatrix} = \begin{pmatrix} 3 \\ 1 \\ 5 \\ 4 \end{pmatrix}.$$

(i) Com que la síndrome no és nul·la, deduïm que hi ha hagut error.

Tenim $\text{rang}() \neq \text{rang}\begin{pmatrix} 3 \\ 1 \\ 5 \\ 4 \end{pmatrix}$, però $\text{rang}\begin{pmatrix} 3 \\ 1 \\ 5 \end{pmatrix} = \text{rang}\begin{pmatrix} 3 & 1 \\ 1 & 5 \\ 5 & 4 \end{pmatrix}$. Per tant, $t = 1$ i només s'ha produït un error. Resolem el sistema $3l_0 = -1$ que té solució $l_0 = 2$. Deduïm que el polinomi localitzador d'errors és $\lambda = x + 2$, que només té l'arrel $5 = 5^1$. Per tant, hi ha un error a la segona posició (primera, si comencem enumerant per 0). Per calcular el valor de l'error resolem el sistema $5^1 e_1 = u(a) = 3$ que ens dona solució $e_1 = 2$. Per tant, la paraula corregida és $c' = u - (020000) = (421632) - (020000) = (401632)$.

(j) Anomenem u indistintament al vector 342650 i al polinomi $3+4x+2x^2+6x^3+5x^4$. Les síndromes de u són

$$\begin{pmatrix} u(a) \\ u(a^2) \\ u(a^3) \\ u(a^4) \end{pmatrix} = \begin{pmatrix} 1 & 5 & 4 & 6 & 2 & 3 \\ 1 & 4 & 2 & 1 & 4 & 2 \\ 1 & 6 & 1 & 6 & 1 & 6 \\ 1 & 2 & 4 & 1 & 2 & 4 \end{pmatrix} \begin{pmatrix} 3 \\ 4 \\ 2 \\ 6 \\ 5 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}.$$

(k) Com que la síndrome és nul·la, deduïm que no hi ha hagut error.

(l) Anomenem u indistintament al vector 025625 i al polinomi $2x+5x^2+6x^3+2x^4+5x^5$. Les síndromes de u són

$$\begin{pmatrix} u(a) \\ u(a^2) \\ u(a^3) \\ u(a^4) \end{pmatrix} = \begin{pmatrix} 1 & 5 & 4 & 6 & 2 & 3 \\ 1 & 4 & 2 & 1 & 4 & 2 \\ 1 & 6 & 1 & 6 & 1 & 6 \\ 1 & 2 & 4 & 1 & 2 & 4 \end{pmatrix} \begin{pmatrix} 0 \\ 2 \\ 5 \\ 6 \\ 2 \\ 5 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ 1 \\ 5 \end{pmatrix}.$$

(m) Com que la síndrome no és nul·la, deduïm que hi ha hagut error.

Tenim $\text{rang}() \neq \text{rang}\begin{pmatrix} 1 \\ 0 \\ 1 \\ 5 \end{pmatrix}$, $\text{rang}\begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix} \neq \text{rang}\begin{pmatrix} 1 & 0 \\ 0 & 1 \\ 1 & 5 \end{pmatrix}$, mentre que $\text{rang}\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \text{rang}\begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 5 \end{pmatrix} = 2$. Per tant, $t = 2$. Resolem el sistema

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} l_0 \\ l_1 \end{pmatrix} = \begin{pmatrix} -1 \\ -5 \end{pmatrix} = \begin{pmatrix} 6 \\ 2 \end{pmatrix},$$

que té solució $l_0 = 6$, $l_1 = 2$. Deduïm que el polinomi localitzador d'errors és

$$\lambda = x^2 + 2x + 6.$$

Les seves arrels són $2 = 5^4$ i $3 = 5^5$ i, per tant, les posicions d'error seran la cinquena i la sisena (o la quarta i la cinquena, si comencem enumerant per 0).

Per calcular el valor de l'error resolem el sistema

$$\begin{pmatrix} 5^4 & 5^5 \\ 5^2 & 5^4 \end{pmatrix}\begin{pmatrix} e_4 \\ e_5 \end{pmatrix} = \begin{pmatrix} 2 & 3 \\ 4 & 2 \end{pmatrix}\begin{pmatrix} e_4 \\ e_5 \end{pmatrix} = \begin{pmatrix} u(a) \\ u(a^2) \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix}.$$

Restant dues vegades la primera fila a la segona obtenim

$$\begin{pmatrix} 2 & 3 \\ 0 & 3 \end{pmatrix}\begin{pmatrix} e_4 \\ e_5 \end{pmatrix} = \begin{pmatrix} 1 \\ 5 \end{pmatrix}.$$

Restant la segona fila a la primera obtenim

$$\begin{pmatrix} 2 & 0 \\ 0 & 3 \end{pmatrix}\begin{pmatrix} e_4 \\ e_5 \end{pmatrix} = \begin{pmatrix} 3 \\ 5 \end{pmatrix}.$$

Deduïm que $e_4 = 5$, $e_5 = 4$.

Per tant, la paraula corregida és $c' = u - (000054) = (025625) - (000054) = (025641)$.

(n) Si escollim la primera matriu generadora (G'), la informació que s'ha codificat era 225001. Si escollim la segona matriu generadora (G), la informació que s'ha codificat era 561234.

11. Considerem el codi C primitiu de Reed-Solomon capaç de corregir tres errors sobre $\mathbb{Z}_{11}$, generat per l'element primitiu $a = 2$.
   (a) Quina distància mínima hem d'agafar per construir C?
   (b) Quina longitud i quina dimensió té C?
   (c) Doneu una matriu generadora de C.
   (d) Considerem la paraula $u = (10, 10, 5, 2, 3, 9, 10, 5, 1, 6)$. Si avaluem el polinomi $u(x) = 6x^9 + x^8 + 5x^7 + 10x^6 + 9x^5 + 3x^4 + 2x^3 + 5x^2 + 10x + 10$ en les primeres potències de 2 ens dona els següents valors:

$$\begin{aligned} u(2^1) &= 5 \\ u(2^2) &= 5 \\ u(2^3) &= 6 \\ u(2^4) &= 0 \\ u(2^5) &= 8 \\ u(2^6) &= 7 \\ u(2^7) &= 5 \\ u(2^8) &= 0 \\ u(2^9) &= 3 \\ u(2^{10}) &= 6 \end{aligned}$$

   Quants errors té la paraula u respecte C?
   (e) Quines són les posicions dels errors?
   (f) Quins són els valors dels errors?
   (g) Quina és la paraula corregida?
   (h) Considerem la paraula $v = (8, 2, 9, 7, 0, 5, 9, 8, 2, 0)$. Si avaluem el polinomi $v(x) = 2x^8 + 8x^7 + 9x^6 + 5x^5 + 7x^3 + 9x^2 + 2x + 8$ en les primeres potències de 2 ens dona els següents valors:

$$\begin{aligned} v(2^1) &= 0 \\ v(2^2) &= 3 \\ v(2^3) &= 8 \\ v(2^4) &= 1 \\ v(2^5) &= 6 \\ v(2^6) &= 9 \\ v(2^7) &= 2 \\ v(2^8) &= 2 \\ v(2^9) &= 10 \\ v(2^{10}) &= 6 \end{aligned}$$

Quants errors té la paraula u respecte C?

(i) Quines són les posicions dels errors?

(j) Quins són els valors dels errors?

(k) Quina és la paraula corregida?

Solució:

(a) $d = 7$.

(b) $n = 10$, $k = 4$.

