

34

Eina-e

Aritmètica entera, cossos finits i codis correctors d'errors

Maria Bras-Amorós
Oriol Farràs Ventura



[publicacions]

u r v

Aritmètica entera, cossos finits i codis correctors d'errors

Maria Bras-Amorós
Oriol Farràs Ventura



Tarragona, 2026

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: octubre de 2026

ISBN (PDF): 978-84-1365-136-1

Aquest llibre és un resultat del Projecte Estratègic "HERMES: Ciberseguretat en computació descentralitzada" 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.



Cita el libro.



Consulta el libro en nuestra web.



Libro bajo una licencia Creative Commons BY-NC-SA.

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.

Introducció

Aquest llibre s'ha elaborat com a material docent per a l'assignatura Computació Algebraica del Grau en Enginyeria Matemàtica i Física de la Universitat Rovira i Virgili. El seu objectiu és proporcionar a l'estudiant una base sòlida dels conceptes algebraics fonamentals necessaris per a l'estudi posterior d'altres estructures algebraiques i per a l'estudi de les matemàtiques aplicades a la computació i a les comunicacions digitals.

El recorregut del llibre s'inicia amb una introducció a l'aritmètica, que es completa amb l'estudi de l'aritmètica modular i dels cossos finits. A partir d'aquests fonaments, el text aprofundeix en les matemàtiques de les comunicacions digitals i en la teoria de la codificació per al tractament d'errors, presentant de manera progressiva els resultats fonamentals relatius als codis lineals. La presentació teòrica va acompanyada de nombrosos exercicis, que inclouen tant problemes bàsics com problemes de nivell avançat, amb l'objectiu de facilitar la comprensió dels conceptes i fomentar un aprenentatge actiu. Una part del contingut d'aquest llibre és comuna amb el del volum Matemàtica Discreta II (Edicions URV, 2025), que constitueix el material de suport de l'assignatura Matemàtica Discreta II del Grau en Enginyeria Informàtica de la mateixa universitat. No obstant això, el present text introdueix diverses diferències rellevants: amplia els continguts dedicats als cossos finits, redueix el nombre de problemes bàsics, incorpora una secció específica de problemes d'aprofundiment, i intercala mostres de codi SAGE amb finalitats il·lustratives, que permeten practicar i experimentar amb diversos exemples computacionals.

Índex

1 Teoria i problemes il·lustratius	9
Unes matemàtiques per a les comunicacions digitals	14
1 Introducció a l'aritmètica	15
2 Aritmètica modular	29
3 Aritmètica polinomial i cossos finits	56
4 Caracterització, existència i unicitat dels cossos finits	90
5 Codis lineals	107
6 Codis cíclics	135
7 Matrius de Vandermonde i codis Reed-Solomon	161
2 Problemes bàsics	187
1 Aritmètica modular i polinomial, cossos finits	189
2 Codis lineals i cíclics	195
3 Matrius de Vandermonde i codis algebraics	204
3 Problemes d'aprofundiment	211
1 Aritmètica entera	213
2 Aritmètica modular	215
3 Aritmètica polinomial i cossos finits	218
4 Caracterització, existència i unicitat dels cossos finits	221
5 Codis lineals	222
6 Codis cíclics	225
7 Codis algebraics	227

TEMA 1

Teoria i problemes il·lustratius

TEMA 1

Teoria i problemes il·lustratius

Índex

Unes matemàtiques per a les comunicacions digitals	14
1 Introducció a l'aritmètica	15
1.1 Divisió d'enters	15
Dividend, divisor, quocient i residu	15
Divisors	15
Criteris de divisibilitat	17
1.2 Màxim comú divisor	18
Màxim comú divisor	18
Algoritme d'Euclides	19
Identitat de Bézout	21
1.3 Nombres primers i teorema fonamental de l'aritmètica	24
Nombres primers	24
Teorema fonamental de l'aritmètica	24
Infinitud dels nombres primers	24
1.4 Solucions	25
1.5 Notes històriques	28
2 Aritmètica modular	29
2.1 Congruències	29
Relació de congruència	29
Operacions amb congruències	31
Resolució de congruències lineals	32
2.2 Aritmètica modular	37
Anells $\mathbb{Z}_m$	37
Aritmètica modular	38
Taules d'operacions	39
Invertibles i divisors de zero	40
Funció d'Euler	41
Teorema de Fermat i teorema d'Euler	42
Ordre i elements primitius	43

	Exponenciació	45
2.3	Exercicis	46
2.4	Solucions	47
2.5	Apèndix 1: Demostració del teorema d'Euler	53
2.6	Apèndix 2: Repàs d'operacions i estructures algebraiques	54
2.7	Notes històriques	55
3	Aritmètica polinomial i cossos finits	56
3.1	Aritmètica polinomial	56
	Polinomis a $\mathbb{Z}_m$	56
	Divisió de polinomis	57
	Algoritme d'Euclides i identitat de Bézout	58
	Arrels de polinomis	60
	Polinomis irreductibles	62
	Factorització de polinomis	63
3.2	Congruències de polinomis i anells quocient $\mathbb{Z}_p/f(\mathbf{x})$	65
	Congruències de polinomis	65
	Anells quocient $\mathbb{Z}_p/f(\mathbf{x})$	65
	Aritmètica dels anells quocient $\mathbb{Z}_p/f(\mathbf{x})$	66
3.3	Cossos finits	67
	Elements invertibles	67
	Construcció de cossos finits	68
	Ordre i elements primitius	69
	Representació d'elements	70
	Resum	71
3.4	Exercicis	73
3.5	Solucions	76
4	Caracterització, existència i unicitat dels cossos finits	90
4.1	Algunes generalitats de cossos	90
	Cossos i isomorfismes de cossos	90
	Extensions de cossos	93
	Polinomis sobre un cos	94
4.2	Característica i cardinal d'un cos finit	94
	Característica d'un cos finit i cos primer	94
	Cardinal d'un cos finit	96
4.3	Ordre multiplicatiu i teorema de l'element primitiu	96
	Ordre multiplicatiu	96

	Teorema de l'element primitiu	97
4.4	Polinomi mínim i caracterització dels cossos finits	98
	Polinomi mínim	98
	Caracterització dels cossos finits	100
4.5	Existència d'un cos finit de p^m elements	100
	Existència d'un cos amb les arrels de $x^{p^m} - x$	100
	Existència d'un cos finit de p^m elements	102
4.6	Unicitat del cos finit de p^m elements	102
	Factorització del polinomi $x^{p^m} - x$	102
	Unicitat del cos finit de p^m elements	103
4.7	Solucions	105
5	Codis lineals	107
5.1	Motivació	107
	Model de comunicació	107
5.2	Codis lineals	109
	Definició	109
	Matriu generadora i codificació	110
	Codificació en símbols i en dígitos	113
	Codi dual i matriu de control	114
5.3	Detecció i correcció d'errors	116
	Distància de Hamming i pes	116
	Distància mínima i capacitat correctora	117
	Detecció d'errors	118
	Correcció d'esborralls	120
	Correcció d'errors	121
	Procés de codificació-descodificació	124
5.4	Solucions	124
5.5	Apèndix: Repàs d'àlgebra lineal i matrius	131
	Repàs d'espais vectorials	131
	Repàs de matrius	133
6	Codis cíclics	135
6.1	Matrius de Vandermonde I	135
	Definició	135
	Determinants	135
6.2	Codis cíclics	137
	Definició	137

	Polinomi generador	138
	Matrius generadores	140
	Codis cíclics primitius	142
	Polinomi de control	143
	Matrius de control	144
	Codificació sistemàtica	145
	Distància mínima prevista	146
6.3	L'exemple del faisà	147
6.4	Solucions	151
6.5	Apèndix: Repàs de determinants	159
6.6	Apèndix: Repàs de més nocions de matrius	160
7	Matrius de Vandermonde i codis Reed-Solomon	161
7.1	Matrius de Vandermonde II	161
	Matrius de Vandermonde de producte nul	161
	Avaluació polinòmica	162
7.2	Codis Reed-Solomon	163
	Matriu generadora	164
	Matriu de control	164
	Distància mínima	165
	Definició com a codi d'avaluació	166
	Definició com a codi cíclic primitiu	167
	Quatre definicions diferents per als codis RS primitius	168
	Codis RS no primitius	170
7.3	Descodificació	171
	Correcció d'esborralls	171
	Algoritme de descodificació	173
7.4	Solucions	176

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 algebraïques**.
- 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 **còs 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 algebraïques** 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

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 $0 \leq r < |b|$.

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

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**. L'enter r és el **residu**.

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 $a|b$ i $b|c$, aleshores $a|c$. [Solució \(p.25\)](#)

Exercici 4

Comproveu que si $a|b$ i existeix d tal que $d|a$ i $d|b$, aleshores $\frac{a}{d}|\frac{b}{d}$. [Solució \(p.25\)](#)

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.25)

Exercici 6

Demostreu que si $a = bq + r$ amb $0 \leq r < |b|$ i d és un divisor comú de a i b , aleshores també és un divisor de r . Solució (p.25)

(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.26)

► 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.

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

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.

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

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 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 $\text{mcd}(0, a) = a$, $\text{mcd}(1, a) = 1$, 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 $\text{mcd}(a, b) = \text{mcd}(b, r)$.

Solució (p.26)

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 $\text{mcm}(a, b)$.

Exercici 10

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

$$\text{mcm}(a, b) \cdot \text{mcd}(a, b) = ab.$$

Algorisme 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 $\text{mcd}(12, 16)$ 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, $\text{mcd}(12, 16) = 4$.

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 $\text{mcd}(5600, 1764)$.

Descomponem els enters en producte de primers.

5600	2		1764	2
2800	2		882	2
1400	2		441	3
700	2		147	3
350	2		49	7
175	5		7	7
35	5		1	
7	7			
1				

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

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

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

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

Més fàcil, no? Doncs ho repetim.

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

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

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

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

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

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

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

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

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

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

De tot aquest procediment hem deduït que

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

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 $\text{mcd}(a, b)$:

Algoritme

Input: a, b

Anomenem $r_{-2} = a$, $r_{-1} = b$.

Sigui $i = -1$.

Mentre $r_i \neq 0$,

- 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.28)

Indicacions per treballar amb sage



El quocient i el residu de la divisió de 5600 entre 1764 són, respectivament,

```
5600 // 1764
5600 % 1764
```

Podem buscar el gcd de 5600 i 1764 per divisions successives

```
rr=5600
r=1764
while r>0:
    rrr=rr
    rr=r
    r=rrr%rr
    print (r)
print("El gcd es",rr)
```

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

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

Aleshores,

- Existeix $k \geq 0$ tal que $r_{k+1} = 0$.
- Es compleix $\text{mcd}(a, b) = r_k$.
- 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**,

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

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

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 \(p.26\)](#)
- 2671 i 156 [Solució \(p.27\)](#)

Indicacions per treballar amb sage



Els coeficients de la identitat de Bézout els podríem trobar anàlogament.

```
rr=5600
r=1764
l1=1
mm=0
l=0
m=1
```

Indicacions per treballar amb sage



```
while r>0:
    rrr=rr
    lll=ll
    mmm=mm
    rr=r
    ll=l
    mm=m
    r=rrr%rr
    q=rrr//rr
    l=lll-q*ll
    m=mmm-q*mm
    print (l,m,r)
```

Per tant, la identitat de Bézout es

```
print (rr,"=",ll,"*5600","+ ",mm,"*1764")
```

Indicacions per treballar amb sage



Sage té una funció per aquest càlcul:

```
xgcd(5600,1764)
```

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 \(p.27\)](#)

Exercici 13

Sabem que donats dos enters a, b *qualssevol*, si d és el $\text{mcd}(a, b)$, 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 $d = \text{mcd}(a, b)$.

[Solució \(p.27\)](#)

Exercici 14

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

[Solució \(p.27\)](#)

1.3 Nombres primers i teorema fonamental de l'aritmètica

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 $\text{mcd}(a, b) = 1$, 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 $p \mid a_1 \cdot a_2 \cdot \dots \cdot a_t$, aleshores existeix algun i entre 1 i t tal que $p \mid a_i$.

Solució (p.27)

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.

Infinitud dels nombres primers

Teorema 4

Hi ha infinits nombres primers. Nota (p.28)

Demostració. Procedim per reducció a l'absurd.

Suposem que $p_1 < \dots < p_n$ són tots els primers.

Aleshores $p_1 \dots p_n + 1$ 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. □

Indicacions per treballar amb sage



Sage té una booleà per determinar si un enter és primer:

```
print("is_prime(72)=", is_prime(72))
print("is_prime(17)=", is_prime(17))
```

i una funció per factoritzar en primers:

```
print("factor(72)=", factor(72))
print("factor(17)=", factor(17))
```

Amb el constructor de llistes `[expressio(x) for x in domini(x) if condicional(x)]` podem escriure els primers primers

```
print([i for i in [1..100] if is_prime(i)])
```

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.16)

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.16)

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.17)

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.17)

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.17)

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 $b = db'$ i $r = dr'$. Per tant, $a = bq + r = db'q + dr' = d(b'q + r')$.

Torna a l'exercici (p.18)

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

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

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

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.22)

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.22)

Solució de l'Exercici 12

Suposem que existeixen dos enters λ i μ tals que

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

Si $\text{mcd}(a, b) \neq 1$, 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.23)

Solució de l'Exercici 13

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

Torna a l'exercici (p.23)

Solució de l'Exercici 14

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

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

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

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

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

Torna a l'exercici (p.23)

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 $\text{mcd}(a, p) = 1$ i, pel punt anterior, deduïm que $p \mid b$.
3. Es pot demostrar per inducció sobre t utilitzant els passos anteriors.

Torna a l'exercici (p.24)

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.20)

- 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.24)

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

$$a = r \pmod{m}.$$

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 **$a \equiv b \pmod{m}$** o bé **$a \equiv b(m)$** .

En el cas anterior, diríem

$$52 \equiv 73(7) \text{ o } 52 \equiv 73 \pmod{7}$$

i

$$149 \equiv 100(7) \text{ o } 149 \equiv 100 \pmod{7}$$

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 $a \equiv b \pmod{m}$ i d divideix m , aleshores $a \equiv b \pmod{d}$. [Solució \(p.47\)](#)

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

$$8726 \equiv 26 \pmod{100}$$

Aleshores també tindrem

$$98726 \equiv 26 \pmod{50}, \quad 98726 \equiv 26 \pmod{10}, \dots$$

El contrari no és cert. Per exemple,

$$1 \equiv 51 \pmod{50}$$

però, en canvi,

$$1 \not\equiv 51 \pmod{100}$$

Lema 2

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

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

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

Operacions amb congruències

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

Si $a_1 \equiv a_2 \pmod{m}$ i $b_1 \equiv b_2 \pmod{m}$, aleshores

$$a_1 + b_1 \equiv a_2 + b_2 \pmod{m},$$

$$a_1 \cdot b_1 \equiv a_2 \cdot b_2 \pmod{m}.$$

Per exemple, tenim que

$$5 \equiv 12 \pmod{7}$$

$$11 \equiv -3 \pmod{7}$$

El que ens diu el lema és que, aleshores,

$$5 + 11 \equiv 12 - 3 \pmod{7}$$

$$5 \cdot 11 \equiv 12 \cdot (-3) \pmod{7}$$

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

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

puc reduir primer els operands:

$$754 \equiv 1 \pmod{3}$$

$$389 \equiv 2 \pmod{3},$$

i les operacions em queden reduïdes a

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

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

Però el recíproc no és cert.

La simplificació no queda ben definida.

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

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

Lema 4

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

$$ka \equiv kb \pmod{m} \iff a \equiv b \pmod{m}.$$

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

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

□

Lema 5

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

$$ka \equiv kb \pmod{m} \iff k'a \equiv k'b \pmod{m'}.$$

Demostració.

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

□

Resolució de congruències lineals

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

$$ax \equiv b \pmod{m}.$$

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 $\text{mcd}(a, m)$ divideix b .

Vegem si tenen solució les congruències anteriors:

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

► **Podem simplificar?**

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

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

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

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

Un cop tenim el paràmetre μ tal que

$$\mu a' \equiv 1 \pmod{m'},$$

deduïm que

$$(b'\mu)a' \equiv b' \pmod{m'}$$

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 resollem 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,

$$7 \cdot 7 \equiv 1 \pmod{12}.$$

Multiplicant-ho tot per 4, es complirà

$$7(7 \cdot 4) \equiv 1 \cdot 4 \pmod{12}$$

$$7 \cdot 28 \equiv 4 \pmod{12}$$

$$7 \cdot 4 \equiv 4 \pmod{12}.$$

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,

$$47 \cdot 23 \equiv 1 \pmod{60}.$$

Multiplicant-ho tot per 17, es complirà

$$47(23 \cdot 17) \equiv 1 \cdot 17 \pmod{60}$$

$$47 \cdot 391 \equiv 17 \pmod{60}$$

$$47 \cdot 31 \equiv 17 \pmod{60}.$$

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,

$$13 \cdot 17 \equiv 1 \pmod{20}.$$

Multiplicant-ho tot per 6, es complirà

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

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 resollem 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,

$$2 \cdot 8 \equiv 1 \pmod{15}.$$

Multiplicant-ho tot per 2, es complirà

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

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

$$a'(x_0 + m') \equiv b'(m'),$$

$$a'(x_0 + 2m') \equiv b'(m'),$$

$$a'(x_0 + 3m') \equiv b'(m'),$$

$\vdots$

Totes les solucions mòdul m seran

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

En total n'hi haurà

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

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 $5 = \text{mcd}(35, 60)$.
2. $32x \equiv 58(60)$ no té solució.
3. $47x \equiv 17(60)$ només té una solució, ja que $\text{mcd}(47, 60) = 1$. 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 $3 = \text{mcd}(39, 60)$.
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 $4 = \text{mcd}(8, 60)$.

Sumari

Lema 6

Considerem la congruència $ax \equiv b \pmod{m}$.

1. Té solució si i només si $\text{mcd}(a, m) \mid b$.

2. L'enter x és solució de $ax \equiv b \pmod{m}$ si i només si ho és de

$$\frac{a}{\text{mcd}(a, m)}x \equiv \frac{b}{\text{mcd}(a, m)} \pmod{\frac{m}{\text{mcd}(a, m)}}.$$

3. Si existeix una solució x_0 , aleshores n'existeixen $\text{mcd}(a, m)$ i el conjunt de solucions és donat per

$$x \equiv x_0 + k \frac{m}{\text{mcd}(a, m)} \pmod{m},$$

amb $k = 0, 1, \dots, \text{mcd}(a, m) - 1$.

Procediment per resoldre $ax \equiv b \pmod{m}$

- Si $\text{mcd}(a, m) \nmid b$, aleshores no hi ha solució.
- Si $\text{mcd}(a, m) \mid b$
 - Si $\text{mcd}(a, m) = 1$
 - * Calculem els coeficients λ i μ de la identitat de Bézout

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

- * La solució és única i és $x \equiv \mu b \pmod{m}$.

- Si $\text{mcd}(a, m) \neq 1$

- * Busquem la solució x_0 de la congruència

$$\frac{a}{\text{mcd}(a, m)}x \equiv \frac{b}{\text{mcd}(a, m)} \pmod{\frac{m}{\text{mcd}(a, m)}}$$

que compleix $\text{mcd}\left(\frac{a}{\text{mcd}(a, m)}, \frac{m}{\text{mcd}(a, m)}\right) = 1$.

- * El conjunt de solucions serà

$$x \equiv x_0 + k \frac{m}{\text{mcd}(a, m)} \pmod{m},$$

amb $k = 0, \dots, \text{mcd}(a, m) - 1$.

Indicacions per treballar amb sage



Podem resoldre congruències amb la funció `solve_mod`

```
print("solve_mod(35*x==20,60)=",solve_mod(35*x==20,60))
print("solve_mod(32*x==58,60)=",solve_mod(32*x==58,60))
print("solve_mod(47*x==17,60)=",solve_mod(47*x==17,60))
print("solve_mod(39*x==18,60)=",solve_mod(39*x==18,60))
print("solve_mod(51*x==26,60)=",solve_mod(51*x==26,60))
print("solve_mod(8*x==8,60)=",solve_mod(8*x==8,60))
```

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,

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

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:

$$\begin{array}{ccccccccccc} & & & & & & & & & & [0]_3 & [1]_3 & [2]_3 \\ & & & & & & & & & & \vdots & \vdots & \vdots \\ & & & & & & & & & & -3 & -2 & -1 \\ \dots & -2 & -1 & 0 & 1 & 2 & 3 & 4 & \dots & \rightarrow & 0 & 1 & 2 \\ & & & & & & & & & & 3 & 4 & 5 \\ & & & & & & & & & & \vdots & \vdots & \vdots \end{array}$$

Per tant,

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

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 p:assoc] associativa i p:commut] commutativa perquè ho és a $\mathbb{Z}$.
- El p:neutre] neutre per a la suma és $[0]_m$ i l'p:invers] 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 p:assoc] associativa i p:commut] commutativa perquè ho és a $\mathbb{Z}$ i satisfà la propietat p:distib] distributiva amb la suma.
- El p:neutre] neutre pel producte és $[1]_m$.

Per tot l'anterior, podem afirmar el següent:

$(\mathbb{Z}_m, +, \cdot)$ és un def:anell] 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 def:cos] 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 $[2]_4 \cdot [a]_4 = [1]_4$.

Indicacions per treballar amb sage



Podem definir $\mathbb{Z}_m$ amb la funció `Integers(m)`

```
print("Integers(27)=", Integers(27))
```

```
Z27=Integers(27)
```

```
print("Z27(50)=", Z27(50))
```

```
print("Z27(20+23)=", Z27(20+23))
```

```
print("Z27(20)+Z27(23)=", Z27(20)+Z27(23))
```

```
print("Z27(30*2)=", Z27(30*2))
```

```
print("Z27(30)*Z27(2)=", Z27(30)*Z27(2))
```

Indicacions per treballar amb sage



Aprofitem per veure la diferència entre conjunt i llista. La podeu veure amb les següents comandes?

```
Z27=Integers(27)
print("[Z27(a) for a in [1..100]]=",
      [Z27(a) for a in [1..100]])
print("{Z27(a) for a in [1..100]}=",
      {Z27(a) for a in [1..100]})
```

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 $(a_1 + a_2 + \dots + a_n)^2 = a_1^2 + a_2^2 + \dots + a_n^2$, per tot n .

Solució (p.47)

Exercici 19

Comproveu que a $\mathbb{Z}_p$, amb p primer, es compleix que

$$(a_1 + a_2 + \dots + a_n)^p = a_1^p + a_2^p + \dots + a_n^p,$$

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

×	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

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

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, $ax = b \pmod m$ 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 $ax = 1 \pmod m$ 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 $ax = 0 \pmod m$ 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,

$$\mu a \equiv 1 \pmod m$$

Deduïm, doncs, que $a^{-1} = \mu$.