(c)
$$G = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 2^0 & 2^1 & 2^2 & 2^3 & 2^4 & 2^5 & 2^6 & 2^7 & 2^8 & 2^9 \\ 2^0 & 2^2 & 2^4 & 2^6 & 2^8 & 2^1 & 2^2 & 2^4 & 2^6 & 2^8 \\ 2^0 & 2^3 & 2^6 & 2^9 & 2^2 & 2^5 & 2^8 & 2^1 & 2^4 & 2^7 \end{pmatrix}$$
$$= \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 2 & 4 & 8 & 5 & 10 & 9 & 7 & 3 & 6 \\ 1 & 4 & 5 & 9 & 3 & 1 & 4 & 5 & 9 & 3 \\ 1 & 8 & 9 & 6 & 4 & 10 & 3 & 2 & 5 & 7 \end{pmatrix}.$$

(d) El vector de síndromes de u és $\begin{pmatrix} 5 \\ 5 \\ 6 \\ 0 \\ 8 \\ 7 \end{pmatrix}$.

Tenim rang() $\neq$ rang $\begin{pmatrix} 5 \\ 5 \\ 6 \\ 0 \\ 8 \\ 7 \end{pmatrix}$ i rang $\begin{pmatrix} 5 \\ 5 \\ 6 \\ 0 \\ 8 \end{pmatrix} \neq$ rang $\begin{pmatrix} 5 & 5 \\ 5 & 6 \\ 6 & 0 \\ 0 & 8 \\ 8 & 7 \end{pmatrix}$. Però rang $\begin{pmatrix} 5 & 5 \\ 5 & 6 \\ 6 & 0 \\ 0 & 8 \end{pmatrix} =$ rang $\begin{pmatrix} 5 & 5 & 6 \\ 5 & 6 & 0 \\ 6 & 0 & 8 \\ 0 & 8 & 7 \end{pmatrix} =$ 2, ja que $\begin{pmatrix} 5 & 5 \\ 5 & 6 \\ 6 & 0 \\ 0 & 8 \end{pmatrix} \begin{pmatrix} 5 \\ 5 \end{pmatrix} = \begin{pmatrix} 6 \\ 0 \\ 8 \\ 7 \end{pmatrix}$. Deduïm que s'han produït dos errors.

(e) Com hem vist, $\begin{pmatrix} 5 & 5 \\ 5 & 6 \end{pmatrix} \begin{pmatrix} 5 \\ 5 \end{pmatrix} = \begin{pmatrix} 6 \\ 0 \end{pmatrix}$. Per tant, $l_0 = -5 = 6$ i $l_1 = -5 = 6$ són la solució del sistema $\begin{pmatrix} 5 & 5 \\ 5 & 6 \end{pmatrix} \begin{pmatrix} l_0 \\ l_1 \end{pmatrix} = \begin{pmatrix} -6 \\ 0 \end{pmatrix}$. Per tant, el polinomi localitzador d'errors és $x^2 + 6x + 6$. Les seves arrels són $2 = 2^1$ i $3 = 2^8$. Per tant, les posicions d'error són la primera i la vuitena (començant per 0).

(f) Per calcular el valor dels errors resolem
$$\begin{pmatrix} 2^1 & 2^8 \\ 2^2 & 2^6 \end{pmatrix} \begin{pmatrix} e_1 \\ e_8 \end{pmatrix} = \begin{pmatrix} 5 \\ 5 \end{pmatrix},$$
és a dir,
$$\begin{pmatrix} 2 & 3 \\ 4 & 9 \end{pmatrix} \begin{pmatrix} e_1 \\ e_8 \end{pmatrix} = \begin{pmatrix} 5 \\ 5 \end{pmatrix},$$
equivalent a
$$\begin{pmatrix} 2 & 3 \\ 0 & 3 \end{pmatrix} \begin{pmatrix} e_1 \\ e_8 \end{pmatrix} = \begin{pmatrix} 5 \\ 6 \end{pmatrix},$$

i a

$$\begin{pmatrix} 2 & 0 \\ 0 & 3 \end{pmatrix}\begin{pmatrix} e_1 \\ e_8 \end{pmatrix} = \begin{pmatrix} 10 \\ 6 \end{pmatrix},$$

que té solució $e_1 = 5$, $e_8 = 2$ i aquests són els valors dels errors.

(g) La paraula corregida serà, doncs, $u - e = (10, 10, 5, 2, 3, 9, 10, 5, 1, 6) - (0, 5, 0, 0, 0, 0, 0, 0, 2, 0) = (10, 5, 5, 2, 3, 9, 10, 5, 10, 6)$.

(h) El vector de síndromes de v és $\begin{pmatrix} 0 \\ 3 \\ 8 \\ 1 \\ 6 \\ 9 \end{pmatrix}$.

Tenim $\mathrm{rang}() \neq \mathrm{rang}\begin{pmatrix} 0 \\ 3 \\ 8 \\ 1 \\ 6 \\ 9 \end{pmatrix}$, $\mathrm{rang}\begin{pmatrix} 0 \\ 3 \\ 8 \\ 1 \\ 6 \end{pmatrix} \neq \mathrm{rang}\begin{pmatrix} 0 & 3 \\ 3 & 8 \\ 8 & 1 \\ 1 & 6 \\ 6 & 9 \end{pmatrix}$, $\mathrm{rang}\begin{pmatrix} 0 & 3 \\ 3 & 8 \\ 8 & 1 \\ 1 & 6 \end{pmatrix} \neq \mathrm{rang}\begin{pmatrix} 0 & 3 & 8 \\ 3 & 8 & 1 \\ 8 & 1 & 6 \\ 1 & 6 & 9 \end{pmatrix}$, ja que, per exemple, $\det\begin{pmatrix} 0 & 3 & 8 \\ 3 & 8 & 1 \\ 8 & 1 & 6 \end{pmatrix} = 2+2-6-10 = -1 = 10$. Com que tindrem $\mathrm{rang}\begin{pmatrix} 0 & 3 & 8 \\ 3 & 8 & 1 \\ 8 & 1 & 6 \end{pmatrix} = \mathrm{rang}\begin{pmatrix} 0 & 3 & 8 & 1 \\ 3 & 8 & 1 & 6 \\ 8 & 1 & 6 & 9 \end{pmatrix} = 3$, deduïm que el nombre d'errors és 3.

(i) Hem de resoldre $\begin{pmatrix} 0 & 3 & 8 \\ 3 & 8 & 1 \\ 8 & 1 & 6 \end{pmatrix}\begin{pmatrix} l_0 \\ l_1 \\ l_2 \end{pmatrix} = \begin{pmatrix} -1 \\ -6 \\ -9 \end{pmatrix} = \begin{pmatrix} 10 \\ 5 \\ 2 \end{pmatrix}$. Com que $10 \cdot 3 = 8$, restem a la tercera fila la segona multiplicada per 10. $\begin{pmatrix} 0 & 3 & 8 \\ 3 & 8 & 1 \\ 0 & 9 & 7 \end{pmatrix}\begin{pmatrix} l_0 \\ l_1 \\ l_2 \end{pmatrix} = \begin{pmatrix} 10 \\ 5 \\ 7 \end{pmatrix}$. Restem a la tercera fila la primera multiplicada per tres. $\begin{pmatrix} 0 & 3 & 8 \\ 3 & 8 & 1 \\ 0 & 0 & 5 \end{pmatrix}\begin{pmatrix} l_0 \\ l_1 \\ l_2 \end{pmatrix} = \begin{pmatrix} 10 \\ 5 \\ 10 \end{pmatrix}$. Deduïm que $l_2 = 2$, $l_1 = 1$, $l_0 = 10$. Per tant, el polinomi localitzador d'errors és $x^3+2x^2+9x+10$. Les seves arrels són $1 = 2^0$, $2 = 2^1$ i $6 = 2^9$. Per tant, les posicions d'error són la 0-èsima, la primera i la novena, començant per 0.

(j) Per calcular el valor dels errors resolem

$$\begin{pmatrix} 2^0 & 2^1 & 2^9 \\ 2^0 & 2^2 & 2^8 \\ 2^0 & 2^3 & 2^7 \end{pmatrix}\begin{pmatrix} e_0 \\ e_1 \\ e_9 \end{pmatrix} = \begin{pmatrix} 0 \\ 3 \\ 8 \end{pmatrix},$$

és a dir,

$$\begin{pmatrix} 1 & 2 & 6 \\ 1 & 4 & 3 \\ 1 & 8 & 7 \end{pmatrix}\begin{pmatrix} e_0 \\ e_1 \\ e_9 \end{pmatrix} = \begin{pmatrix} 0 \\ 3 \\ 8 \end{pmatrix},$$

equivalent a

$$\begin{pmatrix} 1 & 2 & 6 \\ 0 & 2 & 8 \\ 0 & 6 & 1 \end{pmatrix}\begin{pmatrix} e_0 \\ e_1 \\ e_9 \end{pmatrix} = \begin{pmatrix} 0 \\ 3 \\ 8 \end{pmatrix},$$

equivalent a

$$\begin{pmatrix} 1 & 2 & 6 \\ 0 & 2 & 8 \\ 0 & 0 & 10 \end{pmatrix} \begin{pmatrix} e_0 \\ e_1 \\ e_9 \end{pmatrix} = \begin{pmatrix} 0 \\ 3 \\ 10 \end{pmatrix},$$

que té solució $e_9 = 1$, $e_1 = 3$, $e_0 = 10$ i aquests són els valors dels errors.

(k) La paraula corregida serà, doncs, $v - e = (8,2,9,7,0,5,9,8,2,0) - (10,3,0,0,0,0,0,0,0,1) = (9,10,9,7,0,5,9,8,2,10)$.

12. (a) **Definició d'un codi**

Anomenarem C a un codi primitiu, de Reed-Solomon, capaç de corregir dos errors, construït sobre el cos $\mathbb{F}_{3^2}$.

i. Comproveu que el polinomi $x^2 + x + 2 \in \mathbb{F}_3$ és irreductible i utilitzeu-lo per construir $\mathbb{F}_{3^2}$.
Solució:
És irreductible perquè és de grau 2 i no té arrels.

ii. Doneu l'equivalència vectorial-exponencial per a cada element de $\mathbb{F}_{3^2}$.
Solució:

pot.	pol.	vec.
0	0	00
α^0	1	10
α^1	α	01
α^2	$2\alpha + 1$	12
α^3	$2\alpha + 2$	22
α^4	2	20
α^5	2α	02
α^6	$\alpha + 2$	21
α^7	$\alpha + 1$	11

iii. Doneu el polinomi generador del codi C.
Solució:
$(x-\alpha)(x-\alpha^2)(x-\alpha^3)(x-\alpha^4) = \alpha^2 + \alpha^4 x + \alpha^2 x^2 + \alpha^7 x^3 + x^4$.

iv. Doneu la longitud, la dimensió i la distància mínima de C.
Solució:
- $n = 8$,
- $k = n - \text{grau}(g) = 8 - 4 = 4$,
- $d = 5$.

v. Doneu la matriu de control del codi C.
Solució:

$$H = \begin{pmatrix} 1 & \alpha & \alpha^2 & \alpha^3 & \alpha^4 & \alpha^5 & \alpha^6 & \alpha^7 \\ 1 & \alpha^2 & \alpha^4 & \alpha^6 & 1 & \alpha^2 & \alpha^4 & \alpha^6 \\ 1 & \alpha^3 & \alpha^6 & \alpha & \alpha^4 & \alpha^7 & \alpha^2 & \alpha^5 \\ 1 & \alpha^4 & 1 & \alpha^4 & 1 & \alpha^4 & 1 & \alpha^4 \end{pmatrix}$$

(b) **Procés de codificació-descodificació**

Codificarem la imatge 0 1 1 2 2 2 1 0 0 0 0 . Tot seguit l'introduirem en un canal ternari amb soroll additiu i, després, la descodificarem.

i. Amb la tècnica de codificació sistemàtica per a codis cíclics, codifiqueu el primer bloc de l'anterior informació usant el codi C.
Solució:
Hem de codificar la informació $\alpha\alpha^2\alpha^3 1$, corresponent als primers $k = 4$ símbols. La paraula codificada serà $\alpha^4\alpha^7\alpha^2\alpha^3\alpha\alpha^2\alpha^3 1$.

ii. El canal pel qual circularà la paraula codificada és un canal ternari en què hi ha un soroll additiu que ens donarà el vector d'error següent:
$e = (121200000000000000000000000000000\ldots)$.

Calculeu la paraula que trobarem a la sortida del canal.
Solució:
$\alpha^4\alpha^7\alpha^2\alpha^3\alpha\alpha^2\alpha^3 1 + \alpha^2\alpha^2 000000 = \alpha^5\alpha^4\alpha^2\alpha^3\alpha\alpha^2\alpha^3 1$.

iii. Calculeu el polinomi localitzador d'errors necessaris per corregir el vector rebut.
Solució:
Considerem el polinomi

$$u(x) = \alpha^5 + \alpha^4 x + \alpha^2 x^2 + \alpha^3 x^3 + \alpha x^4 + \alpha^2 x^5 + \alpha^3 x^6 + x^7.$$

Les síndromes seran

- $u(\alpha) = \alpha$
- $u(\alpha^2) = \alpha^5$
- $u(\alpha^3) = \alpha^7$
- $u(\alpha^4) = 0$

Tenim rang() $\neq$ rang $\begin{pmatrix} \alpha \\ \alpha^5 \\ \alpha^7 \\ 0 \end{pmatrix}$, rang $\begin{pmatrix} \alpha \\ \alpha^5 \\ \alpha^7 \end{pmatrix} \neq$ rang $\begin{pmatrix} \alpha & \alpha^5 \\ \alpha^5 & \alpha^7 \\ \alpha^7 & 0 \end{pmatrix}$, mentre que rang $\begin{pmatrix} \alpha & \alpha^5 \\ \alpha^5 & \alpha^7 \end{pmatrix} =$ rang $\begin{pmatrix} \alpha & \alpha^5 & \alpha^7 \\ \alpha^5 & \alpha^7 & 0 \end{pmatrix} = 2$. Per tant, $t = 2$. Resolem el sistema

$$\begin{pmatrix} \alpha & \alpha^5 \\ \alpha^5 & \alpha^7 \end{pmatrix} \begin{pmatrix} l_0 \\ l_1 \end{pmatrix} = \begin{pmatrix} -\alpha^7 \\ 0 \end{pmatrix} = \begin{pmatrix} \alpha^3 \\ 0 \end{pmatrix}$$

que ens dona solució $l_0 = \alpha$, $l_1 = \alpha^3$. Deduïm que el polinomi localitzador d'errors és $\lambda = x^2 + \alpha^3 x + \alpha$.

iv. Doneu la posició i el valor dels errors que cal corregir.
Solució:
Per força bruta veiem que λ s'anul·la a α^0 i a α^1, d'on deduïm que hi ha error a la primera i segona posicions. Per calcular el valor dels errors resolem el sistema

$$\begin{pmatrix} 1 & \alpha \\ 1 & \alpha^2 \end{pmatrix} \begin{pmatrix} e_0 \\ e_1 \end{pmatrix} = \begin{pmatrix} \alpha \\ \alpha^5 \end{pmatrix}$$

que ens dona solució $e_0 = \alpha^2$, $e_1 = \alpha^2$.

v. Doneu la primera paraula-codi de la codificació de la imatge (cadena de blancs, grisos i negres), després de la correcció d'errors.
Solució:
2011122201122210.

vi. Quin és el bloc d'informació que es dedueix que s'ha volgut enviar?
Solució:
01122210.