Teorema 5

$\mathbb{Z}_m$ és un def:cos] 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.47)

Funció d'Euler

Ara definim una funció $\phi : \mathbb{N} \rightarrow \mathbb{N}$ que s'anomena **funció d'Euler**. Nota (p.55)

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.48)

Exercici 22Comproveu que si la descomposició d'un enter n en producte de primers és $n = p_1^{n_1} \cdots p_k^{n_k}$, aleshores

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

Solució (p.48)

Indicacions per treballar amb sage

Podem trobar els invertibles utilitzant el gcd

```
[a for a in Integers(27) if gcd(a,27) == 1]
```

Quants n'hi ha?

```
print("len([a for a in Integers(27) if gcd(a,27)==1])=",
      len([a for a in Integers(27) if gcd(a,27) == 1]))
print("euler_phi(27)=", euler_phi(27))
```

També podem trobar l'invers de cadascun dels invertibles

```
[[a,a^(-1)] for a in Integers(27) if gcd(a,27)==1]
```

O bé

```
[[a,inverse_mod(a,27)] for a in [0..26] if gcd(a,27)==1]
```

Indicacions per treballar amb sageComprovem que $\mathbb{Z}_{27}$ no és un cos

```
is_field(Integers(27))
```

Teorema de Fermat i teorema d'Euler**Teorema 6: Teorema de Fermat** Nota (p.55)Si p és primer i $\text{mcd}(a, p) = 1$, aleshores

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

Teorema 7: Teorema d'Euler

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

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

Podeu veure una demostració del teorema d'Euler a l'apèndix (p.53) 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

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

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

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

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.48)

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 $\text{ord}_m(a)$.

Lema 9

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

Demostració. Si existeix l'ordre de l'element a aleshores existeix l'invers de a , ja que és $a^{\text{ord}_m(a)-1}$. Pel lema 7 es dedueix que $\text{mcd}(a, m) = 1$. Si $\text{mcd}(a, m) = 1$, 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. $\square$

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.49)

Exercici 26

Demostreu que si $a \in \mathbb{Z}_m^*$ i a^{-1} és l'invers de a a $\mathbb{Z}_m$, aleshores $\text{ord}_m(a^{-1}) = \text{ord}_m(a)$. Solució (p.49)

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 $\text{ord}_m(a)$ té quocient q i residu r , aleshores $a^k = (a^{\text{ord}_m(a)})^q a^r$. Però com que $a^k = 1$ i $a^{\text{ord}_m(a)} = 1$, aleshores $a^r = 1$. Això, tenint en compte que $0 \leq r < \text{ord}_m(a)$, només és possible si $r = 0$, és a dir, si $\text{ord}_m(a) \mid k$. $\square$

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.49)

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.50)

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

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

Lema 11

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

Demostració. Tindrem que $(\beta^j)^k = \beta^{kj}$ és igual a 1 si i només si $\text{ord}_m(\beta) \mid kj$, 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 $\text{mcd}(j, \phi(m)) \neq 1$, aleshores $\phi(m)$ divideix $\frac{\phi(m)}{\text{mcd}(j, \phi(m))}j$ que, pel que acabem de veure, suposa que β^j no és primitiu.

Si $\text{mcd}(j, \phi(m)) = 1$, aleshores $\phi(m)$ només pot dividir kj si $\phi(m)$ divideix k , cosa que no és possible si $k \leq \phi(m) - 1$. 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 \(p.50\)](#)
2. Quants i quins són els elements primitius de $\mathbb{Z}_{18}$? [Solució \(p.50\)](#)

Indicacions per treballar amb sage



Podem calcular l'ordre d'un element amb `multiplicative_order`:

```
Z27=Integers(27)
multiplicative_order(Z27(8))
```

Mirant la llista de tots els ordres, veiem que tots divideixen $\phi(27)$:

```
[multiplicative_order(a) for a in Z27 if gcd(27,a)==1]
```

Construïm nosaltres mateixes una funció booleana per a veure si un element és primitiu:

```
def is_primitive(a,m):
    ep=euler_phi(m)
    return(multiplicative_order((Integers(m))(a))==ep)
```

Indicacions per treballar amb sage



Comprovem que a $\mathbb{Z}_{23}$ el 2 no és primitiu però el 7 sí que ho és

```
print("is_primitive(2,23)=",is_primitive(2,23))
print("is_primitive(7,23)=",is_primitive(7,23))
```

Exponenciació

Lema 12

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

Demostració.

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

□

2.3 Exercicis**Exercici 30**

- (a) Calculeu l'invers de 16 a $\mathbb{Z}_{29}$ [Solució \(p.50\)](#)
- (b) Calculeu l'invers de 258 a $\mathbb{Z}_{2791}$. [Solució \(p.51\)](#)

Exercici 31

1. Expressau tots els elements no nuls de $\mathbb{Z}_{19}$ com a potències de 2. [Solució \(p.51\)](#)
2. És possible expressar tots els elements no nuls de $\mathbb{Z}_{23}$ com a potències de 2? [Solució \(p.51\)](#)
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 \(p.51\)](#)

Exercici 32Sigui 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 \(p.52\)](#)**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 \(p.52\)](#)

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

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

Solució (p.52)

Exercici 35

Calculeu el residu de dividir

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

Solució (p.53)

Exercici 36

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

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

Solució (p.53)

Exercici 37

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

Solució (p.53)

2.4 Solucions**Solució de l'Exercici 17**

$a \equiv b \pmod{m}$ 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 $a \equiv b \pmod{d}$.

Torna a l'exercici (p.30)

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 $(a + b)^2 = a^2 + 2ab + b^2 \equiv a^2 + b^2 \equiv a + b \pmod{2}$.
- Sabem que és cert per $n = 2$. Suposem que és cert fins a $n - 1$, aleshores $(a_1 + a_2 + \dots + a_{n-1} + a_n)^2 = ((a_1 + a_2 + \dots + a_{n-1}) + a_n)^2 = (a_1 + a_2 + \dots + a_{n-1})^2 + a_n^2 = a_1^2 + a_2^2 + \dots + a_{n-1}^2 + a_n^2$.

Torna a l'exercici (p.39)

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.41)

Solució de l'Exercici 21

•

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

$$\begin{aligned}\phi(2) &= 1 \text{ (propietat 1)} \\ \phi(9) &= \phi(3^2) = 3^2 - 3^1 = 9 - 3 = 6 \text{ (propietat 3)}\end{aligned}$$

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

•

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

•

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

Torna a l'exercici (p.42)

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.42)

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 $8^{18} = 1 \pmod{27}$, 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 $32 \equiv 5 \pmod{27}$) $= 5 \cdot 5 \cdot 5 = 125 = 4 \cdot 27 + 17 = 17$.
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.43)

Solució de l'Exercici 25

Observem,

$$\begin{array}{ll}
 3^1 &= 3 \\
 3^2 &= 9 \\
 3^3 &= 3 \cdot 3^2 = 3 \cdot 9 = 27 = 18 + 9 = 9 \\
 3^4 &= 3 \cdot 3^3 = 3 \cdot 9 = 27 = 18 + 9 = 9 \\
 &\vdots
 \end{array}
 \qquad
 \begin{array}{ll}
 7^1 &= 7 \\
 7^2 &= 49 = 18 \cdot 2 + 13 = 13 \\
 7^3 &= 7 \cdot 7^2 = 7 \cdot 13 = 91 = 18 \cdot 5 + 1 = 1 \\
 &\vdots
 \end{array}$$

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.44)

Solució de l'Exercici 26

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

Torna a l'exercici (p.44)

Solució de l'Exercici 27

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

$$\begin{array}{llllll}
 1^1 = 1 & 2^1 = 2 & 3^1 = 3 & 4^1 = 4 & 5^1 = 5 & 6^1 = 6 \\
 & 2^2 = 4 & 3^2 = 2 & 4^2 = 2 & 5^2 = 4 & 6^2 = 1 \\
 & 2^3 = 1 & 3^3 = 6 & 4^3 = 1 & 5^3 = 6 & \\
 & & 3^4 = 4 & & 5^4 = 2 & \\
 & & 3^5 = 5 & & 5^5 = 3 & \\
 & & 3^6 = 1 & & 5^6 = 1 & \\
 \text{ord}_7(1) = 1 & \text{ord}_7(2) = 3 & \text{ord}_7(3) = 6 & \text{ord}_7(4) = 3 & \text{ord}_7(5) = 6 & \text{ord}_7(6) = 2
 \end{array}$$

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

Torna a l'exercici (p.44)

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:

$$\begin{array}{llll}
 1^1 = 1 & 3^1 = 3 & 5^1 = 5 & 7^1 = 7 \\
 & 3^2 = 9 = 1 & 5^2 = 25 = 1 & 7^2 = 49 = 1 \\
 \text{ord}_8(1) = 1 & \text{ord}_8(3) = 2 & \text{ord}_8(5) = 2 & \text{ord}_8(7) = 2
 \end{array}$$

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.44)

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:

$$\begin{array}{ll}
 5^1 = 5 \\
 5^2 = 25 = 7 \\
 5^3 = -1
 \end{array}$$

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 $\text{mcd}(j, \phi(18)) = 1$ 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.45)

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.46)

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.46)

Solució de l'Exercici 31(a)

1.

$2^0 = 1$	$1 = 2^0$
$2^1 = 2$	$2 = 2^1$
$2^2 = 4$	$3 = 2^{13}$
$2^3 = 8$	$4 = 2^2$
$2^4 = 16$	$5 = 2^{16}$
$2^5 = 13$	$6 = 2^{14}$
$2^6 = 7$	$7 = 2^6$
$2^7 = 14$	$8 = 2^3$
$2^8 = 9$	$9 = 2^8$
$2^9 = 18$	$10 = 2^{17}$
$2^{10} = 17$	$11 = 2^{12}$
$2^{11} = 15$	$12 = 2^{15}$
$2^{12} = 11$	$13 = 2^5$
$2^{13} = 3$	$14 = 2^7$
$2^{14} = 6$	$15 = 2^{11}$
$2^{15} = 12$	$16 = 2^4$
$2^{16} = 5$	$17 = 2^{10}$
$2^{17} = 10$	$18 = 2^9$

Solució de l'Exercici 31(b,c)

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

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

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

Torna a l'exercici (p.46)

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.46)

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.46)

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.47)

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 $\text{mcd}(2, 5) = 1$ 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.47)

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 $\text{mcd}(a, m) = 1$, 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.47)

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.47)

2.5 Apèndix 1: Demostració del teorema d'Euler

Demostració. Suposem que $\mathbb{Z}_m^* = \{u_1, \dots, u_{\phi(m)}\}$.

Anomenem $U = u_1 \cdot u_2 \cdot \dots \cdot u_{\phi(m)}$.

Observem que $U \in \mathbb{Z}_m^*$ i que el seu invers és

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

Ara considerem $a \in \mathbb{Z}_m^*$.

Observem que els elements $au_1, \dots, au_{\phi(m)}$ pertanyen tots a $\mathbb{Z}_m^*$, per tenir inversos, respectivament, $u_1^{-1}a^{-1}, \dots, u_{\phi(m)}^{-1}a^{-1}$.

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, $\mathbb{Z}_m^* = \{au_1, \dots, au_{\phi(m)}\}$.

Així doncs, U també el podem escriure com $au_1 \cdot au_2 \cdot \dots \cdot au_{\phi(m)} = a^{\phi(m)}U$, 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 $\mathbb{Z}_m$. $\square$

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

$$\begin{aligned} + : (\mathbb{N}, \mathbb{N}) &\rightarrow \mathbb{N} \\ (a, b) &\mapsto a + b \end{aligned}$$

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 $a * e_a = e_a * a = e_n$.
- **Propietat commutativa** si $a * b = b * a$ per tot $a, b \in A$.

Torna a les propietats aritmètiques de $\mathbb{Z}_m$ (p.38)

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 propietat 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.38) .

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.41)

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.41)

Teorema 6: 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.42)

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 producte 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 $\text{grau}(a(x)b(x)) \neq \text{grau}(a(x)) + \text{grau}(b(x))$.
- Proveu que si m és primer, aleshores $\text{grau}(a(x)b(x)) = \text{grau}(a(x)) + \text{grau}(b(x))$.

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 $2x^3$:

$$\begin{array}{r} 4x^7 + 3x^4 + x + 3 \\ - (4x^7 + x^3) \\ \hline 3x^4 + 4x^3 + x + 3 \end{array} \quad \begin{array}{r} 2x^4 + 3 \\ 2x^3 + \end{array}$$

i continuem pel terme 4:

$$\begin{array}{r} 4x^7 + 3x^4 + x + 3 \\ - (4x^7 + x^3) \\ \hline 3x^4 + 4x^3 + x + 3 \\ - (3x^4 + 2) \\ \hline 4x^3 + x + 1 \end{array} \quad \begin{array}{r} 2x^4 + 3 \\ 2x^3 + 4 \end{array}$$

En notació anglosaxona és

$$\begin{array}{r} 2x^4 + 3 \overline{) 4x^7 + 3x^4 + x + 3} \\ \underline{-(4x^7 + x^3)} \\ 3x^4 + 4x^3 + x + 3 \end{array}$$

i continuem pel terme 4:

$$\begin{array}{r} 2x^4 + 3 \overline{) 4x^7 + 3x^4 + x + 3} \\ \underline{-(4x^7 + x^3)} \\ 3x^4 + 4x^3 + x + 3 \\ \underline{-(3x^4 + 2)} \\ 4x^3 + x + 1 \end{array}$$

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 $b(x)$.

Indicacions per treballar amb sage



Definim l'estructura (anell) dels polinomis sobre un anell $\mathbb{Z}_m$ de la manera següent:

```
Z5=Integers(5)
P.<x>=PolynomialRing(Z5)
```

En fer aquesta definició també estem definint la indeterminada x . Aleshores podem escriure els polinomis de la manera habitual.

```
a=4*x^7+3*x^4+x+3
b=2*x^3+1
```

o en forma de llista:

```
a=P([3,1,0,0,3,0,0,4])
b=P([1,0,0,2])
```

Indicacions per treballar amb sage



Podem operar els polinomis de la manera habitual:

```
a+b
a*b
```

El quocient i el residu d'una divisió s'escriuen com hem vist pels enters

```
a // b
a % b
```

Podem avaluar-los en una constant:

```
a(3)
b(4)
```

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.

Exercici 39

Demostreu que el màxim comú divisor de dos polinomis és unívocament definit llevat del producte per constants no nul·les.

Solució (p.76)

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:

$$\begin{array}{r} x^5 \\ -(x^5 + x^4) \\ \hline 4x^4 \\ -(4x^4 + 4x^3) \\ \hline x^3 \\ -(x^3 + x^2) \\ \hline 4x^2 + x + 1 \end{array} \quad \begin{array}{l} x^3 + x^2 \\ \hline x^2 + 4x + 1 \end{array}$$

$$\begin{array}{r} x^3 + x^2 \\ -(x^3 + 4x^2 + 4x) \\ \hline 2x^2 + x \\ -(2x^2 + 3x + 3) \\ \hline 3x + 2 \end{array} \quad \begin{array}{l} 4x^2 + x + 1 \\ \hline 4x + 3 \end{array}$$

$$\begin{array}{r} 4x^2 + x + 1 \\ -(4x^2 + x) \\ \hline 1 \end{array} \quad \begin{array}{l} 3x + 2 \\ \hline 3x \end{array}$$

$$\begin{array}{r} 3x + 2 \\ -(3x) \\ \hline 2 \\ -(2) \\ \hline 0 \end{array} \quad \begin{array}{l} 1 \\ \hline 3x + 2 \end{array}$$

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 40

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.76)

Exercici 41

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.76)

Exercici 42: 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:

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

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.77)

Lema 14

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

Exercici 43

Demostreu el lema anterior.

Solució (p.77)

Indicacions per treballar amb sage

Per trobar les arrels de a podem escriure

```
[a(y) for y in Z5]
```

o, més precisament,

```
[y for y in Z5 if a(y)==0]
```

Sage té la seva pròpia funció per trobar les arrels (amb multiplicitat)

```
print("roots(a)=", a.roots())
```

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 44

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

Solució (p.78)

Exercici 45

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

Solució (p.78)

Exercici 46

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.79)

Exercici 47

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

Solució (p.79)

Exercici 48

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.79)

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 49

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

Solució (p.80)

Indicacions per treballar amb sage



Podem coprovar si un polinomi és irreductible

```
a.is_irreducible()
```

O mirar de factoritzar-lo

```
factor(a)
```

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

$$a(x) = r(x) \pmod{m(x)}.$$

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

$$4x^7 + 3x^4 + x + 3 = 4x^3 + x + 1 \pmod{2x^4 + 3}$$

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

$$a(x) \equiv b(x) \pmod{f(x)}$$

Exercici 50

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 51

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

Solució (p.80)

Deduïm el següent:

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

Exercici 52

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.80)

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.

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

Troblem, 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 $\text{mcd}(f(x), a(x)) = 1$, 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,

$$\mu(x)a(x) \equiv 1 \pmod{f(x)}.$$

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

Exercici 53

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.80)

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 54

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.81)

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 55

Utilitzeu l'Exercici 48 per donar un polinomi que generi $\mathbb{F}_{27}$. [Solució \(p.82\)](#)

Ordre i elements primitius

Teorema 10

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

Exercici 56

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 $\text{ord}_{\mathbb{F}_{p^n}}(\beta)$

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 57

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 58

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 \(p.82\)](#)

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

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

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:

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

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 $(a_0, \dots, a_{d-1})$ on a_i és el coeficient de grau i de la notació polinomial.
 És el que anomenem **notació vectorial**.

Exemple. En l'exemple anterior,

$$\alpha^{11} \text{ (notació exponencial)} = 1 + \alpha^2 + \alpha^3 \text{ (notació polinomial)} = (1, 0, 1, 1) \text{ (notació vectorial)}.$$

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

$\mathbb{Z}_m$	$\mathbb{Z}_p[x]/f(x)$ (amb p primer)
Divisió euclidian a $\mathbb{Z}$: Donats $a, b \in \mathbb{Z}$ existeixen $q, r \in \mathbb{Z}$ tals que $a = bq + r$ amb $0 \leq r < b$. Fer congruències mòdul m és quedar-nos amb el residu de dividir per m $\Rightarrow$ obtenim enters $< m$.	Divisió euclidian 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 $f(x)$ és quedar-nos amb el residu de dividir per $f(x)$ $\Rightarrow$ obtenim polinomis de grau $< \text{grau}(f(x))$.
$\mathbb{Z}_m = \{0, 1, \dots, m-1\}$ amb les operacions reduïdes mòdul m. $\mathbb{Z}_m$ té m elements.	$\mathbb{Z}_p[x]/f(x) = \{a_0 + a_1x + \dots + a_{n-1}x^{n-1} \text{ amb } a_0, \dots, a_{n-1} \in \mathbb{Z}_p\}$ amb les operacions reduïdes mòdul p i mòdul $f(x)$, on $n = \text{grau } f(x)$. $\mathbb{Z}_p[x]/f(x)$ 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 $\mathbb{Z}_m$. 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: $a^{\phi(m)} \equiv 1 \pmod{m}$ 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 $\mathbb{F}_p$.	$a(x) \in \mathbb{Z}_p[x]/f(x)$ 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 $\mathbb{Z}_p[x]/f(x)$.  $\mathbb{Z}_p[x]/f(x)$ 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 $a^i \equiv 1 \pmod{m}$. L'ordre sempre és un divisor de $\phi(m)$. Diem que $a \in \mathbb{Z}_m$ és primitiu si el seu ordre és $\phi(m)$. 	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 $p^n - 1$. Diem que $\beta \in \mathbb{F}_{p^n}$ és primitiu si el seu ordre és $p^n - 1$. Si β és primitiu, aleshores $\mathbb{F}_{p^n} = \{0, 1, \beta, \dots, \beta^{p^n-2}\}$. Diem que $f(x)$ és primitiu si la classe de x és un element primitiu de $\mathbb{Z}_p[x]/f(x)$.

Indicacions per treballar amb sage



Sage permet construir cossos finits amb la comanda `FiniteField`

```
F64.<alpha>=FiniteField(64)
F64
```

`alpha` serà la classe de x com a congruència mòdul el polinomi generador. Així podem escriure, per exemple,

```
alpha^100
alpha^63
```

Per veure quin polinomi ha utilitzat sage per la construcció del cos:

```
charpoly(alpha)
```

Comprovem que la potència α^6 és la que correspon pel polinomi generador:

```
alpha^6
```

Indicacions per treballar amb sage



També podem forçar nosaltres que sage utilitzi un determinat polinomi amb de la manera següent:

```
F64.<alpha>=FiniteField(64,modulus=x^6+x^5+x^2+x+1)
```

Suposem que treballem en un cos finit F de p^m elements. Podem calcular qui són la p i la m així:

```
F=FiniteField(125)
p=F.characteristic()
print(p)
```

```
m=F.degree()
print(m)
```

Indicacions per treballar amb sage



Els vectors de m coordenades a $\mathbb{Z}_p$ els podem escriure així:

```
V=VectorSpace(FiniteField(p),m)
```

Si v és un element de V , aleshores $F(v)$ és l'element de F que té forma vectorial igual a v . Observeu què passa quan executeu les comandes següents:

```
v=V.random_element()
print(v)
print(F(v))
```

Indicacions per treballar amb sage



Una manera de trobar la forma vectorial d'un element amb sage pot ser aquesta:

```
def formavect(F,beta):
    llista=[v for v in
        VectorSpace(FiniteField(F.characteristic()),F.degree())
        if F(v)==beta]
    return llista[0]
```

Fem unes comprovacions:

```
print(v,F(v),formavect(F,F(v)))
F.<a>=FiniteField(125)
print(a^101,formavect(F,a^101),F(formavect(F,a^101)))
```

3.4 Exercicis

Exercici 59

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.82)

Exercici 60

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.83)

Exercici 61

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

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

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.84)

Exercici 62

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.85)

Exercici 63

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

Solució (p.86)

Exercici 64

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 $\frac{x^3 - 1}{x^4 + \alpha^6 x^3 + x^2 + \alpha^3 x + \alpha^2}$.

Solució (p.87)

Exercici 65

- (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.88)

3.5 Solucions**Solució de l'Exercici 39**

Torna a l'exercici (p.59)

Solució de l'Exercici 40

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

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

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

Com que $325 \equiv 1 \pmod{2}$, 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.60)

Solució de l'Exercici 41

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.60)

Solució de l'Exercici 42

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

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

4.