13. (a) **Definició d'un codi**

Anomenarem C a un codi primitiu, de Reed-Solomon, capaç de corregir tres esborralls, construït sobre el cos $\mathbb{F}_{3^2}$.

i. Comproveu que el polinomi $x^2 + x + 2 \in \mathbb{F}_3$ és irreductible i utilitzeu-lo per construir $\mathbb{F}_{3^2}$.
Solució:
És irreductible perquè és de grau 2 i no té arrels.

ii. Doneu l'equivalència vectorial-exponencial per a cada element de $\mathbb{F}_{3^2}$.
Solució:

pot.	pol.	vec.
0	0	00
α^0	1	10
α^1	α	01
α^2	$2\alpha+1$	12
α^3	$2\alpha+2$	22
α^4	2	20
α^5	2α	02
α^6	$\alpha+2$	21
α^7	$\alpha+1$	11

iii. Doneu el polinomi generador del codi C.
Solució:
$g(x) = (x-\alpha)(x-\alpha^2)(x-\alpha^3) = x^3+\alpha x^2+\alpha^7 x+\alpha^2$.

iv. Doneu la longitud, la dimensió i la distància mínima de C.
Solució:
- $n = 8$,
- $k = n - \text{grau}(g) = 8-3 = 5$,
- $d = 4$.

v. Doneu la matriu de control del codi C.
Solució:
$$H = \begin{pmatrix} 1 & \alpha & \alpha^2 & \alpha^3 & \alpha^4 & \alpha^5 & \alpha^6 & \alpha^7 \\ 1 & \alpha^2 & \alpha^4 & \alpha^6 & 1 & \alpha^2 & \alpha^4 & \alpha^6 \\ 1 & \alpha^3 & \alpha^6 & \alpha & \alpha^4 & \alpha^7 & \alpha^2 & \alpha^5 \end{pmatrix}.$$

(b) **Procés de codificació-descodificació**

Codificarem la imatge 0 1 0 0 0 1 2 2 1 2 0 . Tot seguit l'introduirem en un canal ternari amb soroll additiu i, després, la descodificarem.

i. Amb la tècnica de codificació sistemàtica per a codis cíclics, codifiqueu el primer bloc de l'anterior informació usant el codi C.
Solució:
Hem de codificar la informació $\alpha 0 \alpha \alpha^3 \alpha^2$, corresponent als primers $k = 5$ símbols. Agafem $i(x) = \alpha + \alpha x^2 + \alpha^3 x^3 + \alpha^2 x^4$ i considerem el residu $R(x)$ de dividir $x^3 i(x) = \alpha x^3 + \alpha x^5 + \alpha^3 x^6 + \alpha^2 x^7$ entre $g(x) = x^3+\alpha x^2+\alpha^7 x+\alpha^2$. Obtenim $R(x) = \alpha^3 x^2 + \alpha^6 x$. La paraula codificada serà, doncs, la que correspon a $x^3 i(x) - R(x) = \alpha x^3 + \alpha x^5 + \alpha^3 x^6 + \alpha^2 x^7 - \alpha^3 x^2 - \alpha^6 x = \alpha^2 x + \alpha^7 x^2 + \alpha x^3 + \alpha x^5 + \alpha^3 x^6 + \alpha^2 x^7$, que és $0\alpha^2\alpha^7\alpha 0\alpha\alpha^3\alpha^2$.

ii. Multipliqueu la paraula obtinguda per la matriu de control. Especifiqueu totes les operacions. Quin és el resultat?
Solució:
$$\begin{pmatrix} 0+\alpha^3+\alpha+\alpha^4+0+\alpha^6+\alpha+\alpha \\ 0+\alpha^4+\alpha^3+\alpha^7+0+\alpha^3+\alpha^7+1 \\ 0+\alpha^5+\alpha^5+\alpha^2+0+1+\alpha^5+\alpha^7 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}.$$

iii. El canal pel qual circularà la paraula codificada és un canal ternari en què hi ha un soroll additiu que ens donarà, en dígits, el vector d'error següent:
$e = (01000000000000000000000000000000\ldots)$.
Calculeu la paraula en símbols que trobarem a la sortida del canal.
Solució:
$\alpha\alpha^2\alpha^7\alpha 0\alpha\alpha^3\alpha^2$.

iv. Calculeu el polinomi localitzador d'errors.
Solució:
Considerem el polinomi
$$u(x) = \alpha + \alpha^2 x + \alpha^7 x^2 + \alpha x^3 + \alpha x^5 + \alpha^3 x^6 + \alpha^2 x^7.$$

Les síndromes seran

- $u(\alpha) = \alpha + \alpha^2\alpha + \alpha^7\alpha^2 + \alpha\alpha^3 + \alpha\alpha^5 + \alpha^3\alpha^6 + \alpha^2\alpha^7 = \alpha + \alpha^3 + \alpha + \alpha^4 + \alpha^6 + \alpha + \alpha = \alpha$
- $u(\alpha^2) = \alpha + \alpha^2\alpha^2 + \alpha^7\alpha^4 + \alpha\alpha^6 + \alpha\alpha^2 + \alpha^3\alpha^4 + \alpha^2\alpha^6\alpha + \alpha^4 + \alpha^3 + \alpha^7 + \alpha^3 + \alpha^7 + 1 = \alpha$
- $u(\alpha^3) = \alpha + \alpha^2\alpha^3 + \alpha^7\alpha^6 + \alpha\alpha + \alpha\alpha^7 + \alpha^3\alpha^2 + \alpha^2\alpha^5 = \alpha + \alpha^5 + \alpha^5 + \alpha^2 + 1 + \alpha^5 + \alpha^7 = \alpha$

Tenim $\text{rang}() \neq \text{rang}\begin{pmatrix} \alpha \\ \alpha \\ \alpha \end{pmatrix}$ i, en canvi, $\text{rang}\begin{pmatrix} \alpha \\ \alpha \end{pmatrix} = \text{rang}\begin{pmatrix} \alpha & \alpha \\ \alpha & \alpha \end{pmatrix} = 1$. Per tant, $t = 1$.
Resolem el sistema $\alpha l_0 = -\alpha$ i obtenim $l_0 = -1$ i, per tant, el localitzador d'errors és $\lambda = x - 1$.

v. Doneu la posició i el valor dels errors que cal corregir.
Solució:
Com que $\lambda(\alpha^0) = 0$, deduïm que l'error és a la primera posició. Resolem el sistema $1e_0 = u(\alpha)$, que ens dona $e_0 = \alpha$.

vi. Doneu la primera paraula-codi de la codificació de la imatge (cadena de blancs, grisos i negres), després de la correcció d'errors.
Solució:
0012110100012212.

vii. Quin és el bloc d'informació que es dedueix que s'ha volgut enviar?
Solució:
0100012212.