$\sqrt{0}^{\mathbb{Z}_7} = \{0\}$
$\sqrt{1}^{\mathbb{Z}_7} = \{1, 6\}$
$\sqrt{2}^{\mathbb{Z}_7} = \{3, 4\}$
$\sqrt{3}^{\mathbb{Z}_7} = \emptyset = \{\}$
$\sqrt{4}^{\mathbb{Z}_7} = \{2, 5\}$

- Si substituïm x per 4 a $x^2 + 3x + 2 \in \mathbb{Z}_5[x]$ ens dona $4^2 + 3 \cdot 4 + 2 = 16 + 12 + 2 = 30 = 0$.
Si substituïm x per 3 a $x^2 + 3x + 2 \in \mathbb{Z}_5[x]$ ens dona $3^2 + 3 \cdot 3 + 2 = 9 + 9 + 2 = 20 = 0$.
- Per $x^2 + 5x + 1$ tenim $b = 5, c = 1$ i les arrels seran $(2 + y)4 \pmod{7}$ 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 $(x)4 \pmod{7}$ 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 $(2 + x)4 \pmod{7}$ 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.
- 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 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 $3^2 + 5 \cdot 3 + 4 = 2 + 1 + 4 = 0$. Si substituïm x per 6 a $x^2 + 5x + 4 \in \mathbb{Z}_5[x]$ ens dona $6^2 + 5 \cdot 6 + 4 = 1 + 2 + 4 = 0$.

Torna a l'exercici (p.61)

Solució de l'Exercici 43

Suposem que $\text{grau}(f(x)) = n$. Vegem per inducció que, si $a_1, \dots, a_s$ són arrels diferents de $f(x)$, aleshores $f(x) = (x - a_1) \cdots (x - a_s)q(x)$ per algun polinomi $q(x)$ de grau $n - s$, amb el que $s \leq n$.

Suposem $s = 1$. Si $x - a_1$ divideix $f(x)$, aleshores $f(x) = (x - a_1)q(x)$ per algun polinomi $q(x)$. Com que $\text{grau}(f(x)) = \text{grau}(x - a_1) + \text{grau}(q(x))$, tenim que $\text{grau}(q(x)) = n - 1$.

Suposem que el resultat és cert per $s - 1$ i demostrem-lo per s . Suposem que $a_1, \dots, a_s$ són arrels diferents de $f(x)$. Per la hipòtesi d'inducció, $f(x) = (x - a_1) \cdots (x - a_{s-1})q(x)$ per algun polinomi $q(x)$ de grau $n - s + 1$.

Com que $x - a_s$ divideix $f(x) = (x - a_1) \cdots (x - a_{s-1})q(x)$, aleshores $f(a_s) = (a_s - a_1) \cdots (a_s - a_{s-1})q(a_s)$ ha de ser zero. Com que $a_s - a_1 \neq 0, \dots, a_s - a_{s-1} \neq 0$ i a $\mathbb{Z}_p$ no hi ha divisors de zero, $q(a_s) = 0$. Per tant, $x - a_s$ divideix $q(x)$ i $q(x) = (x - a_s)\tilde{q}(x)$ per algun polinomi $\tilde{q}(x)$ de grau $n - s$.

Deduïm que $f(x) = (x - a_1) \cdots (x - a_{s-1})q(x) = (x - a_1) \cdots (x - a_s)\tilde{q}(x)$ per algun polinomi $\tilde{q}(x)$ de grau $n - s$.

[Torna a l'exercici \(p.62\)](#)

Solució de l'Exercici 44

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 grau(f) = 2		Si grau(f) = 3	
grau(g)	grau(h)	grau(g)	grau(h)
1	1	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 \(p.63\)](#)

Solució de l'Exercici 45

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 44, 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.63)

Solució de l'Exercici 46

1. Fem la divisió de polinomis

$$\begin{array}{r} x^5 + x^2 + 1 \\ -(x^5 + x^4 + x^3) \\ \hline x^4 + x^3 + x^2 + 1 \\ -(x^4 + x^3 + x^2) \\ \hline 1 \end{array} \quad \left| \begin{array}{l} x^2 + x + 1 \\ x^3 + x^2 \end{array} \right.$$

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

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.63)

Solució de l'Exercici 47

1. Hi ha 9 polinomis mòncics 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.63)

Solució de l'Exercici 48

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.63)

Solució de l'Exercici 49

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 $x^2 + 2x + 2$.

$$\begin{array}{r}
 2x^4 \qquad \qquad + 4x^2 + 3x + 1 \qquad \qquad \left| \begin{array}{l} x^2 + 2x + 2 \\ 2x^2 + x + 3 \end{array} \right. \\
 -(2x^4 + 4x^3 + 4x^2 \qquad \qquad) \\
 \hline
 \qquad x^3 \qquad \qquad + 3x + 1 \\
 -(x^3 + 2x^2 + 2x \qquad \qquad) \\
 \hline
 \qquad \qquad 3x^2 + x + 1 \\
 -(3x^2 + x + 1) \\
 \hline
 \qquad \qquad \qquad \qquad \qquad \qquad 0
 \end{array}$$

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.64)

Solució de l'Exercici 51

$$\mathbb{Z}_2[x]/x^3 + x + 1 = \{[0], [1], [x], [x+1], [x^2], [x^2+1], [x^2+x], [x^2+x+1]\}.$$

Torna a l'exercici (p.66)

Solució de l'Exercici 52

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.66)

Solució de l'Exercici 53

1.

$$\begin{array}{r}
 x^2 + 2x + 2 \\
 -(x^2 + 2x \qquad \qquad) \\
 \hline
 \qquad \qquad \qquad \qquad \qquad \qquad 2
 \end{array}$$

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. • $(2x+1)(2x) = 4x^2 + 2x = x^2 + 2x = x^2 + 2x - (x^2 + 2x + 2) = -2 = 1 \pmod{x^2 + 2x + 2}$.
 • $(x+2)(x) = x^2 + 2x = x^2 + 2x - (x^2 + 2x + 2) = -2 = 1 \pmod{x^2 + 2x + 2}$.

Torna a l'exercici (p.68)

Solució de l'Exercici 54

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]

×	[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.68)

Solució de l'Exercici 55

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.69)

Solució de l'Exercici 58

Si l'ordre de la classe $[x]_f$ és k , aleshores tenim $x^k \equiv 1 \pmod{f(x)}$ 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.69)

Solució de l'Exercici 59

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.
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

×	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,

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

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

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

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

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

Torna a l'exercici (p.73)

Solució de l'Exercici 60

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,

$$f(0) = 2 \neq 0$$

$$f(1) = 1 \neq 0$$

$$f(2) = 2 \neq 0$$

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,

$$\alpha^3 = \alpha\alpha^2 = \alpha(2\alpha + 1) = 2\alpha^2 + \alpha = 2(2\alpha + 1) + \alpha = 2\alpha + 2$$

$$\alpha^4 = \alpha\alpha^3 = \alpha(2\alpha + 2) = 2\alpha^2 + 2\alpha = 2(2\alpha + 1) + 2\alpha = 2$$

$$\alpha^5 = \alpha\alpha^4 = \alpha(2) = 2\alpha$$

$$\alpha^6 = \alpha\alpha^5 = \alpha(2\alpha) = 2\alpha^2 = 2(2\alpha + 1) = \alpha + 2$$

$$\alpha^7 = \alpha\alpha^6 = \alpha(\alpha + 2) = \alpha^2 + 2\alpha = (2\alpha + 1) + 2\alpha = \alpha + 1$$

$$\alpha^8 = \alpha\alpha^7 = \alpha(\alpha + 1) = \alpha^2 + \alpha = (2\alpha + 1) + \alpha = 1$$

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.73)

Solució de l'Exercici 61

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

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

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

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

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.74)

Solució de l'Exercici 62

(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.74)

Solució de l'Exercici 63

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.

·	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

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

Fem la divisió:

$$\begin{array}{r}
 x^5 + \alpha^3 x^4 + \alpha^5 x^3 + \alpha^2 x^2 + \alpha x + \alpha^6 \\
 - (x^5 + \alpha^2 x^4 + \alpha x^3) \\
 \hline
 \alpha^5 x^4 + \alpha^6 x^3 + \alpha^2 x^2 + \alpha x + \alpha^6 \\
 - (\alpha^5 x^4 + x^3 + \alpha^6 x^2) \\
 \hline
 \alpha^2 x^3 + x^2 + \alpha x + \alpha^6 \\
 - (\alpha^2 x^3 + \alpha^4 x^2 + \alpha^3 x) \\
 \hline
 \alpha^5 x^2 + x + \alpha^6 \\
 - (\alpha^5 x^2 + x + \alpha^6) \\
 \hline
 0
 \end{array}
 \quad \left| \begin{array}{l} x^2 + \alpha^2 x + \alpha \\ x^3 + \alpha^5 x^2 + \alpha^2 x + \alpha^5 \end{array} \right.$$

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

Torna a l'exercici (p.75)

Solució de l'Exercici 64

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.

·	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

$$\begin{array}{r}
 5. \quad x^8 \qquad \qquad \qquad + \alpha^4 \quad \left| \begin{array}{l} x^4 + \alpha^6 x^3 + x^2 + \alpha^3 x + \alpha^2 \\ x^4 + \alpha^2 x^3 + x^2 + \alpha^7 x + \alpha^2 \end{array} \right. \\
 - (x^8 + \alpha^6 x^7 + x^6 + \alpha^3 x^5 + \alpha^2 x^4) \\
 \hline
 \alpha^2 x^7 + \alpha^4 x^6 + \alpha^7 x^5 + \alpha^6 x^4 \qquad + \alpha^4 \\
 - (\alpha^2 x^7 + x^6 + \alpha^2 x^5 + \alpha^5 x^4 + \alpha^4 x^3) \\
 \hline
 x^6 + x^5 + \alpha^4 x^4 + x^3 \qquad + \alpha^4 \\
 - (x^6 + \alpha^6 x^5 + x^4 + \alpha^3 x^3 + \alpha^2 x^2) \\
 \hline
 \alpha^7 x^5 + x^4 + \alpha x^3 + \alpha^6 x^2 \qquad + \alpha^4 \\
 - (\alpha^7 x^5 + \alpha^5 x^4 + \alpha^7 x^3 + \alpha^2 x^2 + \alpha x) \\
 \hline
 \alpha^2 x^4 + x^3 + \alpha^2 x^2 + \alpha^5 x + \alpha^4 \\
 - (\alpha^2 x^4 + x^3 + \alpha^2 x^2 + \alpha^5 x + \alpha^4) \\
 \hline
 0
 \end{array}$$

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

Torna a l'exercici (p.75)

Solució de l'Exercici 65

- (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	$\alpha^2 + 1$	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.

Torna a l'exercici (p.76)

4 Caracterització, existència i unicitat dels cossos finits

4.1 Algunes generalitats de cossos

Cossos i isomorfismes de cossos

Recordem les definicions.

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 $a * e_a = e_a * a = e_n$.
- **Propietat commutativa** si $a * b = b * a$ per tot $a, b \in A$.

Definició

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.

Exemple. 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.

Exemple. 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 $a, b, c \in A$.

Definició

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 propietat distributiva respecte de $\oplus$.

Exercici 66

Demostreu que en un anell amb les operacions $\oplus$ i $\otimes$ l'element neutre de $\oplus$ multiplicat per qualsevol element de l'anell dona altra vegada el neutre respecte de $\otimes$.

Solució (p.105)

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

Definició

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 $\otimes$.

Exemple. El conjunt $\{a, e, i, o\}$ dels exemples anteriors és un cos respecte de l'operació $\oplus = +$ amb neutre o , i respecte l'operació $\otimes = *$ 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 $+$, que ho deixem com a exercici.

Definició

Un **morfisme** entre dos cossos E i F és una aplicació

$$f: E \rightarrow F$$

tal que per tot $a, b \in E$ es compleix $f(a + b) = f(a) + f(b)$ i $f(ab) = f(a)f(b)$.

Exercici 67

Demostreu que si f és un morfisme entre els cossos E i F , si 0_E i 0_F són els neutres per la suma de E i F , respectivament, i 1_E i 1_F són els neutres pel producte de E i F , respectivament, aleshores

- $f(0_E) = 0_F$, $f(1_E) = 1_F$,
- $f(-a) = -f(a)$ i $f(a^{-1}) = (f(a))^{-1}$ per tot $a \in E \setminus \{0_E\}$.

Solució (p.105)

Definició

Un **isomorfisme** entre dos cossos E i F és un morfisme injectiu i exhaustiu. Diem que dos cossos són **isomorfs** si existeix un isomorfisme entre ells. En aquest cas escrivim $E \cong F$.

Exemple. Considerem $E = \mathbb{Z}_2[x]/(x^3 + x^2 + 1)$ i anomenem α a la classe de x en E . Considerem $F = \mathbb{Z}_2[x]/(x^3 + x + 1)$ i anomenem β a la classe de x en F .

Les taules d'equivalències a E i a F són

0	0	0	0
α^0	1	β^0	1
α^1	α	β^1	β
α^2	α^2	β^2	β^2
α^3	$\alpha^2 + 1$	β^3	$\beta + 1$
α^4	$\alpha^2 + \alpha + 1$	β^4	$\beta^2 + \beta$
α^5	$\alpha + 1$	β^5	$\beta^2 + \beta + 1$
α^6	$\alpha^2 + \alpha$	β^6	$\beta^2 + 1$

Considerem l'aplicació

$$\begin{aligned}
 f: E &\rightarrow F \\
 0 &\mapsto 0 \\
 \alpha^i &\mapsto (\beta + 1)^i
 \end{aligned}$$

És a dir,

$$\begin{aligned}
 0 &\mapsto 0 \\
 1 &\mapsto 1 \\
 \alpha &\mapsto \beta + 1 = \beta^3 \\
 \alpha^2 &\mapsto (\beta + 1)^2 = (\beta^3)^2 = \beta^6 \\
 \alpha^3 &\mapsto (\beta + 1)^3 = (\beta^3)^3 = \beta^2 \\
 \alpha^4 &\mapsto (\beta + 1)^4 = (\beta^3)^4 = \beta^5 \\
 \alpha^5 &\mapsto (\beta + 1)^5 = (\beta^3)^5 = \beta \\
 \alpha^6 &\mapsto (\beta + 1)^6 = (\beta^3)^6 = \beta^4
 \end{aligned}$$

Per veure si és morfisme ompliu i observeu les taules de $f(a + b)$ i de $f(a) + f(b)$:

$f(a + b)$	$a = 0$	$a = 1$	$a = \alpha$	$a = \alpha^2$	$a = \alpha^3$	$a = \alpha^4$	$a = \alpha^5$	$a = \alpha^6$
$b = 0$	$f(0) = 0$	$f(1) = 1$	$f(\alpha) = \beta^3$	$f(\alpha^2) = \beta^6$	$f(\alpha^3) = \beta^2$	$f(\alpha^4) = \beta^5$	$f(\alpha^5) = \beta$	$f(\alpha^6) = \beta^4$
$b = 1$	$f(1) = 1$	$f(0) = 0$	$f(\alpha + 1) = \beta$	$f(\alpha^2 + 1) = \beta^2$	$f(\alpha^3 + 1) = \beta^6$	$f(\alpha^4 + 1) = \beta^4$	$f(\alpha^5 + 1) = \beta^3$	$f(\alpha^6 + 1) = \beta^5$
$b = \alpha$								
$b = \alpha^2$								
$b = \alpha^3$								
$b = \alpha^4$								
$b = \alpha^5$								
$b = \alpha^6$								

$f(a) + f(b)$	$a = 0$	$a = 1$	$a = \alpha$	$a = \alpha^2$	$a = \alpha^3$	$a = \alpha^4$	$a = \alpha^5$	$a = \alpha^6$
$b = 0$	$0 + 0 = 0$	$1 + 0 = 1$	$\beta^3 + 0 = \beta^3$	$\beta^6 + 0 = \beta^6$	$\beta^2 + 0 = \beta^2$	$\beta^5 + 0 = \beta^5$	$\beta + 0 = \beta$	$\beta^4 + 0 = \beta^4$
$b = 1$	$0 + 1 = 1$	$1 + 1 = 0$	$\beta^3 + 1 = \beta$	$\beta^6 + 1 = \beta^2$	$\beta^2 + 1 = \beta^6$	$\beta^5 + 1 = \beta^4$	$\beta + 1 = \beta^3$	$\beta^4 + 1 = \beta^5$
$b = \alpha$								
$b = \alpha^2$								
$b = \alpha^3$								
$b = \alpha^4$								
$b = \alpha^5$								
$b = \alpha^6$								

Ompliu i observeu les taules de $f(ab)$ i de $f(a)f(b)$:

$f(ab)$	$a = 0$	$a = 1$	$a = \alpha$	$a = \alpha^2$	$a = \alpha^3$	$a = \alpha^4$	$a = \alpha^5$	$a = \alpha^6$
$b = 0$	$f(0) = 0$	$f(0) = 0$	$f(0) = 0$	$f(0) = 0$	$f(0) = 0$	$f(0) = 0$	$f(0) = 0$	$f(0) = 0$
$b = 1$	$f(0) = 0$	$f(1) = 1$	$f(\alpha) = \beta^3$	$f(\alpha^2) = \beta^6$	$f(\alpha^3) = \beta^2$	$f(\alpha^4) = \beta^5$	$f(\alpha^5) = \beta$	$f(\alpha^6) = \beta^4$
$b = \alpha$	$f(0) = 0$	$f(\alpha) = \beta^3$	$f(\alpha^2) = \beta^6$	$f(\alpha^3) = \beta^2$	$f(\alpha^4) = \beta^5$	$f(\alpha^5) = \beta$	$f(\alpha^6) = \beta^4$	$f(1) = 1$
$b = \alpha^2$								
$b = \alpha^3$								
$b = \alpha^4$								
$b = \alpha^5$								
$b = \alpha^6$								

$f(a)f(b)$	$a = 0$	$a = 1$	$a = \alpha$	$a = \alpha^2$	$a = \alpha^3$	$a = \alpha^4$	$a = \alpha^5$	$a = \alpha^6$
$b = 0$	$0 \cdot 0 = 0$	$1 \cdot 0 = 0$	$\beta^3 \cdot 0 = 0$	$\beta^6 \cdot 0 = 0$	$\beta^2 \cdot 0 = 0$	$\beta^5 \cdot 0 = 0$	$\beta \cdot 0 = 0$	$\beta^4 \cdot 0 = 0$
$b = 1$	$0 \cdot 1 = 0$	$1 \cdot 1 = 1$	$\beta^3 \cdot 1 = \beta^3$	$\beta^6 \cdot 1 = \beta^6$	$\beta^2 \cdot 1 = \beta^2$	$\beta^5 \cdot 1 = \beta^5$	$\beta \cdot 1 = \beta$	$\beta^4 \cdot 1 = \beta^4$
$b = \alpha$	$0 \cdot \beta^3 = 0$	$1 \cdot \beta^3 = \beta^3$	$\beta^3 \cdot \beta^3 = \beta^6$	$\beta^6 \cdot \beta^3 = \beta^2$	$\beta^2 \cdot \beta^3 = \beta^5$	$\beta^5 \cdot \beta^3 = \beta$	$\beta \cdot \beta^3 = \beta^4$	$\beta^4 \cdot \beta^3 = 1$
$b = \alpha^2$								
$b = \alpha^3$								
$b = \alpha^4$								
$b = \alpha^5$								
$b = \alpha^6$								

Es tracta d'un morfisme? I d'un isomorfisme?

Extensions de cossos

Definició

Si E és un cos, diem que $F \subseteq E$ és un **subcòs** de E si F també té estructura de cos amb les mateixes operacions que E . Diem que E és una **extensió** de F .

Per demostrar que un subconjunt F d'un cos E és un subcòs s'ha de comprovar que

1. Si $a, b \in F$, aleshores $a + b, a - b \in F$ i $ab \in F$,
2. Si $a \in F$, aleshores a té invers a F .

Exercici 68

Demostreu que si E és una extensió de F , aleshores E és un espai vectorial sobre F .

Definició

Anomenem **grau** de l'extensió de E sobre F a la dimensió de E com a F -espai vectorial, si aquesta és finita. La denotem $[E : F]$.

Exemple. $\mathbb{R}$ és una extensió de $\mathbb{Q}$ de dimensió infinita mentre que $\mathbb{C}$ és una extensió de $\mathbb{R}$ de dimensió 2. Una base de $\mathbb{C}$ respecte $\mathbb{R}$ és $\{1, i\}$.

Exemple. $\mathbb{Z}_2[x]/(x^3 + x + 1)$ és una extensió de $\mathbb{Z}_2$ de dimensió 3, que té per base respecte $\mathbb{Z}_2$ els elements $\{1, \alpha, \alpha^2\}$, on α és la classe de x .

Polinomis sobre un cos

Donat un cos F direm $F[X]$ al conjunt de polinomis amb coeficients a F en la indeterminada X .

Per exemple, si $F = \mathbb{Z}_3[x]/(x^2 + 2x + 2)$ i diem α a la classe de x en $\mathbb{Z}_3[x]/(x^2 + 2x + 2)$, aleshores $F = \{0, 1, \alpha, \alpha^2, \dots, \alpha^7\}$.

L'element $\alpha^2 X^7 + \alpha^6 X^4 + 2X^3 + 1$ serà un polinomi de $F[X]$. Podem avaluar-lo, per exemple, en α i ens donarà $\alpha^9 + \alpha^{10} + 2\alpha^3 + 1 = \alpha + \alpha^2 + \alpha^7 + 1 = \dots$

L'element $X^8 + X^5 + 2X + 1$ serà un polinomi que el podem veure tant com un polinomi de $\mathbb{Z}_3[X]$ com un polinomi de $F[X]$ perquè els seus coeficients són de $\mathbb{Z}_3 \subset F$.

Quan la distinció entre x i X quedi clara pel context, emprarem x en ambdós casos. Així, si estem treballant a F , podrem dir que el polinomi $\alpha^2 x^7 + \alpha^6 x^4 + 2x^3 + 1$ és un polinomi de $F[x]$.

4.2 Característica i cardinal d'un cos finit**Característica d'un cos finit i cos primer****Definició**

Diem que un cos té **característica** a si a és el menor enter positiu tal que

$$\underbrace{1 + 1 + \dots + 1}_a = 0,$$

si aquest enter existeix. Diem que la característica del cos és 0 en cas contrari.

Exemple. El cos $\{a, e, i, o\}$ definit en exemples anteriors té característica 2, el cos $\mathbb{Z}_3[x]/(x^2 + 2x + 2)$ té característica 3.

Lema 15

Si un cos té característica positiva, aleshores la seva característica és necessàriament un nombre primer.