14. (a) Digueu tots els cossos primers i tots els polinomis mònics que podem utilitzar per construir el cos finit de 9 elements.
(b) Escolliu un dels polinomis de l'apartat anterior que sigui primitiu.
(c) Amb el polinomi escollit en l'apartat anterior, doneu una taula potencial-vectorial.
(d) Doneu el polinomi generador d'un codi Reed-Solomon primitiu en sentit estricte capaç de corregir un error.
(e) Quina longitud i quina dimensió té el codi?
(f) Doneu una paraula no nul·la del codi.
(g) Afegiu-li un error i doneu les síndromes de la paraula amb l'error.
(h) Apliqueu l'algoritme per determinar la posició d'error.
(i) Apliqueu l'algoritme per calcular el valor de l'error.

Solució:

(a) El cos primer ha de ser $\mathbb{Z}_3$ i els polinomis han de ser els irreductibles d'entre els següents:
- x^2,
- $x^2 + 1$,
- $x^2 + 2$,
- $x^2 + x$,
- $x^2 + x + 1$,
- $x^2 + x + 2$,
- $x^2 + 2x$,
- $x^2 + 2x + 1$,
- $x^2 + 2x + 2$.

Observem que, tenint en compte que tots són de grau 2,
- x^2 és divisible per x, per tant, és reductible.
- $x^2 + 1$ **no s'anul·la en** 0**, ni** 1**, ni** 2**, per tant, és IRREDUCTIBLE**.
- $x^2 + 2$ s'anul·la en 1, per tant, és reductible.
- $x^2 + x$ és divisible per x, per tant, és reductible.
- $x^2 + x + 1$ s'anul·la en 1, per tant, és reductible.
- $x^2 + x + 2$ **no s'anul·la en** 0**, ni** 1**, ni** 2**, per tant, és IRREDUCTIBLE**.
- $x^2 + 2x$ és divisible per x, per tant, és reductible.
- $x^2 + 2x + 1$ s'anul·la en 2, per tant, és reductible.

- $x^2 + 2x + 2$ **no s'anul·la en** 0**, ni** 1**, ni** 2**, per tant, és IRREDUCTIBLE**.

Per tant, el cos primer ha de ser $\mathbb{Z}_3$ i el polinomi ha de ser qualsevol d'aquests tres: $x^2 + 1, x^2 + x + 2, x^2 + 2x + 2$.

(b) Si considerem $\mathbb{Z}_3/(x^2 + 1)$ i anomenem α a la classe de x dins de $\mathbb{Z}_3/(x^2 + 1)$, tenim $\alpha^2 = 2$ i, per tant, $\alpha^4 = 1$, amb la qual cosa α no és un element primitiu i, per tant, $x^2 + 1$ no és un polinomi primitiu.

Si considerem $\mathbb{Z}_3/(x^2 + x + 2)$ i anomenem α a la classe de x dins de $\mathbb{Z}_3/(x^2 + x + 2)$, veiem que podem construir la taula potencial-vectorial següent:

pot.	*vect*
α^0	10
α^1	01
α^2	12
α^3	22
α^4	20
α^5	02
α^6	21
α^7	11

Per tant, α és primitiu i també ho és el polinomi $x^2 + x + 2$.

Si considerem $\mathbb{Z}_3/(x^2 + 2x + 2)$ i anomenem α a la classe de x dins de $\mathbb{Z}_3/(x^2 + 2x + 2)$, veiem que podem construir la taula potencial-vectorial següent:

pot.	*vect*
α^0	10
α^1	01
α^2	11
α^3	12
α^4	20
α^5	02
α^6	22
α^7	21

Per tant, α és primitiu i també ho és el polinomi $x^2 + 2x + 2$.

(c) Escollim una de les taules de l'apartat anterior. Per exemple la primera.

(d) Per corregir un error cal una distància mínima ≥ 3. Agafem $d = 3$. El polinomi generador serà $g(x) = (x - \alpha)(x - \alpha^2) = x^2 + (-\alpha^2 - \alpha)x + \alpha^3 = x^2 + \alpha^4 x + \alpha^3$.

(e) La longitud és $9 - 1 = 8$. La dimensió és $8 - \text{grau}(g) = 8 - 2 = 6$.

(f) Com a paraula no nul·la del codi podem agafar $(\alpha^3\alpha^4 100000)$, que correspon al polinomi g.

(g) Es pot fer de moltes maneres. Per exemple, podem posar un error a la primera posició de manera que ens quedi nul·la. En aquest cas l'error seria $(\alpha^7 0000000)$ i rebríem la paraula $u = (0\alpha^4 100000)$.

Calculem les síndromes: $u(\alpha) = \alpha^5 + \alpha^2 = \alpha^7$, $u(\alpha^2) = \alpha^6 + \alpha^4 = \alpha^7$.

(h) Busquem el nombre d'errors. Com que $0 \neq \text{rang}\begin{pmatrix} u(\alpha) \\ u(\alpha^2) \end{pmatrix}$, deduïm que el nombre d'errors no és 0. Com que $\text{rang}(u(\alpha)) = \text{rang}(u(\alpha)u(\alpha^2))$ deduïm que el nombre d'errors és 1.

Resolem el sistema $u(\alpha)l_0 = -u(\alpha^2)$, que és equivalent a $\alpha^7 l_0 = -\alpha^7 = \alpha^3$ i que té solució $l_0 = \alpha^4$. Deduïm que el polinomi localitzador d'errors és $\lambda = x + \alpha^4$.

Com que $\lambda(\alpha^0) = 0$, deduïm que la posició d'error és 0.

(i) El valor de l'error serà la solució del sistema $\alpha^0 e_0 = u(\alpha) = \alpha^7$, que és $e_0 = \alpha^7$.

15. (a) És $\mathbb{Z}_{11}$ un cos? Per què?

   (b) Comproveu que $a = 2$ és un element primitiu de $\mathbb{Z}_{11}$.

   (c) Volem construir un codi C de Reed-Solomon primitiu sobre $\mathbb{Z}_{11}$ capaç de corregir tres errors, basat en l'element primitiu $a = 2$. Quina longitud i quina dimensió hem d'agafar?

   (d) Doneu una matriu generadora de C.

   (e) Quantes files i quantes columnes té una matriu de control de C? Doneu les tres primeres files d'una matriu de control.

   (f) Codifiqueu la informació 1 2 3 4.

   (g) Rebem la paraula $u = 8\ 2\ 9\ 7\ 6\ 5\ 4\ 2\ 5\ 10$ que té síndromes $u(2) = 1$, $u(2^2) = 6$, $u(2^3) = 2$, $u(2^4) = 4$, $u(2^5) = 6$, $u(2^6) = 7$. Podeu determinar si la paraula u té errors a partir de les síndromes? Expliqueu com.

   (h) Determineu el nombre d'errors de u.

   (i) Determineu el polinomi localitzador d'errors.

   (j) Determineu les posicions d'error.

   (k) Determineu els valors dels errors.

   (l) Quina era la paraula del codi enviada abans que se li produïssin els errors?

Solució:

(a) $\mathbb{Z}_{11}$ és un cos perquè 11 és primer.

(b) En efecte, les seves potències són

2^0	1
2^1	2
2^2	4
2^3	8
2^4	5
2^5	10
2^6	9
2^7	7
2^8	3
2^9	6
2^{10}	1

(c) Per poder corregir tres errors hem d'agafar $d = 7$. Aleshores la longitud i la dimensió són

$$n = q - 1 = 10,$$

$$k = n - d + 1 = 10 - 7 + 1 = 4.$$

(d) Fent servir l'element primitiu $a = 2$,

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

(e) La matriu H té 6 files i 10 columnes. Les tres primeres files són les següents.