Demostració. Diem F al cos. Si la característica a de F pogués descomposar de manera no trivial en dos enters positius, $a = bc$, aleshores,

$$0 = \underbrace{1 + 1 + \dots + 1}_b + \underbrace{1 + 1 + \dots + 1}_b + \dots + \underbrace{1 + 1 + \dots + 1}_b.$$

c

Com que $b < a$, l'element $\underbrace{1 + 1 + \dots + 1}_b$ és no nul i, per tant, té un invers dins de F . Anomenem $\tilde{b}$ aquest invers. Multiplicant la igualtat anterior per $\tilde{b}$ obtenim que $\underbrace{1 + 1 + \dots + 1}_c = 0$, en contradicció amb l'elecció de c . □

Lema 16

En un cos F de característica $p > 0$, per tota col·lecció finita d'elements $a_1, \dots, a_i \in F$ es té

$$(a_1 + a_2 + \dots + a_i)^p = a_1^p + a_2^p + \dots + a_i^p.$$

Demostració. Per $i = 2$, $(a_1 + a_2)^p = \sum_{j=0}^p \binom{p}{j} a_1^j a_2^{p-j}$. Però tots els coeficients $\binom{p}{j}$ són múltiples de p llevat de $\binom{p}{0}$ i $\binom{p}{p}$, d'on es dedueix que $(a_1 + a_2)^p = \binom{p}{0} a_1^0 a_2^p + \binom{p}{p} a_1^p a_2^0 = a_1^p + a_2^p$. Per $i > 2$, utilitzant el cas anterior i la hipòtesi d'inducció, $(a_1 + a_2 + \dots + a_i)^p = ((a_1 + a_2 + \dots + a_{i-1}) + a_i)^p = (a_1 + a_2 + \dots + a_{i-1})^p + a_i^p = a_1^p + a_2^p + \dots + a_i^p$. □

Exercici 69

Què passa en el lema anterior si canviem algun $+$ per $-$? Indicació: Podeu separar els casos de característica parell i de característica senar.

Suposem que F és un cos de característica positiva i diem p a la característica de F . El conjunt

$$K = \{1, 1 + 1, \dots, \underbrace{1 + 1 + \dots + 1}_{p-1}, \underbrace{1 + 1 + \dots + 1}_p = 0\}$$

és un subcòs de F . De fet, K és isomorf a $\mathbb{Z}_p$.

Definició

El **cos primer** de F és el seu subcòs $K = \{1, 1 + 1, \dots, \underbrace{1 + 1 + \dots + 1}_{p-1}, \underbrace{1 + 1 + \dots + 1}_p = 0\}$ o, simplement, $\mathbb{Z}_p$.

Lema 17

El cos primer K d'un cos F de característica positiva p compleix que K és el conjunt d'arrels de $x^p - x \in F[x]$.

Demostració. L'element 0 és òbviament una arrel de $x^p - x$ i, pel teorema petit de Fermat, també tots els elements de $\mathbb{Z}_p$ no nuls són arrels de $x^p - x$. Com que F és un cos, el polinomi $x^p - x$ té com a molt p arrels i com que hem vist que els p elements de $\mathbb{Z}_p$ són arrels, aquestes seran exactament totes les arrels. □

Com a conseqüència, un element $a \in F$ pertany a K si i només si $a^p = a$.

Lema 18

Sigui F un cos de característica $p > 0$. Un polinomi $f(x) \in F(x)$ pertany a $\mathbb{Z}_p[x]$ si i només si $(f(x))^p = f(x^p)$.

Demostració. Suposem que $f(x) = a_0 + a_1x + a_2x^2 + \dots + a_rx^r$ per algun enter r i per $a_0, \dots, a_r \in F$. Aleshores $(f(x))^p = (a_0 + a_1x + a_2x^2 + \dots + a_rx^r)^p = a_0^p + a_1^p x^p + a_2^p (x^p)^2 + \dots + a_r^p (x^p)^r$ mentre que $f(x^p) = a_0 + a_1x^p + a_2(x^p)^2 + \dots + a_r(x^p)^r$. Per tant, $(f(x))^p = f(x^p)$ si i només si $a_i^p = a_i$ per tot i entre 0 i r , és a dir, si i només si $f(x) \in \mathbb{Z}_p[x]$. $\square$

Cardinal d'un cos finit

Teorema 11

Si un cos F és finit, aleshores el seu cardinal és p^m per algun primer p i un enter positiu m .

Demostració. Sigui p la característica i sigui K el cos primer de F . Per l'Exercici 68, sabem que F és un K -espai vectorial. Si la dimensió de F sobre K és m , aleshores existeix una base $x_1, \dots, x_m$ de F sobre K . Aleshores els elements de F són totes les combinacions lineals $\lambda_1 x_1 + \dots + \lambda_m x_m$ amb tots els $\lambda_i \in K$. Com que K té p elements, necessàriament, $|F| = p^m$. $\square$

4.3 Ordre multiplicatiu i teorema de l'element primitiu

Ordre multiplicatiu

Lema 19

En un cos finit F de q elements, qualsevol element $\alpha \in F \setminus \{0\}$ satisfà que $\alpha^{q-1} = 1$.

Demostració. Per tot $\beta, \beta' \in F \setminus \{0\}$, es té que $\alpha\beta = \alpha\beta'$ si i només si $\beta = \beta'$ i, a més a més, $\alpha\beta \neq 0$. Per tant, $\{\alpha\beta : \beta \in F \setminus \{0\}\} = \{\beta : \beta \in F \setminus \{0\}\}$ i

$$\prod_{\beta \in F \setminus \{0\}} \alpha\beta = \prod_{\beta \in F \setminus \{0\}} \beta.$$

En conseqüència, $\alpha^{q-1} \prod_{\beta \in F \setminus \{0\}} \beta = \prod_{\beta \in F \setminus \{0\}} \beta$, d'on deduïm que $\alpha^{q-1} = 1$, ja que el producte $\prod_{\beta \in F \setminus \{0\}} \beta$ és invertible. $\square$

Definició

En un cos finit F , l'**ordre multiplicatiu** d'un element $\alpha \in F \setminus \{0\}$ és el mínim exponent $i > 0$ tal que $\alpha^i = 1$. L'anomenem $\text{ord}_F(\alpha)$.

Lema 20

En un cos finit F , si $\alpha \in F \setminus \{0\}$ satisfà $\alpha^c = 1$ amb $c > 0$, aleshores $\text{ord}_F(\alpha) \mid c$.

Demostració. Suposem que $a = \text{ord}_F(\alpha)$. Sigui r el residu de la divisió euclidiana de c entre a . Tindrem $\alpha^r = \alpha^c = 1$ amb $0 \leq r < a$. Això només és possible si $r = 0$ i, per tant, si a divideix c . $\square$

Corol·lari 1

Si F és un cos finit de q elements i $\alpha \in F \setminus \{0\}$, aleshores $\text{ord}_F(\alpha) \mid q - 1$.

Lema 21

En un cos finit F , si existeixen $\alpha, \beta \in F \setminus \{0\}$ amb $a = \text{ord}_F(\alpha)$ i $b = \text{ord}_F(\beta)$, aleshores existeix $\gamma \in F \setminus \{0\}$ tal que $\text{ord}_F(\gamma) = \text{mcm}(a, b)$.

Demostració. Si $\text{mcd}(a, b) = 1$, aleshores $\alpha\beta$ té ordre ab . En efecte, d'una banda $(\alpha\beta)^{ab} = 1^b 1^a = 1$. D'altra banda, si per algun $0 < c < ab$ es compleix $(\alpha\beta)^c = 1$, aleshores $1 = (\alpha\beta)^{bc} = \alpha^{bc}$. Deduïm que $a \mid bc$ i, com que $\text{mcd}(a, b) = 1$, aleshores $a \mid c$. De manera anàloga podem veure que $b \mid c$. Per tant, $ab \mid c$, en contradicció amb l'elecció de c . Si $\text{mcd}(a, b) = d > 1$,

- Podem descompondre d en producte de primers $d = p_1^{e_1} \cdots p_s^{e_s}$ de manera que $p_1^{e_1+1} \nparallel a, \dots, p_k^{e_k+1} \nparallel a$ mentre que $p_{k+1}^{e_{k+1}+1} \nparallel b, \dots, p_s^{e_s+1} \nparallel b$. Diem $d_1 = p_1^{e_1} \cdots p_k^{e_k}$, $d_2 = p_{k+1}^{e_{k+1}} \cdots p_s^{e_s}$. Tindrem $\text{mcd}(\frac{a}{d_1}, \frac{b}{d_2}) = 1$ mentre que $\text{mcm}(a, b) = \frac{a}{d_1} \frac{b}{d_2}$.
- α^{d_1} té ordre $\frac{a}{d_1}$. En efecte, d'una banda $(\alpha^{d_1})^{\frac{a}{d_1}} = 1$. D'altra banda, si per algun enter $c < \frac{a}{d_1}$ es compleix $(\alpha^{d_1})^c = 1$, aleshores $\alpha^{d_1 c} = 1$ i, per tant, $a \mid d_1 c$. Deduïm que $\frac{a}{d_1} \mid c$. Anàlogament, β^{d_2} té ordre $\frac{b}{d_2}$.
- Com que $\text{mcd}(\frac{a}{d_1}, \frac{b}{d_2}) = 1$, aleshores $\alpha^{d_1} \beta^{d_2}$ té ordre $\frac{a}{d_1} \frac{b}{d_2} = \text{mcm}(a, b)$. $\square$

Teorema de l'element primitiu**Lema 22**

Suposem que en un cos finit F els ordres multiplicatius de tots els elements no nuls són $a_1, a_2, \dots, a_k$. Aleshores existeix un element $\xi \in F \setminus \{0\}$ tal que $\text{ord}_F(\xi) = \text{mcm}(a_1, \dots, a_k)$.

El lema es pot demostrar per inducció utilitzant el resultat demostrat per dos elements i la recurrència

$$\text{mcm}(a_1, \dots, a_k) = \text{mcm}(\text{mcm}(a_1, \dots, a_{k-1}), a_k).$$

Lema 23

En un cos finit de q elements, el mínim comú múltiple dels ordres de tots els elements no nuls del cos és $q - 1$.

Demostració. Diem M al mínim comú múltiple dels ordres de tots els elements no nuls del cos. D'una banda $M \leq q - 1$, ja que tots els ordres de tots elements no nuls del cos són divisors de $q - 1$ i, per tant, M serà un divisor de $q - 1$. D'altra banda es pot veure que $M \geq q - 1$. En efecte, per a tot $\alpha \in F \setminus \{0\}$ es té $\alpha^M = 1$, per tant tot $\alpha \in F \setminus \{0\}$ és arrel de $x^M - 1 \in F[x]$ i, com que F és un cos, $q - 1 \leq M$. $\square$

Definició

Diem que un element no nul ξ d'un cos finit F de q elements és un **element primitiu** del cos si el seu ordre multiplicatiu és $q - 1$.

De tots els lemes anteriors es dedueix el teorema següent:

Teorema 12: Teorema de l'element primitiu

Tot cos finit té un element primitiu.

Exercici 70

Demostreu que en un cos finit de q elements hi ha exactament $\phi(q - 1)$ elements primitius.

Lema 24

En un cos finit F de q elements, per a tot divisor de $q - 1$ existeix un element del cos amb ordre multiplicatiu igual a aquest divisor.

Demostració. Sigui ξ un element primitiu de F i sigui d un divisor de $q - 1$. L'element $\xi^r = \xi^{(q-1)/d}$ tindrà ordre d . En efecte, d'una banda $\xi^{rd} = 1$. D'altra banda, si $\xi^{rc} = 1$, aleshores $\xi^{c(q-1)/d} = 1$ amb el que $c(q - 1)/d \geq q - 1$ i, per tant, $c \geq d$. $\square$

4.4 Polinomi mínim i caracterització dels cossos finits

Polinomi mínim

Suposem que tenim un cos finit F de p^m elements.

Observem que si un element $\gamma \in F$ té $\text{ord}_F(\gamma) = r$, aleshores anul·la els polinomis $x^r - 1$ i $x^{p^m-1} - 1$.

Considerem el polinomi

$$m_\gamma(x) = (x - \gamma)(x - \gamma^p)(x - \gamma^{p^2}) \cdots (x - \gamma^{p^{s-1}}) \in \mathbb{Z}_p[x],$$

on s és el mínim enter positiu tal que $\gamma^{p^s} = \gamma$.

En particular, $s \leq m$ i, si γ és primitiu, aleshores $s = m$.

Veurem que $m_\gamma(x) \in \mathbb{Z}_p[x]$ i que té grau mínim d'entre tots els polinomis de $\mathbb{Z}_p[x]$ que s'anul·len quan els avaluem a γ .

Per això s'anomena el **polinomi mínim** de γ respecte $\mathbb{Z}_p$

Lema 25

Sigui F un cos finit i sigui $\gamma \in F \setminus \{0\}$.

1. $m_\gamma(x) \in \mathbb{Z}_p[x]$.
2. Tot polinomi de $\mathbb{Z}_p[x]$ que s'anul·li a γ serà un múltiple de $m_\gamma(x)$.
3. $m_\gamma(x)$ és irreductible a $\mathbb{Z}_p[x]$.

Demostració. 1. Observem que $(m_\gamma(x))^p = (x^p - \gamma^p)(x^p - \gamma^{p^2}) \dots (x^p - \gamma^{p^{s-1}})(x^p - \gamma) = m_\gamma(x^p)$.
Per tant, $m_\gamma(x) \in \mathbb{Z}_p[x]$.

2. Si un polinomi $f(x) \in \mathbb{Z}_p[x]$ satisfà $f(\gamma) = 0$, aleshores $(f(\gamma))^{p^i} = 0$ per qualsevol i . Però $(f(\gamma))^{p^i} = f(\gamma^{p^i}) = 0$ i, per això, f haurà de tenir les arrels $\gamma, \gamma^p, \dots, \gamma^{p^{s-1}}$. En conseqüència, haurà de ser un múltiple de $m_\gamma(x)$.

3. Com que $m_\gamma(\gamma) = 0$, algun dels factors irreductibles de $m_\gamma(x)$ s'haurà d'anul·lar també a γ . Pel punt anterior, aquest factor irreductible haurà de ser un múltiple de $m_\gamma(x)$ amb el que no queda més remei que $m_\gamma(x)$ sigui el propi factor irreductible. □

Exemple. Considerem el cos $E = \mathbb{Z}_3[x]/(x^2 + x + 2)$ i diem α a la classe de x dins el quocient. Tenim la taula d'equivalències

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	$\alpha + 1$

Els polinomis mínims dels elements de E seran

$$\begin{aligned}
 m_0(x) &= x \\
 m_1(x) &= x - 1 \\
 m_\alpha(x) &= (x - \alpha)(x - \alpha^3) = x^2 - (\alpha + \alpha^3)x + \alpha^4 = x^2 + x + 2 \\
 m_{\alpha^2}(x) &= (x - \alpha^2)(x - \alpha^6) = x^2 - (\alpha^2 + \alpha^6)x + 1 = x^2 + 1 \\
 m_{\alpha^3}(x) &= (x - \alpha^3)(x - \alpha) = m_\alpha(x) \\
 m_{\alpha^4}(x) &= x - \alpha^4 = x - 2 \\
 m_{\alpha^5}(x) &= (x - \alpha^5)(x - \alpha^7) = x^2 - (\alpha^5 + \alpha^7)x + \alpha^4 = x^2 + 2x + 2 \\
 m_{\alpha^6}(x) &= (x - \alpha^6)(x - \alpha^2) = m_{\alpha^2}(x) \\
 m_{\alpha^7}(x) &= (x - \alpha^7)(x - \alpha^5) = m_{\alpha^5}(x)
 \end{aligned}$$

Caracterització dels cossos finits

Teorema 13: Caracterització dels cossos finits

Tot cos finit és isomorf a un cos de la forma $\mathbb{Z}_p/(f(x))$ amb p primer i $f(x)$ un polinomi irreductible de $\mathbb{Z}_p[x]$.

Demostració. Sigui F un cos finit i sigui p la seva característica. Sabem que existeix un element primitiu $\xi \in F$. Considerem el morfisme d'anells

$$\begin{aligned}\mathbb{Z}_p[x] &\rightarrow F \\ f(x) &\mapsto f(\xi)\end{aligned}$$

Es tracta d'un morfisme exhaustiu (F és la imatge de $0, 1, x, \dots, x^{|F|-2}$) i té nucli l'ideal generat per $m_\xi(x)$. Pel teorema d'isomorfisme, deduïm que $F \simeq \mathbb{Z}_p/(f(x))$. $\square$

4.5 Existència d'un cos finit de p^m elements

Existència d'un cos amb les arrels de $x^{p^m} - x$

Donat un cos qualsevol F i un polinomi $f(x)$ de $F[x]$ podem definir les classes de congruència dels elements de $F[x]$ mòdul el polinomi $f(x)$ tal i com havíem fet per $\mathbb{Z}_p[x]$.

El conjunt de classes formarà un cos si i només si el polinomi $f(x)$ és irreductible a $F[x]$. El grau de l'extensió serà el grau del polinomi.

Exemple. El polinomi $x^2 + 1$ és irreductible a $\mathbb{R}[x]$. En el conjunt de classes de $C = \mathbb{R}[x]/(x^2 + 1)$ podem anomenar i a la classe de x . Qualsevol element de C el podrem escriure com $a + bi$ amb $a, b \in \mathbb{R}$. Les operacions suma i producte seran

$$(a + bi) + (a' + b'i) = (a + a') + (b + b')i,$$

$$(a + bi)(a' + b'i) = (aa') + (ab' + a'b)i + (bb')i^2 = (aa' - bb') + (ab' + a'b)i.$$

Observem que $C \cong \mathbb{C}$.

Definició

Donat un cos F i un polinomi irreductible $f(x) \in F[x]$, del cos format pel conjunt de classes de congruència mòdul el polinomi $f(x)$ en diem l'**extensió de F pel polinomi $f(x)$** i el denotem $F[x]/(f(x))$.

És fàcil comprovar que $F[x]/(f(x))$ tindrà la mateixa característica i el mateix cos primer que F .

Observem com el polinomi $f(x)$, que no tenia arrels a F , ara té l'arrel corresponent a la classe de x dins de $F[x]/(f(x))$. En particular, el nombre d'arrels de $f(x)$ ha augmentat, de F a $F[x]/(f(x))$.

Lema 26

Per tot enter positiu m existeix una extensió de $\mathbb{Z}_p$ que conté totes les arrels de $x^{p^m} - x$.

Demostració. Diem $E_1 = \mathbb{Z}_p$. Suposem que totes les arrels de $x^{p^m} - x$ dins de E_1 són $\alpha_1 = 0, \alpha_2, \dots, \alpha_{n_1}$ (poden ser repetides). Aleshores,

$$x^{p^m} - x = x(x - \alpha_2) \cdots (x - \alpha_{n_1}) f_1(x)$$

per un únic polinomi mònic $f_1(x) \in E_1[x]$. Diem $i_1(x)$ a un qualsevol dels factors irreductibles de $f_1(x)$ dins de $E_1[x]$. Construïm $E_2 = E_1[x]/(i_1(x))$.

Ara suposem que totes les arrels de $x^{p^m} - x$ dins de E_2 són $\alpha_1 = 0, \alpha_2, \dots, \alpha_{n_1}, \dots, \alpha_{n_2}$ (amb repeticions si cal). Necessàriament, $n_2 > n_1$ per la manera com hem construït E_2 . A més, com que E_2 és un cos, $n_2 \leq \text{grau}(x^{p^m} - x) = p^m$. Així,

$$n_1 < n_2 \leq p^m.$$

Mentre $n_i < p^m$ podem repetir el procediment. És a dir, considerem l'únic polinomi mònic $f_2(x) \in E_2[x]$ tal que

$$x^{p^m} - x = x(x - \alpha_2) \cdots (x - \alpha_{n_2}) f_2(x).$$

Diem $i_2(x)$ a un qualsevol dels factors irreductibles de $f_2(x)$ dins de $E_2[x]$ i construïm $E_3 = E_2[x]/(i_2(x))$. Ara totes les arrels de $x^{p^m} - x$ dins de E_3 seran $\alpha_1 = 0, \alpha_2, \dots, \alpha_{n_1}, \dots, \alpha_{n_2}, \dots, \alpha_{n_3}$ amb

$$n_1 < n_2 < n_3 \leq p^m.$$

En algun moment n_i coincidirà amb p^m i, en aquest moment, E_i contindrà totes les arrels de $x^{p^m} - x$.
□

Definició

Donat un cos F i un polinomi $f(x) = \sum_{i=0}^d a_i x^i \in F[x]$, definim la **derivada formal** de $f(x)$ com

$$f'(x) = \sum_{i=1}^d i a_i x^{i-1}.$$

Exercici 71

Comproveu les següents propietats:

- $(f(x)g(x))' = f(x)'g(x) + f(x)g'(x)$,
- $(f(g(x)))' = f'(g(x))g'(x)$.

Lema 27

Si una extensió E de F conté totes les arrels de $f(x) \in F[x]$, aleshores totes les arrels de f en E són diferents si i només si $\text{mcd}(f(x), f'(x)) = 1$.

Demostració. Si $f(x)$ tingués una arrel múltiple α , aleshores $f(x) = (x - \alpha)^2 g(x)$ amb $g(x)$ un polinomi de grau dos menys que el grau de $f(x)$. Aleshores $f'(x) = 2(x - \alpha)g(x) + (x - \alpha)^2 g'(x)$. Observem que en aquest cas $(x - \alpha)$ divideix tant $f(x)$ com $f'(x)$ i, per tant, $\text{mcd}(f(x), f'(x)) \neq 1$. Recíprocament, si $\text{mcd}(f(x), f'(x)) \neq 1$, el polinomi $r(x) = \text{mcd}(f(x), f'(x)) \neq 1$ també tindrà totes les arrels a E . Sigui α una arrel de $r(x)$. Escrivim $f(x) = (x - \alpha)h(x)$ amb $h(x)$ un polinomi de grau un menys que el grau de $f(x)$. Tindrem $f'(x) = h(x) + (x - \alpha)h'(x)$, d'on deduïm que $(x - \alpha)$ ha de dividir $h(x)$ i, per tant, α és una arrel múltiple de $f(x)$.
□

El lema següent és una conseqüència del Lema 26, el Lema 27, i el fet que la derivada formal de $x^{p^m} - x$ és

-1 a $\mathbb{Z}_p$.

Lema 28

Per tot enter positiu m existeix una extensió de $\mathbb{Z}_p$ que conté totes les arrels de $x^{p^m} - x$ i totes elles són diferents.

Existència d'un cos finit de p^m elements

Teorema 14: Existència de cossos finits

Per tot enter positiu m existeix un cos finit de cardinal p^m .

Demostració. Pel Lema 28 existeix una extensió E de $\mathbb{Z}_p$ que conté totes les arrels de $x^{p^m} - x$ i totes elles són diferents. Considerem el conjunt $A \subseteq E$ de totes les arrels de $x^{p^m} - x$. Com que sabem que són diferents i el grau de $x^{p^m} - x$ és p^m podem afirmar que el cardinal de A és exactament p^m . Vegem que A és un subcòs de E (i, per tant, és un cos). Suposem que $a, b \in A$, aleshores hem de comprovar que $a + b, a - b, ab, a^{-1}$ són arrels de $x^{p^m} - x$. En efecte,

- $(a + b)^{p^m} - (a + b) = a^{p^m} + b^{p^m} - a - b = (a^{p^m} - a) + (b^{p^m} - b) = 0$,
- $(a - b)^{p^m} - (a - b) = a^{p^m} - b^{p^m} - a + b = (a^{p^m} - a) - (b^{p^m} - b) = 0$,
- $(ab)^{p^m} - (ab) = a^{p^m} b^{p^m} - ab = ab - ab = 0$,
- $(a^{-1})^{p^m} - a^{-1} = (a^{p^m})^{-1} - a^{-1} = a^{-1} - a^{-1} = 0$.

□

4.6 Unicitat del cos finit de p^m elements

Factorització del polinomi $x^{p^m} - x$

Lema 29

En un cos finit F de p^m elements, els seus p^m elements són exactament les arrels de $x^{p^m} - x$. És a dir,

$$\prod_{\alpha \in F} (x - \alpha) = x^{p^m} - x$$

Demostració. Com que els p^m elements de F són arrels de $x^{p^m} - x$ tenim que $\prod_{\alpha \in F} (x - \alpha)$ divideix $x^{p^m} - x$. Però com que tots dos polinomis són mònics i tenen el mateix grau, han de coincidir. □

En particular, totes les arrels de $x^{p^m} - x$ dins de F són diferents.

Exercici 72

Demostreu que els factors irreductibles de la descomposició de $x^{p^m} - x$ dins de $\mathbb{Z}_p[x]$ són tots diferents.

Exercici 73

Demostreu que si $f(x) \in \mathbb{Z}_p[x]$ és irreductible a $\mathbb{Z}_p[x]$, aleshores $f(x)$ ha de dividir $x^{p^{\text{grau}(f)}} - x$.

Solució (p.105)

Exercici 74

Sigui F un cos finit de p^m elements. Si $\gamma \in F$ definim $C_\gamma = \{\gamma, \gamma^p, \gamma^{p^2}, \dots, \gamma^{p^{s-1}}\}$ on s és el mínim enter positiu tal que $\gamma^{p^s} = \gamma$.

- Qui són C_0 i C_1 ?
- Demostreu que si $\gamma' \notin C_\gamma$, aleshores $C_\gamma \cap C_{\gamma'} = \emptyset$.
- Demostreu que existeix un subconjunt $\Gamma(F) = \{\gamma_1, \dots, \gamma_r\} \subseteq F$ tal que F és la unió disjunta de $C_{\gamma_1}, \dots, C_{\gamma_r}$.
- Demostreu que

$$x^{p^m} - x = \prod_{\gamma \in \Gamma(F)} m_\gamma(x).$$

Solució (p.105)

Exemple. Considerem el cos $E = \mathbb{Z}_3[x]/(x^2 + x + 2)$ de l'exemple anterior. Es pot comprovar que $x^9 - x = m_0(x)m_1(x)m_\alpha(x)m_{\alpha^2}(x)m_{\alpha^4}(x)m_{\alpha^5}(x) = x(x-1)(x^2+x+2)(x^2+1)(x-2)(x^2+2x+2)$.

Exercici 75

Demostreu que en un cos finit F de p^m elements,

- $\prod_{\alpha \in F \setminus \{0\}} \alpha = -1$
- Si $p^m \neq 2$, $\sum_{\alpha \in F \setminus \{0\}} \alpha = 0$

Solució (p.106)

Unicitat del cos finit de p^m elements**Teorema 15: Unicitat del cos finit de p^m elements**

Tots els cossos finits del mateix cardinal són isomorfs.

Demostració. Suposem que E i F són dos cossos finits amb el mateix cardinal. Pel Teorema 11 sabem que aquest cardinal és p^m per algun primer p i algun enter positiu m . Pel Teorema 12 sabem que E té un element primitiu que anomenem ξ . Com que ξ és primitiu, el grau del seu polinomi mínim és m . Per l'Exercici 74 sabem que el polinomi mínim de ξ coincidirà amb el polinomi mínim d'algun element $\zeta \in F$. Sabem que $\{1, \xi, \xi^2, \dots, \xi^{m-1}\}$ és una $\mathbb{Z}_p$ -base de E mentre que $\{1, \zeta, \zeta^2, \dots, \zeta^{m-1}\}$ és una $\mathbb{Z}_p$ -base de F i que, per tot exponent i , les coordenades de ξ^i en la base $\{1, \xi, \xi^2, \dots, \xi^{m-1}\}$ coincidiran amb les coordenades de ζ^i en la base $\{1, \zeta, \zeta^2, \dots, \zeta^{m-1}\}$. Aquestes coordenades les denotem $(\lambda_0^i, \dots, \lambda_{m-1}^i)$. Recíprocament diem que $i = \log(\lambda_0^i + \lambda_1^i \xi + \dots + \lambda_{m-1}^i \xi^{m-1}) = \log(\lambda_0^i + \lambda_1^i \zeta + \dots + \lambda_{m-1}^i \zeta^{m-1})$. Definim l'aplicació $f : E \rightarrow F$ que assigna $0 \in E$ a $0 \in F$ i que per tot $i > 0$ assigna $f(\xi^i) = \zeta^i$. Vegem que és un isomorfisme.

$$\begin{aligned}
 f(\xi^i + \xi^j) &= f((\lambda_0^i + \lambda_1^i \xi + \dots + \lambda_{m-1}^i \xi^{m-1}) + (\lambda_0^j + \lambda_1^j \xi + \dots + \lambda_{m-1}^j \xi^{m-1})) \\
 &= f((\lambda_0^i + \lambda_0^j)1 + (\lambda_1^i + \lambda_1^j)\xi + \dots + (\lambda_{m-1}^i + \lambda_{m-1}^j)\xi^{m-1}) \\
 &= f(\xi^{\log((\lambda_0^i + \lambda_0^j)1 + \dots + (\lambda_{m-1}^i + \lambda_{m-1}^j)\xi^{m-1})}) \\
 &= \zeta^{\log((\lambda_0^i + \lambda_0^j)1 + \dots + (\lambda_{m-1}^i + \lambda_{m-1}^j)\zeta^{m-1})} \\
 &= (\lambda_0^i + \lambda_0^j)1 + \dots + (\lambda_{m-1}^i + \lambda_{m-1}^j)\zeta^{m-1} \\
 &= (\lambda_0^i + \lambda_1^i \zeta + \dots + \lambda_{m-1}^i \zeta^{m-1}) + (\lambda_0^j + \lambda_1^j \zeta + \dots + \lambda_{m-1}^j \zeta^{m-1}) \\
 &= \zeta^i + \zeta^j = f(\xi^i) + f(\xi^j).
 \end{aligned}$$

De la mateixa manera podem provar que $f(\xi^i - \xi^j) = f(\xi^i) - f(\xi^j)$.

D'altra banda,

$$\begin{aligned}
 f(\xi^i \xi^j) &= f(\xi^{i+j}) & f((\xi^i)^{-1}) &= f(\xi^{p^m-1-i}) \\
 &= \zeta^{i+j} & &= \zeta^{p^m-1-i} \\
 &= \zeta^i \zeta^j & &= (\zeta^i)^{-1} \\
 &= f(\xi^i) f(\xi^j), & &= (f(\xi^i))^{-1}.
 \end{aligned}$$

□

Pel teorema anterior, donada una potència de primer p^m podem escriure $\mathbb{F}_{p^m}$ per denotar l'únic cos finit de p^m elements.

Exercici 76

Construïu $\mathbb{F}_9$ utilitzant dos polinomis generadors diferents.

- Doneu les taules d'equivalències potencial polinòmica en ambdós casos.
- Expliciteu l'isomorfisme que existeix entre els dos cossos.

Exercici 77

Pel que hem dit, el cos finit $\{a, e, i, o\}$ que té taula de sumes i de producte

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

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

ha de ser isomorf a $\mathbb{F}_4$. Construïu $\mathbb{F}_4$ a partir del seu cos primer i un polinomi generador i doneu la correspondència entre els elements obtinguts en aquesta construcció i els elements $\{a, e, i, o\}$.

4.7 Solucions**Solució de l'Exercici 66**

Segui a un element de l'anell i sigui 0 el neutre per l'operació $\oplus$. Tenim

$$0 \otimes a = (0 \oplus 0) \otimes a = (0 \otimes a) \oplus (0 \otimes a).$$

Si ara sumem l'oposat de $0 \otimes a$ a banda i banda de la igualtat obtenim que

$$0 = 0 \otimes a,$$

com volíem veure.

Torna a l'exercici (p.91)

Solució de l'Exercici 67

Segui a un element de l'anell i sigui 0 el neutre per l'operació $\oplus$. Tenim

$$0 \otimes a = (0 \oplus 0) \otimes a = (0 \otimes a) \oplus (0 \otimes a).$$

Si ara sumem l'oposat de $0 \otimes a$ a banda i banda de la igualtat obtenim que

$$0 = 0 \otimes a,$$

com volíem veure.

Torna a l'exercici (p.91)

Solució de l'Exercici 73

L'anell $\mathbb{Z}_p[x]/(f(x))$ és un cos de cardinal $p^{\text{grau}(f)}$. Diem α a la classe de x dins del cos $\mathbb{Z}_p[x]/(f(x))$. Com que f té els coeficients a $\mathbb{Z}_p$, satisfà $f(\alpha) = 0$ i f és irreductible, deduïm que $f = m_\alpha(x)$. D'altra banda, el polinomi $x^{p^{\text{grau}(f)}} - x$ també s'anul·la en α . Per això, $x^{p^{\text{grau}(f)}} - x$ ha de ser un múltiple de $m_\alpha(x) = f(x)$.

Torna a l'exercici (p.103)

Solució de l'Exercici 74

- $C_0 = \{0\}$, $C_1 = \{1\}$.
- Suposem que $C_\gamma \cap C_{\gamma'} \neq \emptyset$. Siguin s, s' els menors enters no negatius tals que $\gamma^{p^s} = \gamma$ i $(\gamma')^{p^{s'}} = \gamma'$. Com que $C_\gamma \cap C_{\gamma'} \neq \emptyset$, existeixen enters k, k' amb $1 \leq k \leq s$ i $1 \leq k' \leq s'$ tals que $\gamma^{p^k} = (\gamma')^{p^{k'}}$. Elevant les dues bandes de la igualtat a $p^{s'-k'}$ tindrem que $\gamma^{p^{k+s'-k'}} = (\gamma')^{p^{s'}} = \gamma'$, d'on es dedueix que $\gamma' \in C_\gamma$.

- Es dedueix de manera directa de l'apartat anterior.
- Es dedueix directament de l'apartat anterior i el Lema 29.

Torna a l'exercici (p.103)

Solució de l'Exercici 75

Suposem que q és potència d'un primer. Sabem que

$$x^q - x = (x - a_1)(x - a_2) \cdots (x - a_q)$$

on els $a_1, \dots, a_q$ són els elements d'un cos de cardinal q i també que

$$x^{q-1} - 1 = (x - a_1)(x - a_2) \cdots (x - a_{q-1})$$

on els $a_1, \dots, a_{q-1}$ són els elements *no nuls* d'un cos de cardinal q . Ara mirem coeficient a coeficient a les dues bandes de la segona igualtat.

El coeficient constant és -1 a l'esquerra de la igualtat i $(-1)^{q-1} a_1 a_2 \cdots a_{q-1}$ a la dreta. Si q és parell deduïm (a) del fet que $-1 = 1$. Si q és senar deduïm (a) del fet que $(-1)^{q-1} = -1$.

El coeficient de grau $q-1$ és 0 a l'esquerra de la igualtat i $-a_1 - a_2 - \dots - a_{q-1}$ a la dreta, d'on es dedueix (b).

Torna a l'exercici (p.103)

5 Codis lineals

5.1 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.

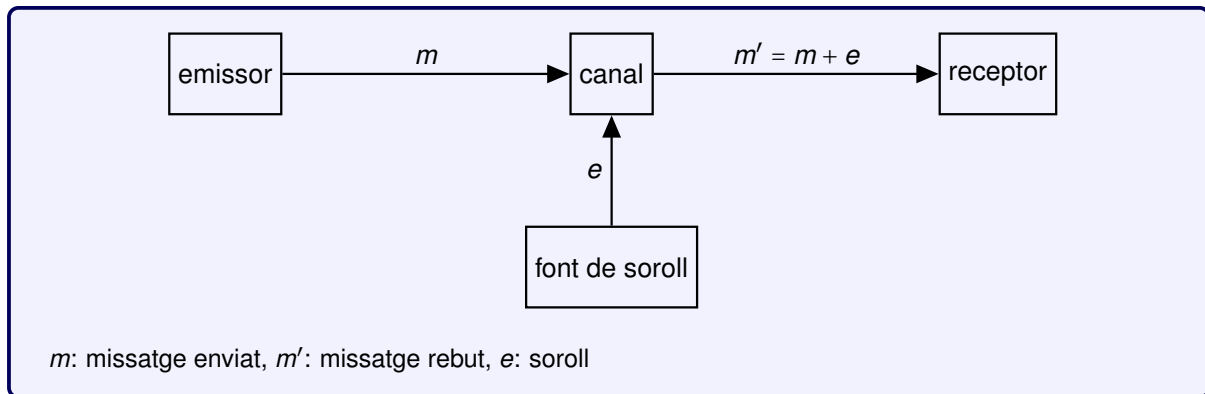
Podríem corregir un sol error en cada paraula i fins a tres esborralls.

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.



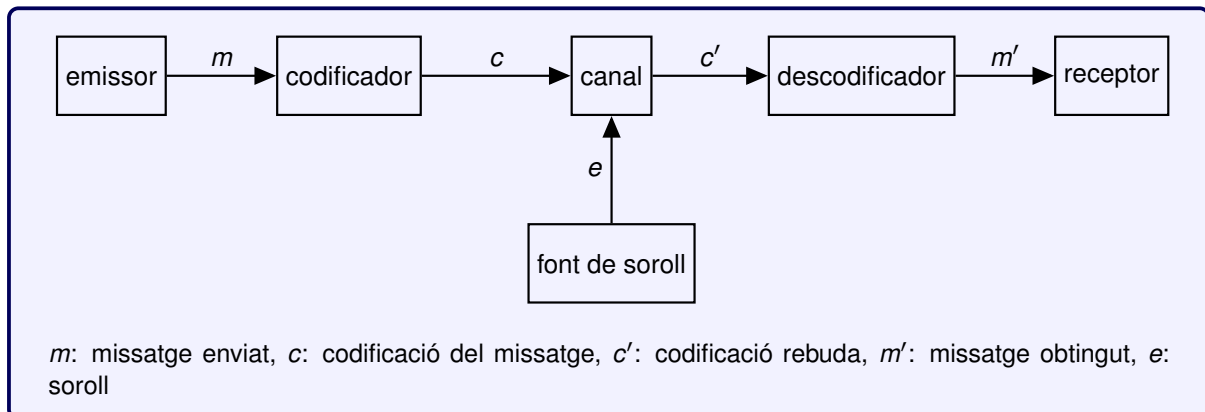
Perquè la comunicació sigui satisfactòria, el que volem és que el receptor pugui conèixer m .

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.



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.

5.2 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 78

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.124)

Si $q = 2$, aleshores diem que el codi és **binari**, mentre que si $q = 3$, aleshores diem que el codi és **ternari**.

Exercici 79

Com és el codi $C = \{(000), (111), (101), (010)\}$ de l'exercici anterior?

Solució (p.125)

La **dimensió** k del codi és la dimensió del subespai.

Exercici 80

Quina seria la dimensió del codi

$$C = \{(000), (111), (101), (010)\} \subseteq \mathbb{F}_2^3? \quad \text{Solució (p.125)}$$

La **taxa de transmissió** és $\frac{k}{n}$. La **codimensió** és $n - k$.

Exercici 81

Quines serien la taxa de transmissió i la codimensió del codi $C = \{(000), (111), (101), (010)\} \subseteq \mathbb{F}_2^3$?

Solució (p.125)

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 82

Doneu una matriu generadora del codi
 $C = \{(000), (111), (101), (010)\} \subseteq \mathbb{F}_2^3$.

Solució (p.125)

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:

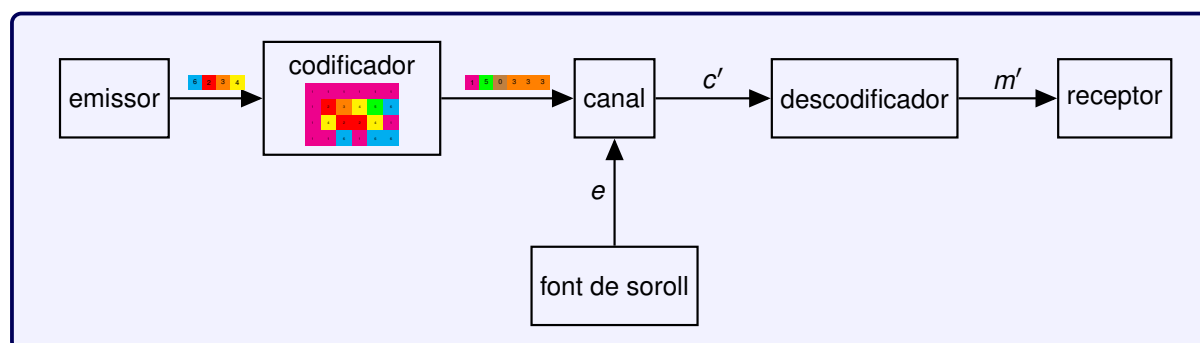
$$\mathbb{Z}_7 = \{ \text{0}, \text{1}, \text{2}, \text{3}, \text{4}, \text{5}, \text{6} \}$$

Considerem el codi generat per la matriu

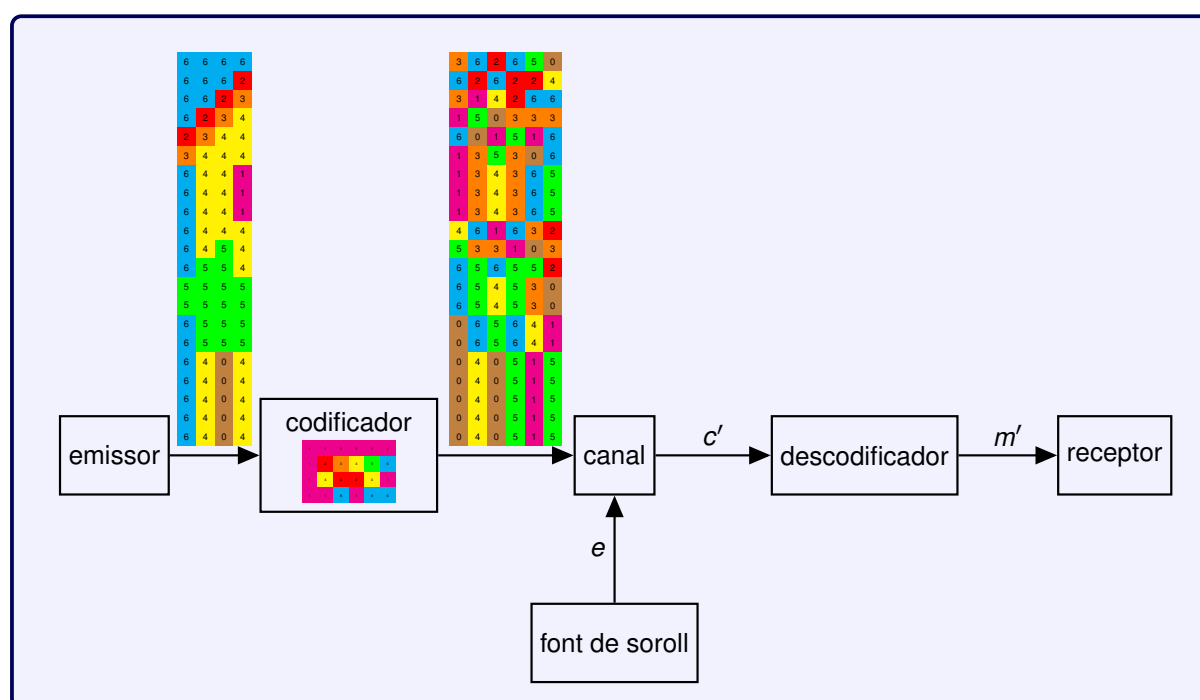
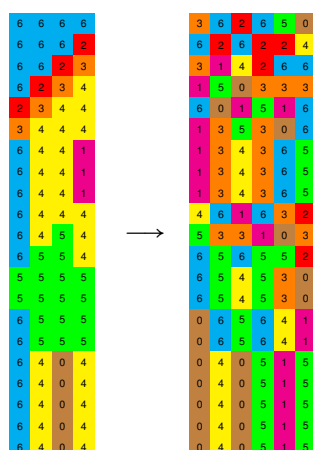
$$G = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 2 & 3 & 4 & 5 & 6 & 6 \\ 1 & 4 & 2 & 2 & 4 & 1 & 1 \\ 1 & 1 & 6 & 1 & 6 & 6 & 1 \end{pmatrix}$$

Per codificar una paraula com 6 2 3 4 amb la matriu G , la multipliquem per G .

$$\begin{pmatrix} 6 & 2 & 3 & 4 \end{pmatrix} \cdot \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 2 & 3 & 4 & 5 & 6 & 6 \\ 1 & 4 & 2 & 2 & 4 & 1 & 1 \\ 1 & 1 & 6 & 1 & 6 & 6 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 5 & 0 & 3 & 3 & 3 \end{pmatrix}$$



Suposem que ara volem codificar la imatge següent. Codificarem cadascuna de les seves files.



Exercici 83

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.125)

► 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.132)

Exemple. Recordem l'exemple de **codi** sobre $\mathbb{Z}_7$.