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

(f)

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

La informació codificada serà, doncs, 10 5 5 2 3 9 10 5 10 6.

(g) Com que les síndromes no són nul·les, deduïm que hi ha hagut error.

(h) Tenim $\operatorname{rang}() \neq \operatorname{rang}\begin{pmatrix} 1 \\ 6 \\ 2 \\ 4 \\ 6 \\ 7 \end{pmatrix}$, $\operatorname{rang}\begin{pmatrix} 1 \\ 6 \\ 2 \\ 4 \\ 6 \end{pmatrix} \neq \operatorname{rang}\begin{pmatrix} 1 & 6 \\ 6 & 2 \\ 2 & 4 \\ 4 & 6 \\ 6 & 7 \end{pmatrix}$, mentre que $\operatorname{rang}\begin{pmatrix} 1 & 6 \\ 6 & 2 \\ 2 & 4 \\ 4 & 6 \end{pmatrix} = \operatorname{rang}\begin{pmatrix} 1 & 6 & 2 \\ 6 & 2 & 4 \\ 2 & 4 & 6 \\ 4 & 6 & 7 \end{pmatrix}$.

En efecte, $\begin{pmatrix} 1 & 6 & 2 \\ 6 & 2 & 4 \\ 2 & 4 & 6 \\ 4 & 6 & 7 \end{pmatrix} \sim \begin{array}{l} f2' = f2 - 6f1 \\ f3' = f3 - 2f1 \\ f4' = f4 - 4f1 \end{array} \begin{pmatrix} 1 & 6 & 2 \\ 0 & 10 & 3 \\ 0 & 3 & 2 \\ 0 & 4 & 10 \end{pmatrix} \sim \begin{array}{l} f2' = 10f2 \\ f3' = 4f3 \\ f4' = 3f4 \end{array} \begin{pmatrix} 1 & 6 & 2 \\ 0 & 1 & 8 \\ 0 & 1 & 8 \\ 0 & 1 & 8 \end{pmatrix} \sim \begin{array}{l} f3' = f3 - f1 \\ f4' = f4' - f2 \end{array}$

$\begin{pmatrix} 1 & 6 & 2 \\ 0 & 1 & 8 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$.

Per tant, $t = 2$.

(i) Resolem el sistema

$$\begin{pmatrix} 1 & 6 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} l_0 \\ l_1 \end{pmatrix} = \begin{pmatrix} -2 \\ -8 \end{pmatrix} = \begin{pmatrix} 9 \\ 3 \end{pmatrix},$$

que té solució $l_1 = 3$, $l_0 = 9 - 6l_1 = 9 - 7 = 2$. Deduïm que el polinomi localitzador d'errors és

$$\lambda = x^2 + 3x + 2.$$

(j) Busquem les arrels de λ:

$$\begin{aligned} \lambda(2^0) &= 1 + 3 + 2 = 6 \neq 0 \\ \lambda(2) &= 4 + 6 + 2 = 1 \neq 0 \\ \lambda(2^2) &= 5 + 1 + 2 = 8 \neq 0 \\ \lambda(2^3) &= 9 + 2 + 2 = 2 \neq 0 \\ \lambda(2^4) &= 4 + 1 + 2 = 7 \neq 0 \\ \lambda(2^5) &= 1 + 8 + 2 = 0 \\ \lambda(2^6) &= 4 + 5 + 2 = 0 \end{aligned}$$

Per tant, les seves arrels són 2^5 i 2^6 i, per tant, les posicions d'error seran la cinquena i la sisena (començant l'enumeració per 0).

(k) Per calcular els valors dels errors resolem el sistema

$$\begin{pmatrix} 2^5 & 2^6 \\ 1 & 2^2 \end{pmatrix}\begin{pmatrix} e_5 \\ e_6 \end{pmatrix} = \begin{pmatrix} 10 & 9 \\ 1 & 4 \end{pmatrix}\begin{pmatrix} e_5 \\ e_6 \end{pmatrix} = \begin{pmatrix} u(2) \\ u(2^2) \end{pmatrix} = \begin{pmatrix} 1 \\ 6 \end{pmatrix}.$$

Restant deu vegades la segona fila a la primera obtenim

$$\begin{pmatrix} 0 & 2 \\ 1 & 4 \end{pmatrix}\begin{pmatrix} e_5 \\ e_6 \end{pmatrix} = \begin{pmatrix} 7 \\ 6 \end{pmatrix} \underset{\substack{f1' = 6f1 \\ f2' = f2 - 2f1}}{\sim} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} e_5 \\ e_6 \end{pmatrix} = \begin{pmatrix} 9 \\ 3 \end{pmatrix}.$$

Deduïm que $e_5 = 3$, $e_6 = 9$.

(l) La paraula corregida és $c' = u-(0\,0\,0\,0\,0\,3\,9\,0\,0\,0) = (8\,2\,9\,7\,6\,5\,4\,2\,5\,10)-(0\,0\,0\,0\,0\,3\,9\,0\,0\,0) = (8\,2\,9\,7\,6\,(5-3)\,(4-9)\,2\,5\,10) = (8\,2\,9\,7\,6\,2\,6\,2\,5\,10)$.

16. (a) Construcció d'un cos finit.
   i. Comproveu que el polinomi $x^3 + x + 1$ és irreductible i primitiu sobre $\mathbb{F}_2$.
   ii. Anomenem α a la classe de x dins de $\mathbb{F}_2/(x^3 + x + 1)$. Doneu-ne una taula exponencial-vectorial.

Solució:

És irreductible perquè té grau 3 i no té arrels. És primitiu perquè l'ordre de la classe de x, que anomenem α, és $q - 1 = 7$, com es pot desprendre de la taula:

exp.	*vect.*
α	010
α^2	001
α^3	110
α^4	011
α^5	111
α^6	101
α^7	100

(b) Definiu un codi RS primitiu sobre el cos de l'apartat anterior capaç de corregir dos errors.
   i. Quina distància mínima hem d'agafar? Doneu-ne la longitud i la dimensió.
   ii. Doneu-ne el polinomi generador.
   iii. Doneu-ne una matriu generadora G a partir del polinomi generador.
   iv. Doneu una matriu de control H que tingui com a primera fila les potències no nul·les de α.
   v. Calculeu el resultat de multiplicar la primera fila de G per la primera fila de H **indicant els càlculs**.
   vi. Calculeu $G \cdot H^T$.

Solució:

i. Hem d'agafar $d = 5$. La longitud és $n = q - 1 = 7$ i la dimensió és $k = n - d + 1 = 3$.

ii. El polinomi generador serà $(x-\alpha)(x-\alpha^2)(x-\alpha^3)(x-\alpha^4) = x^4 - (\alpha+\alpha^2+\alpha^3+\alpha^4)x^3 + (\alpha\alpha^2+\alpha\alpha^3+\alpha\alpha^4+\alpha^2\alpha^3+\alpha^2\alpha^4+\alpha^3\alpha^4)x^2 - (\alpha^2\alpha^3\alpha^4+\alpha\alpha^3\alpha^4+\alpha\alpha^2\alpha^4+\alpha\alpha^2\alpha^3)x + \alpha\alpha^2\alpha^3\alpha^4 = x^4 + \alpha^3x^3 + x^2 + \alpha x + \alpha^3$.