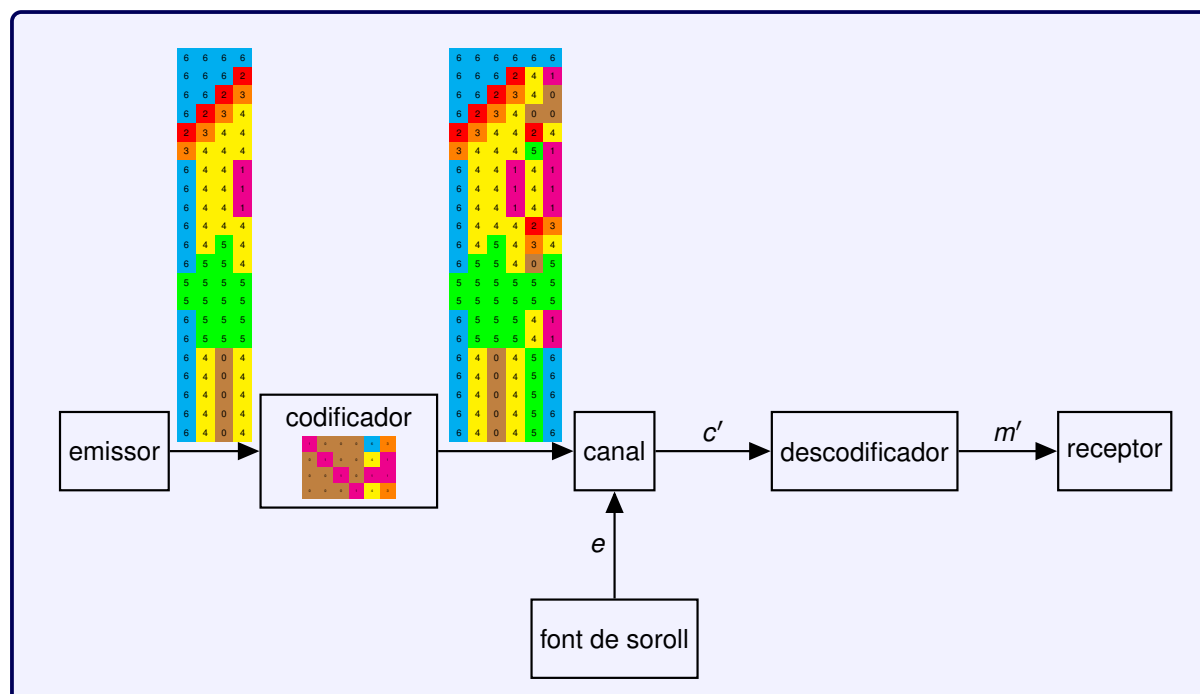
Una alternativa per codificar és fer servir la següent matriu sistemàtica equivalent a G :

$$G_s = \begin{pmatrix} 1 & 0 & 0 & 0 & 6 & 3 \\ 0 & 1 & 0 & 0 & 4 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 4 & 3 \end{pmatrix}$$

Així, codificar una paraula com **6 2 3 4** serà

$$\begin{pmatrix} 6 & 2 & 3 & 4 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 & 0 & 0 & 6 & 3 \\ 0 & 1 & 0 & 0 & 4 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 4 & 3 \end{pmatrix} = \begin{pmatrix} 6 & 2 & 3 & 4 & 0 & 0 \end{pmatrix}$$

Ara, en codificar la imatge, què observem?



Més endavant utilitzarem aquest exemple per a la **detecció d'errors** (p.119) i per a la **error correction** (p.121).

Exercici 84

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.125)

Codificació en símbols i en dígets

En un cos finit de p^m elements distingim

- **dígets**: són els elements de $\mathbb{Z}_p$,
- **símbols**: són els elements de $\mathbb{F}_{p^m}$.

Cada símbol es pot representar amb m dígets mitjançant la notació vectorial.

Els dígets de $\mathbb{Z}_2$ també s'anomenen **bits**. Els dígets de $\mathbb{Z}_3$ també s'anomenen **trits**.

Exemple. Suposem que volem utilitzar un codi sobre $\mathbb{F}_9 = \mathbb{Z}_3[x]/x^2 + 2x + 2$. Si diem α a la classe de x , tenim la taula d'equivalències següent:

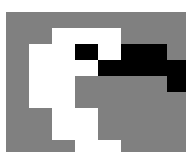
exp.	vect.
0	00
α^0	10
α^1	01
α^2	11
α^3	12
α^4	20
α^5	02
α^6	22
α^7	21

$\uparrow$ $\uparrow$
símbols **parelles de dígets**

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 dígit 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	2	1	1	1	0
1	1	2	2	1	1	1	1
1	1	2	2	1	1	1	1
1	1	1	2	2	1	1	1

I agrupem cada $m = 2$ dígit per formar un símbol, mitjançant la taula d'equivalències anterior.

$$\begin{array}{cccc}
 \begin{array}{cc} 1 & 1 \\ 1 & 1 \\ 1 & 2 \\ 1 & 2 \\ 1 & 2 \\ 1 & 1 \\ 1 & 1 \\ 1 & 1 \end{array} &
 \begin{array}{cc} 1 & 1 \\ 2 & 2 \\ 2 & 0 \\ 2 & 2 \\ 2 & 1 \\ 2 & 2 \\ 2 & 2 \\ 1 & 2 \end{array} &
 \begin{array}{cc} 1 & 1 \\ 2 & 1 \\ 2 & 0 \\ 0 & 0 \\ 1 & 1 \\ 1 & 1 \\ 1 & 1 \\ 2 & 1 \end{array} &
 \begin{array}{cc} 1 & 1 \\ 1 & 1 \\ 0 & 1 \\ 0 & 0 \\ 1 & 0 \\ 1 & 1 \\ 1 & 1 \\ 1 & 1 \end{array}
 \end{array}
 \leftrightarrow
 \begin{pmatrix}
 \alpha^2 & \alpha^2 & \alpha^2 & \alpha^2 \\
 \alpha^2 & \alpha^6 & \alpha^7 & \alpha^2 \\
 \alpha^3 & \alpha^4 & \alpha^4 & \alpha \\
 \alpha^3 & \alpha^6 & 0 & 0 \\
 \alpha^3 & \alpha^7 & \alpha^2 & 1 \\
 \alpha^3 & \alpha^7 & \alpha^2 & \alpha^2 \\
 \alpha^2 & \alpha^6 & \alpha^2 & \alpha^2 \\
 \alpha^2 & \alpha^3 & \alpha^7 & \alpha^2
 \end{pmatrix}$$

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 dígit que li correspon i obtenim la imatge codificada.

$$\begin{pmatrix}
 \alpha^2 & \alpha^2 & \alpha^2 & \alpha^2 & \alpha^2 & \alpha^2 & \alpha^2 & \alpha^2 \\
 \alpha^2 & \alpha^7 & \alpha^4 & \alpha^3 & \alpha^2 & \alpha^6 & \alpha^7 & \alpha^2 \\
 \alpha^3 & \alpha & \alpha & \alpha^4 & \alpha^3 & \alpha^4 & \alpha^4 & \alpha \\
 1 & \alpha^2 & \alpha^4 & \alpha^3 & \alpha^3 & \alpha^6 & 0 & 0 \\
 \alpha^5 & \alpha^4 & 0 & \alpha & \alpha^3 & \alpha^7 & \alpha^2 & 1 \\
 1 & \alpha^2 & \alpha^5 & \alpha^6 & \alpha^3 & \alpha^7 & \alpha^2 & \alpha^2 \\
 0 & \alpha^6 & 0 & 0 & \alpha^2 & \alpha^6 & \alpha^2 & \alpha^2 \\
 \alpha^7 & \alpha^2 & 0 & \alpha^6 & \alpha^2 & \alpha^3 & \alpha^7 & \alpha^2
 \end{pmatrix}
 \rightarrow
 \begin{array}{cccccccccccccccccccc}
 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
 1 & 1 & 2 & 1 & 2 & 0 & 1 & 2 & 1 & 1 & 2 & 2 & 2 & 1 & 1 & 1 & 1 \\
 1 & 2 & 0 & 1 & 0 & 1 & 2 & 0 & 1 & 2 & 2 & 0 & 2 & 0 & 0 & 1 & 1 \\
 1 & 0 & 1 & 1 & 2 & 0 & 1 & 2 & 1 & 2 & 2 & 2 & 0 & 0 & 0 & 0 & 0 \\
 0 & 2 & 2 & 0 & 0 & 0 & 0 & 1 & 1 & 2 & 2 & 1 & 1 & 1 & 1 & 0 & 1 \\
 1 & 0 & 1 & 1 & 0 & 2 & 2 & 2 & 1 & 2 & 2 & 1 & 1 & 1 & 1 & 1 & 1 \\
 0 & 0 & 2 & 2 & 0 & 0 & 0 & 0 & 1 & 1 & 2 & 2 & 1 & 1 & 1 & 1 & 1 \\
 0 & 0 & 2 & 2 & 0 & 0 & 0 & 0 & 1 & 1 & 2 & 2 & 1 & 1 & 1 & 1 & 1 \\
 2 & 1 & 1 & 1 & 0 & 0 & 2 & 2 & 1 & 1 & 1 & 2 & 2 & 1 & 1 & 1 & 1
 \end{array}$$

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.133) 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 $(x_1, \dots, x_6)$ que són solucions de

$$\begin{array}{cccccc} 2x_1 & +2x_2 & & +2x_4 & +x_5 & +x_6 & = 0 \\ 2x_1 & & +x_3 & +x_4 & +2x_5 & +2x_6 & = 0 \\ x_1 & +2x_2 & & +2x_4 & +x_5 & & = 0 \end{array}$$

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.132)

Exercici 85

Considerem el codi ternari de l'Exercici 84 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.126)

Exercici 86

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.126)

5.3 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.

$$d_H(CERT, CART) = 1$$

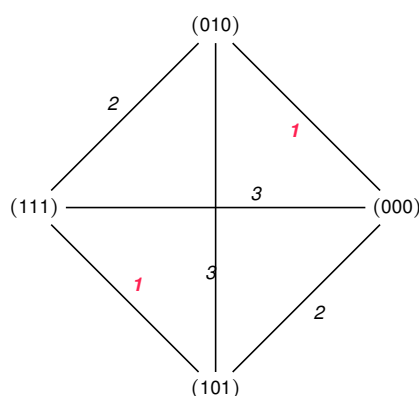
$$d_H(FALS, CART) = 3$$

$$d_H(CERT, CALT) = 2$$

$$d_H(FALS, CALT) = 2$$

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 de H linealment dependents.

Justificació de l'equivalència

Les dues primeres definicions són equivalents pel fet que C és un espai vectorial i pel fet que $d(u, v) = w(u - v)$.

La darrera definició es dedueix del fet que si una paraula c té pes w amb coordenades no nul·les en les posicions $i_1, \dots, i_w$, aleshores el producte de la matriu de control per c és una combinació lineal nul·la de les columnes en posició $i_1, \dots, i_w$ de la matriu de control. En aquest cas, les columnes de H en les posicions $i_1, \dots, i_w$ són linealment dependents.

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

$$k \leq n - d + 1.$$

Demostració. Com que una matriu de control té $n - k$ files, sabem que qualsevol conjunt de $n - k + 1$ columnes de la matriu de control seran linealment dependents. La fita es dedueix pel fet que la distància mínima és el mínim nombre de columnes linealment dependents d'una matriu de control. $\square$

Exercici 87

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.127)

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 .

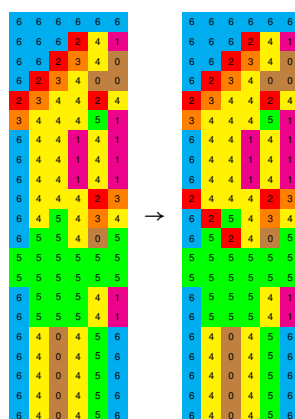
$$\begin{pmatrix} 3 & 1 & 3 & 2 & 1 \\ 4 & 1 & 0 & 4 & 1 \\ 3 & 2 & 2 & 0 & 3 \end{pmatrix} \begin{pmatrix} 1 \\ 1 \\ 1 \\ 1 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix} \Rightarrow \text{paraula de } C$$

$$\begin{pmatrix} 3 & 1 & 3 & 2 & 1 \\ 4 & 1 & 0 & 4 & 1 \\ 3 & 2 & 2 & 0 & 3 \end{pmatrix} \begin{pmatrix} 0 \\ 1 \\ 2 \\ 3 \\ 4 \end{pmatrix} = \begin{pmatrix} 2 \\ 2 \\ 3 \end{pmatrix} \neq \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix} \Rightarrow \text{error detectat}$$

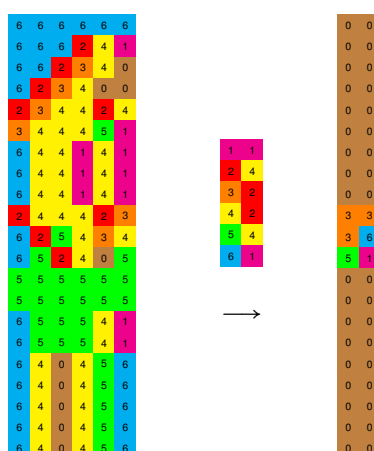
Exemple. Una matriu de control del **codi** que havíem vist és

$$H = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 4 & 2 & 2 & 4 & 1 \end{pmatrix}$$

Suposem que se'ns embruta la imatge codificada:



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).



Allà on el resultat és diferent de zero és on hi ha errors.

Exercici 88

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

011111010011001000000000.

Solució (p.127)

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 sistema 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.

Substituïm els esborralls per incògnites: (324xy) i resollem 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

$$\begin{aligned} 3 + 2x + y &= 0 & \implies 2x + 1 &= 0 & \implies x &= 2 \\ 4 + 4x + y &= 0 \\ 1 + 3y &= 0 & \implies y &= 3 \end{aligned}$$

que té solució $x = 2$ i $y = 3$. Per tant, la paraula corregida és (32423).

Exercici 89

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.128)

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:

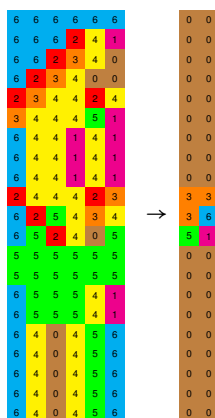
Si només es produeix un error, aleshores

- $e = (0, \dots, 0, e_i, 0, \dots, 0)$,
- $s = H \cdot u = h_i e_i$, on h_i és la columna i -èssima de H .

Aleshores

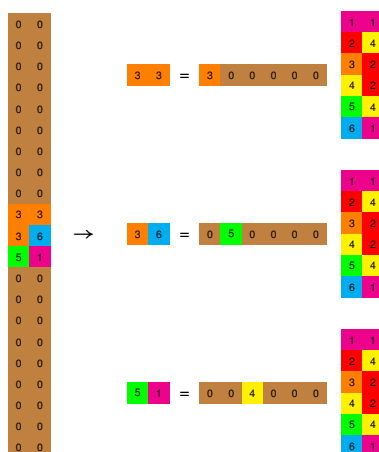
- buscant quina columna de H és un múltiple de s , tindrem la **posició d'error**,
- buscant l'únic valor e_i tal que $s = h_i e_i$, tindrem el **valor de l'error**.

Exemple. Continuem amb el **codi** que havíem vist.



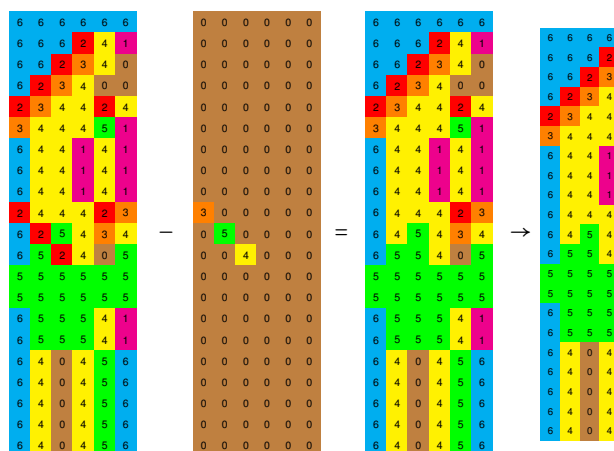
Havíem calculat les síndromes.

Per trobar el valor dels errors, vegem que les síndromes són múltiples de columnes de H :



Deduïm que les paraules d'error són $3\ 0\ 0\ 0\ 0\ 0\ 0\ 0$ $0\ 5\ 0\ 0\ 0\ 0\ 0\ 0$ $0\ 0\ 4\ 0\ 0\ 0\ 0\ 0$

Restem les paraules d'error de les paraules rebudes



I descodifiquem per la part sistemàtica.

Exercici 90

Utilitzem el codi dels Exercicis 84 i 85.
 Useu la síndrome per descodificar el vector rebut 212121.

Solució (p.129)

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 $\alpha_{i_1} h_{i_1} + \dots + \alpha_{i_r} h_{i_r}$ 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 91

Utilitzem el codi dels Exercicis 84 i 85.
 Useu la síndrome per corregir els vectors rebuts

1. 120102, Solució (p.130)
2. 222222. Solució (p.130)

Exercici 92

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.130)

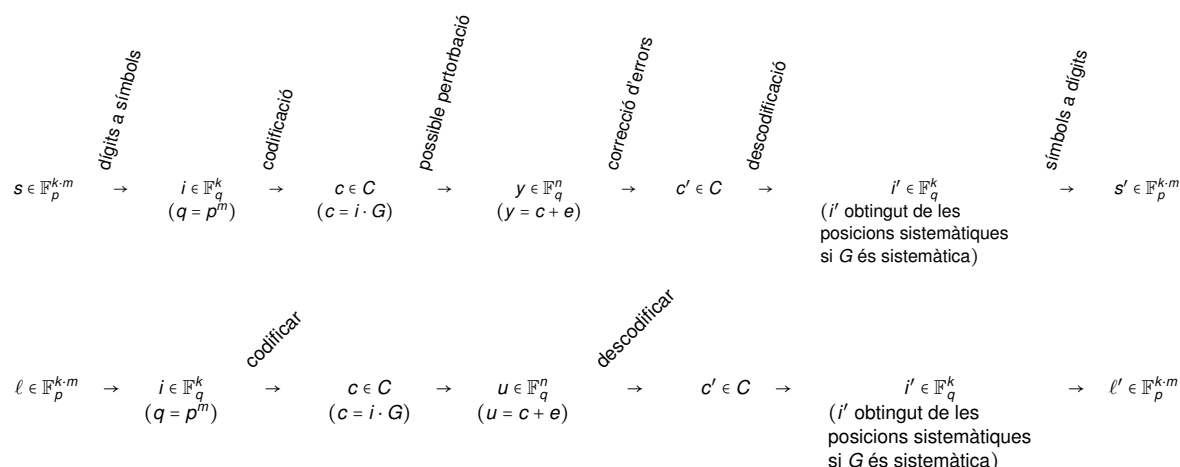
Exercici 93

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.130)

Procés de codificació-descodificació**5.4 Solucions****Solució de l'Exercici 78**

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,

$$\begin{array}{rclcl}
 (000) & + & (000) & = & (000) \in C \\
 (000) & + & (111) & = & (111) \in C \\
 (000) & + & (101) & = & (101) \in C \\
 (000) & + & (010) & = & (010) \in C \\
 (111) & + & (111) & = & (000) \in C \\
 (111) & + & (101) & = & (010) \in C \\
 (111) & + & (010) & = & (101) \in C \\
 (101) & + & (101) & = & (000) \in C \\
 (101) & + & (010) & = & (111) \in C \\
 (010) & + & (010) & = & (000) \in C
 \end{array}$$

Torna a l'exercici (p.109)

Solució de l'Exercici 79

Es tracta d'un codi binari.

Torna a l'exercici (p.109)

Solució de l'Exercici 80

$$k = 2$$

Torna a l'exercici (p.109)

Solució de l'Exercici 81

$$\frac{k}{n} = 0.666, \quad n - k = 1$$

Torna a l'exercici (p.109)

Solució de l'Exercici 82

Per exemple,

$$G = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix},$$

$$\text{però també } \begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 1 & 1 \\ 1 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 1 \end{pmatrix} \dots$$

Torna a l'exercici (p.110)

Solució de l'Exercici 83

Vegem com la matriu G genera tot C :

$$\begin{array}{rcl}
 (0 \ 0) & \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix} & = (0 \ 0 \ 0) \\
 (1 \ 1) & \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix} & = (1 \ 1 \ 1) \\
 (1 \ 0) & \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix} & = (1 \ 0 \ 1) \\
 (0 \ 1) & \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix} & = (0 \ 1 \ 0)
 \end{array}$$

Torna a l'exercici (p.111)

Solució de l'Exercici 84

Busquem la matriu equivalent sistemàtica per l'esquerra:

$$\begin{pmatrix} 2 & 2 & 0 & 2 & 1 & 1 \\ 2 & 0 & 1 & 1 & 2 & 2 \\ 1 & 2 & 0 & 2 & 1 & 0 \end{pmatrix} \sim \begin{matrix} f'_1 = 2f_1 \\ f'_2 = 2f_1 + f_2 \\ f'_3 = f_1 + f_3 \end{matrix} \begin{pmatrix} 1 & 1 & 0 & 1 & 2 & 2 \\ 0 & 1 & 1 & 2 & 1 & 1 \\ 0 & 1 & 0 & 1 & 2 & 1 \end{pmatrix} \sim \begin{matrix} f'_1 = f_1 + 2f_2 \\ f'_3 = 2f_2 + f_3 \end{matrix} \begin{pmatrix} 1 & 0 & 2 & 2 & 1 & 1 \\ 0 & 1 & 1 & 2 & 1 & 1 \\ 0 & 0 & 2 & 2 & 1 & 0 \end{pmatrix} \sim \begin{matrix} f'_1 = f_1 + 2f_3 \\ f'_2 = f_2 + f_3 \\ f'_3 = 2f_3 \end{matrix} \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 2 & 1 \\ 0 & 0 & 1 & 1 & 2 & 0 \end{pmatrix}$$

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.113)

Solució de l'Exercici 85

En la resolució de l'Exercici 84 (p.125) 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

$$I = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \text{ i } P = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 2 & 1 \\ 1 & 2 & 0 \end{pmatrix}$$

$$\text{Ara tindrem } P^T = \begin{pmatrix} 0 & 1 & 1 \\ 0 & 2 & 2 \\ 1 & 1 & 0 \end{pmatrix} \text{ i } -P^T = \begin{pmatrix} 0 & 2 & 2 \\ 0 & 1 & 1 \\ 2 & 2 & 0 \end{pmatrix}$$

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.115)

Solució de l'Exercici 86

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.116)

Solució de l'Exercici 87

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.118)

Solució de l'Exercici 88

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.

$$\begin{array}{c|c} 0 & 00 \\ 1 & 10 \\ \alpha & 01 \\ \alpha^2 & 11 \end{array}$$

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.120)

Solució de l'Exercici 89

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 $\alpha\alpha^3x\alpha^6$. 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 \(p.121\)](#)

Solució de l'Exercici 90

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

$$(2 \ 1 \ 2 \ 1 \ 2 \ 1) - (0 \ 2 \ 0 \ 0 \ 0 \ 0) = (2 \ 2 \ 2 \ 1 \ 2 \ 1)$$

[Torna a l'exercici \(p.123\)](#)

Solució de l'Exercici 91(a)

En el primer cas, la síndrome és

$$\begin{pmatrix} 0 & 2 & 2 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 \\ 2 & 2 & 0 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 \\ 2 \\ 0 \\ 1 \\ 0 \\ 2 \end{pmatrix} = \begin{pmatrix} 2 \\ 2 \end{pmatrix}$$

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

$$(1 \ 2 \ 0 \ 1 \ 0 \ 2) - (0 \ 1 \ 0 \ 0 \ 1 \ 0) = (1 \ 1 \ 0 \ 1 \ 2 \ 2)$$

Torna a l'exercici (p.123)

Solució de l'Exercici 91(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

$$(2 \ 2 \ 2 \ 2 \ 2 \ 2) - (0 \ 0 \ 0 \ 1 \ 0 \ 1) = (2 \ 2 \ 2 \ 1 \ 2 \ 1)$$

o bé

$$(2 \ 2 \ 2 \ 2 \ 2 \ 2) - (0 \ 2 \ 0 \ 0 \ 1 \ 0) = (2 \ 0 \ 2 \ 2 \ 1 \ 2)$$

Torna a l'exercici (p.123)

Solució de l'Exercici 92

1. 3.
2. 3.
3. 1132321031.