iii.
$$G = \begin{pmatrix} \alpha^3 & \alpha & 1 & \alpha^3 & 1 & 0 & 0 \\ 0 & \alpha^3 & \alpha & 1 & \alpha^3 & 1 & 0 \\ 0 & 0 & \alpha^3 & \alpha & 1 & \alpha^3 & 1 \end{pmatrix}.$$

iv.
$$H = \begin{pmatrix} 1 & \alpha & \alpha^2 & \alpha^3 & \alpha^4 & \alpha^5 & \alpha^6 \\ 1 & \alpha^2 & \alpha^4 & \alpha^6 & \alpha & \alpha^3 & \alpha^5 \\ 1 & \alpha^3 & \alpha^6 & \alpha^2 & \alpha^5 & \alpha & \alpha^4 \\ 1 & \alpha^4 & \alpha & \alpha^5 & \alpha^2 & \alpha^6 & \alpha^3 \end{pmatrix}.$$

v. $\alpha^3 + \alpha^2 + \alpha^2 + \alpha^6 + \alpha^4 = 0$.

vi.
$$G \cdot H^T = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}.$$

(c) Considerem el mateix codi RS que en el problema anterior.

i. Codifiqueu de manera sistemàtica utilitzant el polinomi generador el primer bloc d'informació de la cadena de bits
11111000111111000111111111111110001010101010101010101010100011111000...
Doneu el resultat també com a cadena de bits.

ii. Calculeu alguna síndrome de la paraula codificada indicant tots els càlculs intermedis.

Solució:

i. • Separem la informació en blocs de tres bits:

$$(111)(110)(001)(111)(100)(011)(111)(111)(111)(110)(001)(010)(101)(010)\ldots$$

• N'agafem els primers k blocs:

$$(111)(110)(001)$$

• Els passem a símbols:

$$\alpha^5\alpha^3\alpha^2$$

• Obtenim el polinomi d'informació:

$$i(x) = \alpha^5 + \alpha^3 x + \alpha^2 x^2$$

• El passem cap a la "part alta":

$$x^{n-k} i(x) = x^4(\alpha^5 + \alpha^3 x + \alpha^2 x^2) = \alpha^5 x^4 + \alpha^3 x^5 + \alpha^2 x^6$$

• Calculem la redundància:

$$\begin{array}{rl}
\alpha^2 x^6 + \alpha^3 x^5 + \alpha^5 x^4 & \big|\ x^4 + \alpha^3 x^3 + x^2 + \alpha x + \alpha^3 \\
-(\alpha^2 x^6 + \alpha^5 x^5 + \alpha^2 x^4 + \alpha^3 x^3 + \alpha^5 x^2) & \ \ \alpha^2 x^2 + \alpha^2 x + \alpha^2 \\
\hline
\alpha^2 x^5 + \alpha^3 x^4 + \alpha^3 x^3 + \alpha^5 x^2 & \\
-(\alpha^2 x^5 + \alpha^5 x^4 + \alpha^2 x^3 + \alpha^3 x^2 + \alpha^5 x) & \\
\hline
\alpha^2 x^4 + \alpha^5 x^3 + \alpha^2 x^2 + \alpha^5 x & \\
-(\alpha^2 x^4 + \alpha^5 x^3 + \alpha^2 x^2 + \alpha^3 x + \alpha^5) & \\
\hline
\alpha^2 x + \alpha^5 &
\end{array}$$

Per tant, $R(x) = \alpha^2 x + \alpha^5$.

• Calculem el polinomi $c(x) = x^{n-k} i(x) - R(x) = \alpha^5 + \alpha^2 x + \alpha^5 x^4 + \alpha^3 x^5 + \alpha^2 x^6$.

• La paraula codificada en símbols serà:

$$c = (\alpha^5\alpha^2 00\alpha^5\alpha^3\alpha^2)$$

• La paraula codificada en bits serà:

$$c = (111\ 001\ 000\ 000\ 111\ 110\ 001)$$

ii. Calculem $c(\alpha)$ o, equivalentment, calculem el producte de c per la primera fila de H:
$c(\alpha) = \alpha^5 \cdot 1 + \alpha^2 \cdot \alpha + 0 \cdot \alpha^2 + 0 \cdot \alpha^3 + \alpha^5 \cdot \alpha^4 + \alpha^3 \cdot \alpha^5 + \alpha^2 \cdot \alpha^6 = \alpha^5 + \alpha^3 + \alpha^2 + \alpha + \alpha = 0$

(d) Considerem el mateix codi RS que en els problemes anteriors.

i. Rebem la cadena de bits 001100000000000010100. A quina cadena de símbols correspon?

ii. Calculeu totes les síndromes de la paraula rebuda.

iii. Quants errors té de símbol la paraula rebuda?

iv. Quin és el polinomi localitzador d'errors?

v. Trobeu les posicions dels errors.

vi. Calculeu el valor dels errors.

vii. Doneu la cadena de bits corregida.

viii. Quants errors de bit tenia la paraula enviada?

Solució:

i. $u = \alpha^2 1000\alpha 1$.

ii. El polinomi corresponent a u és $u(x) = x^6 + \alpha x^5 + x + \alpha^2$. Calculem les 4 síndromes:

$$\begin{array}{rcl} u(\alpha) & = & \alpha^6 + \alpha^6 + \alpha + \alpha^2 = \alpha^4 \\ u(\alpha^2) & = & \alpha^5 + \alpha^4 + \alpha^2 + \alpha^2 = 1 \\ u(\alpha^3) & = & \alpha^4 + \alpha^2 + \alpha^3 + \alpha^2 = \alpha^6 \\ u(\alpha^4) & = & \alpha^3 + 1 + \alpha^4 + \alpha^2 = 0 \end{array}$$

iii. Anomenem t al nombre d'errors. Tenim $\operatorname{rang}() \neq \operatorname{rang}\begin{pmatrix} \alpha^4 \\ 1 \\ \alpha^6 \\ 0 \end{pmatrix}$, per tant, $t > 0$. I tenim $\operatorname{rang}\begin{pmatrix} \alpha^4 \\ 1 \\ \alpha^6 \end{pmatrix} \neq \operatorname{rang}\begin{pmatrix} \alpha^4 & 1 \\ 1 & \alpha^6 \\ \alpha^6 & 0 \end{pmatrix}$, per tant, $t > 1$. Com que $\operatorname{rang}\begin{pmatrix} \alpha^4 & 1 \\ 1 & \alpha^6 \end{pmatrix} = \operatorname{rang}\begin{pmatrix} \alpha^4 & 1 & \alpha^6 \\ 1 & \alpha^6 & 0 \end{pmatrix} = 2$, deduïm que $t = 2$.

iv. Resolem el sistema $\begin{pmatrix} \alpha^4 & 1 \\ 1 & \alpha^6 \end{pmatrix}\begin{pmatrix} l_0 \\ l_1 \end{pmatrix} = \begin{pmatrix} \alpha^6 \\ 0 \end{pmatrix}$. De la segona fila tenim que $l_0 = \alpha^6 l_1$, i substituint a la primera equació tenim $\alpha^4\alpha^6 l_1 + l_1 = \alpha^6$, és a dir, $(\alpha^3 + 1)l_1 = \alpha^6$. Deduïm que $l_1 = \frac{\alpha^6}{\alpha^3+1} = \frac{\alpha^6}{\alpha} = \alpha^5$ i que $l_0 = \alpha^6\alpha^5 = \alpha^4$.
El polinomi localitzador d'errors serà $\lambda(x) = x^2 + l_1 x + l_0 = x^2 + \alpha^5 x + \alpha^4$.

v. Observem que $\lambda(\alpha^0) = 1 + \alpha^5 + \alpha^4 = 0$ i que $\lambda(\alpha^4) = \alpha + \alpha^2 + \alpha^4 = 0$. Per tant, les seves arrels són α^0 i α^4.
Tindrem error a les posicions indexades amb 0 i 4, és a dir, a la primera i a la cinquena posició.

vi. Per calcular els valors dels errors hem de resoldre el sistema

$$\begin{pmatrix} \alpha^0 & \alpha^4 \\ (\alpha^0)^2 & (\alpha^4)^2 \end{pmatrix}\begin{pmatrix} e_0 \\ e_4 \end{pmatrix} = \begin{pmatrix} u(\alpha) \\ u(\alpha^2) \end{pmatrix},$$

és a dir,

$$\begin{pmatrix} 1 & \alpha^4 \\ 1 & \alpha \end{pmatrix}\begin{pmatrix} e_0 \\ e_4 \end{pmatrix} = \begin{pmatrix} \alpha^4 \\ 1 \end{pmatrix}.$$

La solució del sistema és $e_0 = \alpha^5$ i $e_4 = \alpha^3$, que són els valors dels errors demanats.

vii. La paraula d'errors serà $e = (\alpha^5 000\alpha^3 00)$ i, per tant, la paraula corregida serà $u - e = (\alpha^2 1000\alpha 1) - (\alpha^5 000\alpha^3 00) = (\alpha^3 100\alpha^3\alpha 1)$ corresponent a la cadena de bits

$$110100000000110010100.$$

viii. La paraula enviada tenia 5 errors de bit:

001100000000**00**0010100,

110100000000**11**0010100.

17. Definiu un codi RS primitiu sobre $\mathbb{F}_2/(x^3 + x + 1)$ capaç de corregir dos errors. En aquest context, rebem les paraules en bits

011001100001110110100,

110001000100111010000.

(a) Quina distància mínima hem d'agafar per al codi RS? Doneu-ne la longitud i la dimensió.

(b) A quina cadena de símbols correspon la primera paraula?

(c) A quina cadena de símbols correspon la segona paraula?

(d) Calculeu totes les síndromes de la primera paraula rebuda i doneu tots els detalls del càlcul.

(e) Calculeu totes les síndromes de la segona paraula rebuda i doneu tots els detalls del càlcul.

(f) Quants errors té de símbol la primera paraula rebuda?

(g) Quants errors té de símbol la segona paraula rebuda?

(h) Si alguna o algunes de les paraules té algun error, quin és el polinomi localitzador d'errors?

(i) Si alguna de les paraules té algun error, troba les posicions dels errors.

(j) Calculeu el valor dels errors.

(k) Si alguna o algunes de les paraules té algun error, doneu la cadena de bits corregida.

(l) Quants errors de bit tenia la primera paraula enviada?

(m) Quants errors de bit tenia la segona paraula enviada?

Solució:

(a) Hem d'agafar $d = 5$. La longitud és $n = q - 1 = 7$ i la dimensió és $k = n - d + 1 = 3$.

(b) $v = \alpha^4\alpha^2 1\alpha^2\alpha^3\alpha^3 1$.

(c) $u = \alpha^3\alpha^2 01\alpha^5\alpha 0$.

(d) En el primer cas el polinomi corresponent a v és $v(x) = x^6 + \alpha^3x^5 + \alpha^3x^4 + \alpha^2x^3 + x^2 + \alpha^2x + \alpha^4$. Calculem les 4 síndromes:

$$\begin{aligned}
v(\alpha) &= \alpha^6 + \alpha + 1 + \alpha^5 + \alpha^2 + \alpha^3 + \alpha^4 = 0\\
v(\alpha^2) &= \alpha^5 + \alpha^6 + \alpha^4 + \alpha + \alpha^4 + \alpha^4 + \alpha^4 = 0\\
v(\alpha^3) &= \alpha^4 + \alpha^4 + \alpha + \alpha^4 + \alpha^6 + \alpha^5 + \alpha^4 = 0\\
v(\alpha^4) &= \alpha^3 + \alpha^2 + \alpha^5 + 1 + \alpha + \alpha^6 + \alpha^4 = 0
\end{aligned}$$

(e) En el segon cas el polinomi corresponent a u és $u(x) = \alpha x^5 + \alpha^5x^4 + x^3 + \alpha^2x + \alpha^3$. Calculem les 4 síndromes:

$$\begin{aligned}
u(\alpha) &= \alpha^6 + \alpha^2 + \alpha^3 + \alpha^3 + \alpha^3 = \alpha\\
u(\alpha^2) &= \alpha^4 + \alpha^6 + \alpha^6 + \alpha^4 + \alpha^3 = \alpha^3\\
u(\alpha^3) &= \alpha^2 + \alpha^3 + \alpha^2 + \alpha^5 + \alpha^3 = \alpha^5\\
u(\alpha^4) &= 1 + 1 + \alpha^5 + \alpha^6 + \alpha^3 = 1
\end{aligned}$$

(f) La primera paraula no té cap error perquè totes les síndromes són zero.

(g) Anomenem t al nombre d'errors de símbol de la segona paraula. Tenim $\text{rang}() \neq \text{rang}\begin{pmatrix}\alpha\\ \alpha^3\\ \alpha^5\\ 1\end{pmatrix}$, per tant, $t > 0$. Ara tenim $\text{rang}\begin{pmatrix}\alpha\\ \alpha^3\\ \alpha^5\end{pmatrix} = \text{rang}\begin{pmatrix}\alpha & \alpha^3\\ \alpha^3 & \alpha^5\\ \alpha^5 & 1\end{pmatrix} = 1$, per tant, $t = 1$.

(h) Busquem el polinomi localitzador d'errors de la segona paraula. Resolem el sistema $\alpha l_0 = -\alpha^3 = \alpha^3$. La solució és $l_0 = \alpha^2$ i, per tant, el polinomi localitzador d'errors és $\lambda(x) = x + \alpha^2$.

(i) L'única arrel de $\lambda(x)$ és α^2. Això significa que hi ha un error a la posició indexada amb 2, és a dir, a la tercera posició.

(j) Per calcular el valor de l'error hem de resoldre el sistema $\alpha^2 e_2 = u(\alpha) = \alpha$. La solució del sistema és $e_2 = \frac{\alpha}{\alpha^2} = \frac{\alpha^8}{\alpha^2} = \alpha^6$, que és el valor de l'únic error.

(k) La paraula corregida serà $u = (\alpha^3\alpha^2 01\alpha^5\alpha 0) - (00\alpha^6 0000) = (\alpha^3\alpha^2\alpha^6 1\alpha^5\alpha 0)$ que correspon a la cadena de bits

$$110001101100111010000.$$

(l) La primera paraula enviada tenia 0 errors de bit.

(m) La segona paraula enviada tenia 2 errors de bit:

110001**000**100111010000.

110001**101**100111010000.

El present llibre és una introducció a les matemàtiques de les comunicacions digitals i a la teoria de la codificació per al tractament d'errors. Hi ha un primer bloc amb el contingut dels diferents temes acompanyats d'exemples i exercicis il·lustratius (aritmètica entera, aritmètica modular, aritmètica polinomial, cossos finits, codis lineals, codis cíclics i codis Reed-Solomon) i un segon bloc amb una extensa llista de problemes separats per temes.

Finançat pels fons de la Unió Europea NextGeneration EU, a través d'INCIBE

Financiado por la Unión Europea NextGenerationEU

GOBIERNO DE ESPAÑA
MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA
SECRETARÍA DE ESTADO DE DIGITALIZACIÓN E INTELIGENCIA ARTIFICIAL

Plan de Recuperación, Transformación y Resiliencia

incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD

Universitat Rovira i Virgili