Torna a l'exercici (p.123)

Solució de l'Exercici 93

6. 01110101.
7. 01.

Torna a l'exercici (p.124)

5.5 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 neutre** $\mathbf{0} \in V$ 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 $\mathbf{v} \in V$, aleshores $\alpha \mathbf{v} \in V$.
- Si $\mathbf{v}_1, \mathbf{v}_2 \in V$, aleshores $\mathbf{v}_1 + \mathbf{v}_2 \in V$.

Relacionat: codi lineal (p.109)

Definició

Sigui V un espai vectorial i $\mathbf{x}_1, \dots, \mathbf{x}_n \in V$. Diem que $\mathbf{x}_1, \dots, \mathbf{x}_n$ són **linealment dependents** si existeixen $\alpha_1, \dots, \alpha_n \in \mathbb{F}$ no tots nuls pels quals

$$\alpha_1 \mathbf{x}_1 + \dots + \alpha_n \mathbf{x}_n = \mathbf{0}.$$

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.117)

Definició

Un conjunt $\{\mathbf{x}_1, \dots, \mathbf{x}_n\} \subseteq V$ és un **sistema de generadors** d'un subespai vectorial S si tot element de S es pot escriure com a combinació lineal de $\mathbf{x}_1, \dots, \mathbf{x}_n$.

Definició

Un conjunt $\{\mathbf{x}_1, \dots, \mathbf{x}_n\} \subseteq V$ és una **base** del subespai vectorial S si és un sistema de generadors que és linealment independent. Relacionat: matriu generadora (p.110)

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.109)

Definició

Si E és un K -subespai vectorial de F i $\dim F = n$, aleshores un **sistema d'equacions implícites** 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 $\{j_1, \dots, j_k\}$ (posicions sistemàtiques) és una base $S = \{s_1, \dots, s_k\}$ on

- $(\text{coord}_B(s_i))_{j_r} = 0$ per tot $r \neq i$
- $(\text{coord}_B(s_i))_{j_i} = 1$.

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 $(\text{coord}_B(s_i))_l = 0$ for all $l < j_i$. Aquesta base s'obté per transformacions gaussianes.

Relacionat: matriu generadora sistemàtica (p.112)

Diem G a la matriu $k \times n$ següent:

$$\begin{pmatrix} \leftarrow & \text{coord}_B(s_1) & \rightarrow \\ & \vdots & \\ \leftarrow & \text{coord}_B(s_k) & \rightarrow \end{pmatrix}.$$

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 anomenar $\tilde{G}$, que té l'element de la fila r i columna "corresponent a" l igual a $(\text{coord}_B(s_r))_l$.

Els elements de E seran combinacions lineals dels elements de S i tindran la forma $u = \lambda_1 s_1, \dots, \lambda_k s_k = (\lambda_1 \dots \lambda_k)G$. Si diem $(x_1, \dots, x_n) = \text{coord}_B(u)$, aleshores, $x_{j_i} = \lambda_i$, per tota posició sistemàtica j_i , mentre que per les posicions no sistemàtiques, $x_l = \sum_i \lambda_i (\text{coord}_B(s_i))_l = \sum_i (\text{coord}_B(s_i))_l x_{j_i}$. Això ens permet obtenir un sistema de $n - k$ equacions implícites d'un subespai a partir de la base sistemàtica on les equacions són $-\sum_i (\text{coord}_B(s_i))_l x_{j_i} + x_l = 0$ per tot $l \notin \{j_1, \dots, j_k\}$. 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 $-(\text{coord}_B(s_r))_l$, és a dir, la submatriu és $-\tilde{G}^T$.

Relacionat: matrius generadores i de control sistemàtiques (p.115)

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.114)

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 **transposada**.

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,

$$\begin{pmatrix} 5 & 1 & 3 \\ 9 & 8 & 2 \end{pmatrix} \begin{pmatrix} 4 & 1 \\ 6 & 3 \\ 5 & 2 \end{pmatrix} = \begin{pmatrix} 41 & 14 \\ 94 & 37 \end{pmatrix}.$$

6 Codis cíclics

6.1 Matrius de Vandermonde I

- 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 $v_1, v_2, \dots, v_n \in \mathbb{F}_q$, la **matriu de Vandermonde** de $v_1, \dots, v_n$ d'ordre r es defineix com

$$V_r(v_1, v_2, \dots, v_n) = \begin{pmatrix} 1 & 1 & \dots & 1 \\ v_1 & v_2 & \dots & v_n \\ v_1^2 & v_2^2 & \dots & v_n^2 \\ \vdots & \vdots & \ddots & \vdots \\ v_1^{r-1} & v_2^{r-1} & \dots & v_n^{r-1} \end{pmatrix}$$

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 30

El determinant de la matriu de Vandermonde $V_n(v_1, v_2, \dots, v_n)$ és igual a

$$\det(V_n(v_1, v_2, \dots, v_n)) = \prod_{1 \leq i < j \leq n} (v_j - v_i)$$

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 $\begin{vmatrix} 1 & 1 \\ v_1 & v_2 \end{vmatrix} = v_2 - v_1$.

$$\text{Per } n > 2, \quad |V_n(v_1, v_2, \dots, v_n)| = \begin{vmatrix} 1 & 1 & \dots & 1 \\ v_1 & v_2 & \dots & v_n \\ v_1^2 & v_2^2 & \dots & v_n^2 \\ \vdots & \vdots & \ddots & \vdots \\ v_1^{n-1} & v_2^{n-1} & \dots & v_n^{n-1} \end{vmatrix}.$$

Per cada $i \geq 2$, podem restar a la i -èssima fila l'anterior fila multiplicada per v_1 i obtenir així

$$\begin{vmatrix} 1 & 1 & \dots & 1 \\ 0 & v_2 - v_1 & \dots & v_n - v_1 \\ 0 & v_2^2 - v_1 v_2 & \dots & v_n^2 - v_1 v_n \\ \vdots & \vdots & \ddots & \vdots \\ 0 & v_2^{n-1} - v_1 v_2^{n-2} & \dots & v_n^{n-1} - v_1 v_n^{n-2} \end{vmatrix} = \begin{vmatrix} v_2 - v_1 & \dots & v_n - v_1 \\ v_2(v_2 - v_1) & \dots & v_n(v_n - v_1) \\ \vdots & \vdots & \vdots \\ v_2^{n-2}(v_2 - v_1) & \dots & v_n^{n-2}(v_n - v_1) \end{vmatrix}.$$

Això és igual a $(v_2 - v_1) \cdots (v_n - v_1) |V_{n-1}(v_2, \dots, v_n)|$. I, per la hipòtesis d'inducció, és igual a $(v_2 - v_1) \cdots (v_n - v_1) \prod_{2 \leq i < j \leq n} (v_j - v_i) = \prod_{1 \leq i < j \leq n} (v_j - v_i)$. □

Exercici 94

A $\mathbb{F}_7$,

1. Calculeu la matriu de Vandermonde de rang 4 de 6, 5, 4, 3.
2. Calculeu el seu determinant menor] per menors .
3. Calculeu el seu determinant fent servir el lema i comproveu que coincideixen.

Solució (p.151)

Exercici 95

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 menor] per menors .
3. Calculeu el seu determinant fent servir el lema i comproveu que coincideixen.

Solució (p.151)

Exercici 96

Calculeu el determinant de $V_4(1, \alpha, \alpha^3, \alpha^4)$, on α és la classe de x de $\mathbb{F}_3[x]/x^2 + x + 2$.

- menor] Per menors .
- Pel resultat del lema.

Solució (p.152)

- 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, $\det(V_n(v_1, v_2, \dots, v_n)) = 0$ si i només si $v_i = v_j$ per algun $i \neq j$.
- Obtenim, així, el següent corol·lari:

Corol·lari 2

La matriu $V_n(v_1, v_2, \dots, v_n)$ és invertible si i només si $v_i \neq v_j$ per tot $1 \leq i < j \leq n$.

- Així, agafant $v_i \neq v_j$ per tot $1 \leq i < j \leq n$, podem garantir que $V_n(v_1, v_2, \dots, v_n)$ té rang n .

6.2 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  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 97

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.153)

Exercici 98

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.154)

Polinomi generador

Per treballar amb codis cíclics, identifiquem els vectors amb polinomis

$$(v_0, v_1, \dots, v_{n-1}) \leftrightarrow v_0 + v_1x + v_2x^2 + \dots + v_{n-1}x^{n-1}.$$

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 identificariem amb polinomis de la manera següent:

$$\begin{array}{ll} 0000 & \longrightarrow 0 + 0x + 0x^2 + 0x^3 = 0 \\ 0101 & \longrightarrow 0 + 1x + 0x^2 + 1x^3 = x + x^3 \\ 1010 & \longrightarrow 1 + 0x + 1x^2 + 0x^3 = 1 + x^2 \\ 1111 & \longrightarrow 1 + 1x + 1x^2 + 1x^3 = 1 + x + x^2 + x^3 \end{array}$$

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 31: 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 $g(x) = g_0 + g_1x + g_2x^2 + \dots + g_rx^r$, 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 mòncics 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 $i + \text{grau}(g) < n$, 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 corresponent al conjunt de polinomis $\{a(x)g(x) : a(x) \in \mathbb{F}_q[x], \text{ amb } \text{grau}(a(x)) < n - r\}$ és un codi cíclic de dimensió $n - r$.

Exercici 99

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.154)

Matrius generadores

Una matriu té **forma de cascada** (de grau r) si és de la forma

$$A = \begin{pmatrix} a_0 & a_1 & \dots & a_r & 0 & \dots & 0 \\ 0 & a_0 & a_1 & \dots & a_r & 0 & 0 \\ 0 & 0 & a_0 & a_1 & \dots & a_r & 0 \\ \vdots & & \ddots & & & & \ddots \\ 0 & \dots & & 0 & a_0 & a_1 & \dots & a_r \end{pmatrix}$$

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 superdiagonal 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,

$$A = \left(\begin{array}{cccc|cccc} a_0 & a_1 & \dots & a_r & 0 & \dots & 0 & \dots \\ 0 & a_0 & a_1 & \dots & a_r & \dots & 0 & \dots \\ 0 & 0 & a_0 & a_1 & \dots & a_r & 0 & \dots \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & \dots & \dots & a_0 & a_1 & \dots & a_r & \dots \\ 0 & \dots & \dots & 0 & a_0 & a_1 & \dots & a_r \end{array} \right) \text{ si } r < k \quad \text{o bé} \quad A = \left(\begin{array}{cccc|cccc} a_0 & a_1 & \dots & a_{k-1} & \dots & a_{k-1} & \dots & a_{k-1} \\ 0 & a_0 & a_1 & \dots & a_{k-2} & \dots & a_{k-2} & \dots \\ 0 & 0 & a_0 & a_1 & \dots & a_{k-3} & \dots & a_{k-3} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & \dots & \dots & 0 & a_0 & a_1 & \dots & a_r \end{array} \right) \text{ si } r \geq k$$

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.

$$\begin{pmatrix} 1 & 0 & 0 & 1 & 3 \\ 0 & 1 & 0 & 0 & 2 \\ 0 & 0 & 1 & 3 & 4 \end{pmatrix} \sim f'_1 = f_1 + 3f_2 \quad \begin{pmatrix} 1 & 3 & 0 & 1 & 2 \\ 0 & 1 & 0 & 0 & 2 \\ 0 & 0 & 1 & 3 & 4 \end{pmatrix} \sim \begin{matrix} f'_1 = f_1 + 4f_3 \\ f'_2 = f_2 + 3f_3 \end{matrix} \quad \begin{pmatrix} 1 & 3 & 4 & 6 & 4 \\ 0 & 1 & 3 & 2 & 0 \\ 0 & 0 & 1 & 3 & 4 \end{pmatrix}$$

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

$$Q = \left(\begin{array}{cccc|cccc} a_0 & a_1 & \dots & a_r & 0 & \dots & 0 & \dots \\ 0 & a_0 & a_1 & \dots & a_r & \dots & 0 & \dots \\ 0 & 0 & a_0 & a_1 & \dots & a_r & 0 & \dots \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ \vdots & \vdots & \vdots & \vdots & a_0 & a_1 & \dots & a_r \\ 0 & \dots & \dots & 0 & a_0 & a_1 & \dots & a_r \end{array} \right) \text{ si } r < k \quad \text{o bé} \quad Q = \left(\begin{array}{cccc|cccc} a_0 & a_1 & \dots & a_{k-1} & \dots & a_{k-1} & \dots & a_{k-1} \\ 0 & a_0 & a_1 & \dots & a_{k-2} & \dots & a_{k-2} & \dots \\ 0 & 0 & a_0 & a_1 & \dots & a_{k-3} & \dots & a_{k-3} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & \dots & \dots & 0 & a_0 & a_1 & \dots & a_r \end{array} \right) \text{ si } r \geq k$$

El producte de matrius $Q(I|P)$ és equivalent també a $(I|P)$ i té forma de precascada normalitzada.

Exemple. En l'exemple anterior tindríem $Q = \begin{pmatrix} 1 & 3 & 4 \\ 0 & 1 & 3 \\ 0 & 0 & 1 \end{pmatrix}$

$$i \quad QA = \begin{pmatrix} 1 & 3 & 4 \\ 0 & 1 & 3 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 & 1 & 3 \\ 0 & 1 & 0 & 0 & 2 \\ 0 & 0 & 1 & 3 & 4 \end{pmatrix} = \begin{pmatrix} 1 & 3 & 4 & 6 & 4 \\ 0 & 1 & 3 & 2 & 0 \\ 0 & 0 & 1 & 3 & 4 \end{pmatrix}.$$

Lema 32

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, $G \sim (I|P)$ 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 $1 + a_1x + \dots + a_{n-k}x^{n-k}$ divideix $x^n - 1$.

En aquest cas, el polinomi generador del codi és $a_{n-k}^{-1}(1 + a_1x + \dots + a_{n-k}x^{n-k})$.

Exercici 100

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.155)

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 101

Demostreu que en aquest cas $x - \beta$ divideix $x^n - 1$ per a tot $\beta \in \mathbb{F}_q^*$.

Solució (p.156)

Exercici 102

Demostreu que si $\alpha_1, \dots, \alpha_r$ són elements de $\mathbb{F}_q \setminus \{0\}$ diferents entre ells, aleshores $(x - \alpha_1) \cdots (x - \alpha_r)$ és el polinomi generador d'un codi cíclic primitiu definit a $\mathbb{F}_q$.

Solució (p.156)

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 $(x - \alpha_1) \cdot (x - \alpha_2) \cdots (x - \alpha_r)$ 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

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

Com que $\alpha, \alpha^2, \alpha^3$ són tots diferents, considerem el polinomi

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

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

$$v(x) \in C \iff v(x)h(x) = 0 \pmod{x^n - 1}.$$

Exercici 103

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.156)

Exercici 104Sobre $\mathbb{F}_2$ 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.158)

Matrius de controlUna 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 $v(\beta_1), v(\beta_2), v(\beta_3) \dots$

Justificació de la segona matriu de control

Suposem que $c(x) = c_0 + c_1x + c_2x^2 + \dots + c_{n-1}x^{n-1}$ i $h(x) = h_0 + h_1x + \dots + h_kx^k$.

Sabem que $c(x)$ és una paraula del codi si i només si $c(x)h(x) = 0 \pmod{x^n - 1}$.

Com que el grau de $c(x)h(x)$ és com a molt $n + k - 1$, aleshores $c(x)h(x)$ serà un producte $(x^n - 1)p(x)$ amb $p(x)$ un polinomi de grau com a molt $k - 1$.

Però en aquest cas, $(x^n - 1)p(x)$ és la suma de $-p(x)$ que només té coeficients de graus entre 0 i $k - 1$ i de $x^n p(x)$ que només té coeficients de graus entre n i $n + k - 1$.

Per això els coeficients de $c(x)h(x)$ de graus entre k i $n - 1$ seran tots nuls. Ara només queda observar que els coeficients de graus k fins a $n - 1$ són, respectivament,

$$\begin{aligned} \text{grau } k : \quad c_0h_k + c_1h_{k-1} + \dots + c_kh_0 &= \begin{pmatrix} h_k & \dots & h_0 & 0 & \dots & 0 \end{pmatrix} \begin{pmatrix} c_0 \\ \vdots \\ c_{n-1} \end{pmatrix} \\ \text{grau } k + 1 : \quad c_1h_k + c_2h_{k-1} + \dots + c_{k+1}h_0 &= \begin{pmatrix} 0 & h_k & \dots & h_0 & 0 & \dots & 0 \end{pmatrix} \begin{pmatrix} c_0 \\ \vdots \\ c_{n-1} \end{pmatrix} \\ &\vdots \\ \text{grau } n - 1 : \quad c_{n-k-1}h_k + c_{n-k}h_{k-1} + \dots + c_{n-1}h_0 &= \begin{pmatrix} 0 & \dots & 0 & h_k & \dots & h_0 \end{pmatrix} \begin{pmatrix} c_0 \\ \vdots \\ c_{n-1} \end{pmatrix} \end{aligned}$$

Justificació de la tercera matriu de control

Suposem que $c(x) = c_0 + c_1x + c_2x^2 + \dots + c_{n-1}x^{n-1}$.

Sabem que $c(x)$ és una paraula del codi si i només si és divisible per $g(x)$.

Per això, si $g(x) = (x - \beta_1) \dots (x - \beta_{n-k})$, aleshores $\beta_1, \dots, \beta_{n-k}$ han de ser arrels de $c(x)$.

I, per això, $c(\beta_1) = c(\beta_2) = \dots = c(\beta_{n-k}) = 0$.

Però resulta que

$$\begin{aligned} c(\beta_1) &= c_0 + c_1\beta_1 + \dots + c_{n-1}\beta_1^{n-1} = \begin{pmatrix} 1 & \beta_1 & \beta_1^2 & \dots & \beta_1^{n-1} \end{pmatrix} \begin{pmatrix} c_0 \\ \vdots \\ c_{n-1} \end{pmatrix} \\ c(\beta_2) &= c_0 + c_1\beta_2 + \dots + c_{n-1}\beta_2^{n-1} = \begin{pmatrix} 1 & \beta_2 & \beta_2^2 & \dots & \beta_2^{n-1} \end{pmatrix} \begin{pmatrix} c_0 \\ \vdots \\ c_{n-1} \end{pmatrix} \\ &\vdots \\ c(\beta_{n-k}) &= c_0 + c_1\beta_{n-k} + \dots + c_{n-1}\beta_{n-k}^{n-1} = \begin{pmatrix} 1 & \beta_{n-k} & \beta_{n-k}^2 & \dots & \beta_{n-k}^{n-1} \end{pmatrix} \begin{pmatrix} c_0 \\ \vdots \\ c_{n-1} \end{pmatrix} \end{aligned}$$

Quedaria justificar que la matriu és de rang màxim. Això es dedueix de les propietats de les matrius de Vandermonde.

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 105

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.158)

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 33

Es compleix que, si d és la distància mínima real del codi, aleshores $d \geq \delta$.

Demostració. Considerem la matriu

$$\begin{pmatrix} 1 & \alpha^b & (\alpha^b)^2 & (\alpha^b)^3 & \dots & (\alpha^b)^{n-1} \\ 1 & \alpha^{b+1} & (\alpha^{b+1})^2 & (\alpha^{b+1})^3 & \dots & (\alpha^{b+1})^{n-1} \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \alpha^{b+\delta-2} & (\alpha^{b+\delta-2})^2 & (\alpha^{b+\delta-2})^3 & \dots & (\alpha^{b+\delta-2})^{n-1} \end{pmatrix}$$

Les seves primeres $\delta - 1$ columnes formen una matriu de Vandermonde transposada. Les seves files són per tant, linealment independents i, a més, són del codi dual. Per àlgebra lineal sabem que podem completar el conjunt d'aquestes files obtenint una base del codi dual o, equivalentment, les files d'una matriu de control de C .

Acabarem la demostració veient que qualsevol conjunt de $\delta - 1$ columnes d'aquesta matriu de control són linealment independents. Suposem que prenem les columnes corresponents als exponents $i_1, \dots, i_{\delta-1}$, amb tots aquests exponents entre 0 i $n - 1$. Les primeres $\delta - 1$ files de la matriu formada per aquest subconjunt de $\delta - 1$ columnes és de la forma

$$\begin{pmatrix} (\alpha^b)^{i_1} & (\alpha^b)^{i_2} & \dots & (\alpha^b)^{i_{\delta-1}} \\ (\alpha^{b+1})^{i_1} & (\alpha^{b+1})^{i_2} & \dots & (\alpha^{b+1})^{i_{\delta-1}} \\ \vdots & \vdots & \ddots & \vdots \\ (\alpha^{b+\delta-2})^{i_1} & (\alpha^{b+\delta-2})^{i_2} & \dots & (\alpha^{b+\delta-2})^{i_{\delta-1}} \end{pmatrix} = \begin{pmatrix} 1 & 1 & \dots & 1 \\ \alpha^{i_1} & \alpha^{i_2} & \dots & \alpha^{i_{\delta-1}} \\ \vdots & \vdots & \ddots & \vdots \\ \alpha^{i_1(\delta-2)} & \alpha^{i_2(\delta-2)} & \dots & \alpha^{i_{\delta-1}(\delta-2)} \end{pmatrix} \begin{pmatrix} \alpha^{bi_1} & 0 & \dots & 0 \\ 0 & \alpha^{bi_2} & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \dots & 0 & \alpha^{bi_{\delta-1}} \end{pmatrix},$$

que és de rang $\delta - 1$ si α és primitiu, ja que la primera matriu és Vandermonde amb totes les arrels diferents, mentre que la segona és diagonal sense zeros a la diagonal.

□

Exercici 106

Considerem el codi sobre $\mathbb{F}_2$ generat per la matriu

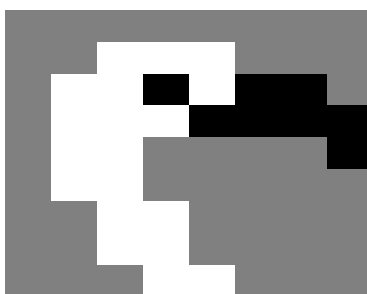
$$G = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}.$$

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.158)

6.3 L'exemple del faisà

Suposem una imatge digital.



La representem amb dígitos 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	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

α^2	α^2	α^2	α^2	$\alpha^2 + \alpha^2 x + \alpha^2 x^2 + \alpha^2 x^3$
α^2	α^6	α^7	α^2	$\alpha^2 + \alpha^6 x + \alpha^7 x^2 + \alpha^2 x^3$
α^3	α^4	α^4	α	$\alpha^3 + \alpha^4 x + \alpha^4 x^2 + \alpha x^3$
α^3	α^6	0	0	$\alpha^3 + \alpha^6 x$
α^3	α^7	α^2	1	$\alpha^3 + \alpha^7 x + \alpha^2 x^2 + x^3$
α^3	α^7	α^2	α^2	$\alpha^3 + \alpha^7 x + \alpha^2 x^2 + \alpha^2 x^3$
α^2	α^6	α^2	α^2	$\alpha^2 + \alpha^6 x + \alpha^2 x^2 + \alpha^2 x^3$
α^2	α^6	α^2	α^2	$\alpha^2 + \alpha^6 x + \alpha^2 x^2 + \alpha^2 x^3$
α^2	α^3	α^7	α^2	$\alpha^2 + \alpha^3 x + \alpha^7 x^2 + \alpha^2 x^3$

En multiplicar pel polinomi generador obtenim les paraules codificades.

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 $g(x)$ i ens queda $\alpha^4 + \alpha x + \alpha x^2 + \alpha^4 x^3 + \alpha^5 x^4 + \alpha^6 x^5 + \alpha x^6 + \alpha^2 x^7$.

$$i(x)g(x) = \alpha^2 g(x) + \alpha^3 x g(x) + \alpha^7 x^2 g(x) + \alpha^2 x^3 g(x)$$

$$\begin{aligned}
\alpha^2 g(x) &= \alpha^2 x^4 + \alpha^8 x^3 + \alpha^2 x^2 + \alpha^5 x + \alpha^4 \\
&= \alpha^2 x^4 + x^3 + \alpha^2 x^2 + \alpha^5 x + \alpha^4 \\
\alpha^3 x g(x) &= \alpha^3 x^5 + \alpha^9 x^4 + \alpha^3 x^3 + \alpha^6 x^2 + \alpha^5 x \\
&= \alpha^3 x^5 + \alpha x^4 + \alpha^3 x^3 + \alpha^6 x^2 + \alpha^5 x \\
\alpha^7 x^2 g(x) &= \alpha^7 x^6 + \alpha^{13} x^5 + \alpha^7 x^4 + \alpha^{10} x^3 + \alpha^9 x^2 \\
&= \alpha^7 x^6 + \alpha^5 x^5 + \alpha^7 x^4 + \alpha^2 x^3 + \alpha x^2 \\
\alpha^2 x^3 g(x) &= \alpha^2 x^7 + \alpha^8 x^6 + \alpha^2 x^5 + \alpha^5 x^4 + \alpha^4 x^3 \\
&= \alpha^2 x^7 + x^6 + \alpha^2 x^5 + \alpha^5 x^4 + \alpha^4 x^3
\end{aligned}$$

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

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

$$1 + \alpha^7 \rightarrow (1, 0) + (2, 1) = (0, 1) \rightarrow \alpha$$

El resultat és

$$\alpha^4 + \alpha x + \alpha x^2 + \alpha^4 x^3 + \alpha^5 x^4 + \alpha^6 x^5 + \alpha x^6 + \alpha^2 x^7.$$

Fem ara el mateix amb totes les files:

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

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

2	1	1	1	0	0	2	2	1	1	1	2	2	1	1	1
---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---

Fem ara el mateix amb totes les files:

$$\begin{array}{cccccccc}
 \alpha^2 & \alpha^2 & \alpha^2 & \alpha^2 & \alpha^2 & \alpha^2 & \alpha^2 & \alpha^2 \\
 \alpha^2 & \alpha^7 & \alpha^4 & \alpha^3 & \alpha^2 & \alpha^6 & \alpha^7 & \alpha^2 \\
 \alpha^3 & \alpha & \alpha & \alpha^4 & \alpha^3 & \alpha^4 & \alpha^4 & \alpha \\
 1 & \alpha^2 & \alpha^4 & \alpha^3 & \alpha^3 & \alpha^6 & 0 & 0 \\
 \alpha^5 & \alpha^4 & 0 & \alpha & \alpha^3 & \alpha^7 & \alpha^2 & 1 \\
 1 & \alpha^2 & \alpha^5 & \alpha^6 & \alpha^3 & \alpha^7 & \alpha^2 & \alpha^2 \\
 0 & \alpha^6 & 0 & 0 & \alpha^2 & \alpha^6 & \alpha^2 & \alpha^2 \\
 0 & \alpha^6 & 0 & 0 & \alpha^2 & \alpha^6 & \alpha^2 & \alpha^2 \\
 \alpha^7 & \alpha^2 & 0 & \alpha^6 & \alpha^2 & \alpha^3 & \alpha^7 & \alpha^2
 \end{array}
 \leftrightarrow
 \begin{array}{cccccccccccccccccccc}
 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
 1 & 1 & 2 & 1 & 2 & 0 & 1 & 2 & 1 & 1 & 2 & 2 & 2 & 1 & 1 & 1 & 1 \\
 1 & 2 & 0 & 1 & 0 & 1 & 2 & 0 & 1 & 2 & 2 & 0 & 2 & 0 & 0 & 1 & 1 \\
 1 & 0 & 1 & 1 & 2 & 0 & 1 & 2 & 1 & 2 & 2 & 2 & 0 & 0 & 0 & 0 & 0 \\
 0 & 2 & 2 & 0 & 0 & 0 & 0 & 1 & 1 & 2 & 2 & 1 & 1 & 1 & 1 & 1 & 0 \\
 1 & 0 & 1 & 1 & 0 & 2 & 2 & 2 & 1 & 2 & 2 & 1 & 1 & 1 & 1 & 1 & 1 \\
 0 & 0 & 2 & 2 & 0 & 0 & 0 & 0 & 1 & 1 & 2 & 2 & 1 & 1 & 1 & 1 & 1 \\
 0 & 0 & 2 & 2 & 0 & 0 & 0 & 0 & 1 & 1 & 2 & 2 & 1 & 1 & 1 & 1 & 1 \\
 2 & 1 & 1 & 1 & 0 & 0 & 2 & 2 & 1 & 1 & 1 & 2 & 2 & 1 & 1 & 1 & 1
 \end{array}$$

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.

$$\begin{array}{cccccccccccccccccccc}
 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
 1 & 1 & 2 & 1 & 2 & 0 & 1 & 2 & 1 & 1 & 2 & 2 & 2 & 1 & 1 & 1 & 1 \\
 1 & 2 & 0 & 1 & 0 & 1 & 2 & 0 & 1 & 2 & 2 & 0 & 2 & 0 & 0 & 1 & 1 \\
 1 & 0 & 1 & 1 & 2 & 0 & 1 & 2 & 1 & 2 & 2 & 2 & 0 & 0 & 0 & 0 & 0 \\
 0 & 2 & 2 & 0 & 0 & 0 & 0 & 1 & 1 & 2 & 2 & 1 & 1 & 1 & 1 & 1 & 0 \\
 1 & 0 & 1 & 1 & 0 & 2 & 2 & 2 & 1 & 2 & 2 & 1 & 1 & 1 & 1 & 1 & 1 \\
 0 & 0 & 2 & 2 & 0 & 0 & 0 & 0 & 1 & 1 & 2 & 2 & 1 & 1 & 1 & 1 & 1 \\
 0 & 0 & 2 & 2 & 0 & 0 & 0 & 0 & 1 & 1 & 2 & 2 & 1 & 1 & 1 & 1 & 1 \\
 2 & 1 & 2 & 2 & 0 & 0 & 2 & 2 & 1 & 1 & 1 & 2 & 2 & 1 & 1 & 1 & 0
 \end{array}$$

El receptor genera una matriu de control per verificar si hi ha hagut errors. El polinomi de control és $h(x) = \frac{x^8-1}{g} = x^4 + \alpha^2 x^3 + x^2 + \alpha^7 x + \alpha^2$.

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

$$(\alpha^7 \alpha^6 0 \alpha^6 \alpha^2 \alpha^3 \alpha^7 1) - (0 \alpha^2 0 0 0 0 0 \alpha^5) = (\alpha^7 \alpha^2 0 \alpha^6 \alpha^2 \alpha^3 \alpha^7 \alpha^2).$$

Com que el codi és sistemàtic, sabem que la redundància és a l'esquerra i que la part d'informació correspon als símbols $\alpha^2 \alpha^3 \alpha^7 \alpha^2$.

6.4 Solucions

Solució de l'Exercici 94

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

$$A_{11} = \det \begin{pmatrix} 5 & 4 & 3 \\ 4 & 2 & 2 \\ 6 & 1 & 6 \end{pmatrix} = 60 + 12 + 48 - 36 - 10 - 96 = 4 + 5 + 6 - 1 - 3 - 5 = 6$$

$$A_{12} = \det \begin{pmatrix} 6 & 4 & 3 \\ 1 & 2 & 2 \\ 6 & 1 & 6 \end{pmatrix} = 72 + 3 + 48 - 36 - 12 - 24 = 2 + 3 + 6 - 1 - 5 - 3 = 2$$

$$A_{13} = \det \begin{pmatrix} 6 & 5 & 3 \\ 1 & 4 & 2 \\ 6 & 6 & 6 \end{pmatrix} = 144 + 18 + 60 - 72 - 72 - 30 = 4 + 4 + 4 - 2 - 2 - 2 = 6$$

$$A_{14} = \det \begin{pmatrix} 6 & 5 & 4 \\ 1 & 4 & 2 \\ 6 & 6 & 1 \end{pmatrix} = 24 + 24 + 60 - 96 - 72 - 5 = 3 + 3 + 4 - 5 - 2 - 5 = 5.$$

$$\text{Per tant, } \det(A) = 1 \cdot A_{11} - 1 \cdot A_{12} + 1 \cdot A_{13} - 1 \cdot A_{14} = 6 - 2 + 6 - 5 = 5.$$

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.136)

Solució de l'Exercici 95

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.136)

Solució de l'Exercici 96

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:

$$\begin{aligned}
 \det(V_4(1, \alpha, \alpha^3, \alpha^4)) &= \det \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & \alpha & \alpha^3 & \alpha^4 \\ 1 & \alpha^2 & \alpha^6 & 1 \\ 1 & \alpha^3 & \alpha & \alpha^4 \end{pmatrix} = \\
 &= \det \begin{pmatrix} \alpha & \alpha^3 & \alpha^4 \\ \alpha^2 & \alpha^6 & 1 \\ \alpha^3 & \alpha & \alpha^4 \end{pmatrix} - \det \begin{pmatrix} 1 & 1 & 1 \\ \alpha^2 & \alpha^6 & 1 \\ \alpha^3 & \alpha & \alpha^4 \end{pmatrix} + \det \begin{pmatrix} 1 & 1 & 1 \\ \alpha & \alpha^3 & \alpha^4 \\ \alpha^3 & \alpha & \alpha^4 \end{pmatrix} - \det \begin{pmatrix} 1 & 1 & 1 \\ \alpha & \alpha^3 & \alpha^4 \\ \alpha^2 & \alpha^6 & 1 \end{pmatrix} = \\
 &= (\alpha^3 + \alpha^6 + \alpha^7 - \alpha^5 - \alpha - \alpha^2) - (\alpha^2 + \alpha^3 + \alpha^3 - \alpha - \alpha - \alpha^6) + (\alpha^7 + \alpha^7 + \alpha^2 - \alpha^6 - \alpha^5 - \alpha^5) - (\alpha^3 + \alpha^6 + \alpha^7 - \alpha^5 - \alpha - \alpha^2) = \\
 &= (\cancel{\alpha^3} + \cancel{\alpha^6} + \cancel{\alpha^7} - \cancel{\alpha^5} - \cancel{\alpha} - \cancel{\alpha^2}) - (\cancel{\alpha^2} + \cancel{\alpha^3} + \cancel{\alpha^3} - \cancel{\alpha} - \cancel{\alpha} - \cancel{\alpha^6}) + (\alpha^7 + \alpha^7 + \cancel{\alpha^2} - \cancel{\alpha^6} - \alpha^5 - \alpha^5) - (\cancel{\alpha^3} + \cancel{\alpha^6} + \cancel{\alpha^7} - \cancel{\alpha^5} - \cancel{\alpha} - \cancel{\alpha^2}) = \\
 &= -\alpha^3 + \alpha + \alpha^7 + \alpha^7 - \alpha^5 - \alpha^5 - \alpha^3 + \alpha = (\alpha + \alpha) + (\alpha^7 + \alpha^7) - (\alpha^3 + \alpha^3) - (\alpha^5 + \alpha^5) = \alpha^4\alpha + \alpha^4\alpha^7 + \alpha^3 + \alpha^5 = \\
 &= \alpha^5 + \alpha^3 + \alpha^3 + \alpha^5 = (\alpha^5 + \alpha^5) + (\alpha^3 + \alpha^3) = \alpha + \alpha^7
 \end{aligned}$$

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 \(p.137\)](#)

Solució de l'Exercici 97

1. És un subespai vectorial perquè totes les combinacions lineals de dues de les quatre paraules pertanyen al codi:

$$\begin{array}{rcl}
 0000 & + & 0000 = 0000 \\
 0000 & + & 0101 = 0101 \\
 0000 & + & 1010 = 1010 \\
 0101 & + & 0101 = 0000 \\
 0101 & + & 1010 = 1111 \\
 0101 & + & 1111 = 1010 \\
 1010 & + & 1010 = 0000 \\
 1010 & + & 1111 = 0101 \\
 1111 & + & 1111 = 0000
 \end{array}$$

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.137)

Solució de l'Exercici 98

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 codificació 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.138)

Solució de l'Exercici 99

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.

$$\begin{array}{r} x^4 \quad + 1 \\ -(x^4 + x^2) \\ \hline x^2 + 1 \\ -(x^2 + 1) \\ \hline 0 \end{array} \quad \left| \begin{array}{l} x^2 + 1 \\ x^2 + 1 \end{array} \right.$$

Veiem que la divisió és exacta.

$$4. \text{ grau}(g) = 2 \text{ i } n - k = 4 - 2 = 2.$$

Torna a l'exercici (p.140)

Solució de l'Exercici 100

$$1. \text{ Per analitzar } G_1 \text{ i } G_2, \text{ considerem } Q = \begin{pmatrix} 1 & 2 & 4 & 0 \\ 0 & 1 & 2 & 4 \\ 0 & 0 & 1 & 2 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

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 $x^6 - 1$.

$$\begin{array}{r} x^6 \qquad \qquad \qquad +6 \qquad \qquad \qquad \left| \begin{array}{l} 4x^2 + 2x + 1 \\ 2x^4 + 6x^3 \end{array} \right. \\ -(x^6 + 4x^5 + 2x^4) \qquad \qquad \qquad) \\ \hline 3x^5 + 5x^4 \qquad \qquad \qquad +6 \\ -(3x^5 + 5x^4 + 6x^3) \qquad \qquad \qquad) \\ \hline x^3 \qquad \qquad \qquad +6 \\ -(x^3 + 4x^2 + 2x) \qquad \qquad \qquad) \\ \hline 3x^2 + 5x + 6 \\ -(3x^2 + 5x + 6) \\ \hline 0 \end{array}$$

Com que la divisió és exacta, concloem que G_2 genera un codi cíclic.

$$3. \text{ Consider } Q_3 = \begin{pmatrix} 1 & 2 & 4 \\ 0 & 1 & 2 \\ 0 & 0 & 1 \end{pmatrix}$$

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 $x^5 - 1$.

$$\begin{array}{r}
 x^5 \qquad \qquad \qquad +6 \\
 -(x^5 + 4x^4 + 2x^3) \qquad \qquad \qquad) \\
 \hline
 3x^4 + 5x^3 \qquad \qquad \qquad +6 \\
 -(3x^4 + 5x^3 + 6x^2) \qquad \qquad \qquad) \\
 \hline
 \qquad \qquad \qquad x^2 \qquad \qquad \qquad +6 \\
 -(x^2 + 4x + 2) \qquad \qquad \qquad) \\
 \hline
 \qquad \qquad \qquad \qquad \qquad \qquad 3x + 4
 \end{array}
 \quad
 \begin{array}{r}
 4x^2 + 2x + 1 \\
 2x^3 + 6x^2 \quad +2
 \end{array}$$

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

$$\begin{aligned}
 x &= 4 \\
 2x + y &= 0 \\
 4x + 2y + z &= 0 \\
 4y + 2z &= 1 \\
 4z &= 2
 \end{aligned}$$

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 \(p.142\)](#)

Solució de l'Exercici 101

Si el codi és primitiu, aleshores $n = q - 1$.

Que $x - \beta$ divideixi $x^n - 1 = x^{q-1} - 1$ 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 \(p.142\)](#)

Solució de l'Exercici 102

Es dedueix de l'exercici anterior i del fet que $(x - \alpha_1), \dots, (x - \alpha_r)$ són tots irreductibles. [Torna a l'exercici \(p.142\)](#)

Solució de l'Exercici 103

1. Cal demostrar que g divideix $x^6 - 1$.

$$\begin{array}{r}
 x^6 \qquad \qquad \qquad +6 \\
 -(x^6 + 4x^5 \qquad \qquad \qquad + 6x^3 + 3x^2) \qquad \qquad \qquad) \\
 \hline
 3x^5 \qquad \qquad \qquad + x^3 + 4x^2 \qquad \qquad \qquad +6 \\
 -(3x^5 + 5x^4 \qquad \qquad \qquad + 4x^2 + 2x) \qquad \qquad \qquad) \\
 \hline
 2x^4 + x^3 \qquad \qquad \qquad + 5x + 6 \\
 -(2x^4 + x^3 \qquad \qquad \qquad + 5x + 6) \qquad \qquad \qquad) \\
 \hline
 0
 \end{array}
 \quad
 \begin{array}{r}
 x^4 + 4x^3 \qquad \qquad \qquad + 6x + 3 \\
 x^2 + 3x + 2
 \end{array}$$

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 $(x \ y \ z \ 2 \ 3 \ 5)$ 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:

$$\begin{array}{r} 5x^7 + 4x^6 + 2x + 3 \\ -(5x^7 + 2x) \\ \hline 4x^6 + 3 \\ -(4x^6 + 3) \\ \hline 0 \end{array} \quad \begin{array}{r} x^6 \\ 5x + 4 \\ \hline \end{array}$$

Torna a l'exercici (p.144)

Solució de l'Exercici 104

1. Es pot veure que

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix} \sim \begin{matrix} f'_1 = f_1 + f_2 + f_3 + f_4 \\ f'_2 = f_2 + f_3 + f_4 + f_5 \\ f'_3 = f_3 + f_4 + f_5 \\ f'_4 = f_4 + f_5 \\ f'_5 = f_5 \end{matrix}$$

$$\begin{pmatrix} 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}$$

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.

$$\begin{array}{r} x^8 \\ -(x^8 + x^7 + x^6 + x^5) \quad +1 \\ \hline x^7 + x^6 + x^5 \quad +1 \\ -(x^7 + x^6 + x^5 + x^4) \quad +1 \\ \hline x^4 \quad +1 \\ -(x^4 + x^3 + x^2 + x) \quad +1 \\ \hline x^3 + x^2 + x + 1 \\ -(x^3 + x^2 + x + 1) \\ \hline 0 \end{array} \quad \left| \begin{array}{l} x^3 + x^2 + x + 1 \\ x^5 + x^4 \quad + x + 1 \end{array} \right.$$

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.144)

Solució de l'Exercici 105

El residu de dividir $i(x)x^{n-k} = x^4 + x^5$ entre g és $R(x) = 5x^3 + x^2 + x + 2$:

$$\begin{array}{r} x^5 + x^4 \\ -(x^5 + 4x^4 \quad + 6x^2 + 3x) \quad +1 \\ \hline 4x^4 \quad + x^2 + 4x \\ -(4x^4 + 2x^3 \quad + 3x + 5) \\ \hline 5x^3 + x^2 + x + 2 \end{array} \quad \left| \begin{array}{l} x^4 + 4x^3 + 6x + 3 \\ x + 4 \end{array} \right.$$

Aleshores $i(x)x^{n-k} - R(x)$ correspon a la paraula codi 566211.

Torna a l'exercici (p.146)

Solució de l'Exercici 106

1. A la solució de l'exercici 104 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.147)

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.135)

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.

6.6 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.140)

7 Matrius de Vandermonde i codis Reed-Solomon

7.1 Matrius de Vandermonde II

Recordem que, donats $v_1, v_2, \dots, v_n \in \mathbb{F}_q$, la matriu de Vandermonde de $v_1, \dots, v_n$ d'ordre r es defineix com

$$V_r(v_1, v_2, \dots, v_n) = \begin{pmatrix} 1 & 1 & \dots & 1 \\ v_1 & v_2 & \dots & v_n \\ v_1^2 & v_2^2 & \dots & v_n^2 \\ \vdots & \vdots & \ddots & \vdots \\ v_1^{r-1} & v_2^{r-1} & \dots & v_n^{r-1} \end{pmatrix}$$

Recordem també que el determinant de la matriu de Vandermonde $V_n(v_1, v_2, \dots, v_n)$ és igual a

$$\det(V_n(v_1, v_2, \dots, v_n)) = \prod_{1 \leq i < j \leq n} (v_j - v_i)$$

Matrius de Vandermonde de producte nul

Teorema 16

Sigui w un element primitiu de $\mathbb{F}_q$. Per tot $1 \leq k \leq q-2$, el producte de les matrius

$$V_k(1, w, w^2, \dots, w^{q-2}) \quad \text{i} \quad V_{q-1}(w, w^2, \dots, w^{q-1-k})$$

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

$$\bullet V_k(1, w, w^2, w^3) = V_2(1, 3, 3^2, 3^3) = V_2(1, 3, 4, 2) = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 3 & 4 & 2 \end{pmatrix}$$

$$\bullet V_{q-1}(w, w^2, \dots, w^{q-1-k}) = V_4(3, 3^2) = V_4(3, 4) = \begin{pmatrix} 1 & 1 \\ 3 & 4 \\ 4 & 1 \\ 2 & 4 \end{pmatrix}$$

• 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 primitiu. Ara podem fer els càlculs:

$$\bullet V_k(1, \alpha, \alpha^2, \dots, \alpha^{q-2}) = V_1(1, \alpha, \alpha^2) = \begin{pmatrix} 1 & 1 & 1 \end{pmatrix}$$

$$\bullet V_{q-1}(\alpha, \alpha^2, \dots, \alpha^{q-1-k}) = V_3(\alpha, \alpha^2) = \begin{pmatrix} 1 & 1 \\ \alpha & \alpha^2 \\ \alpha^2 & \alpha \end{pmatrix}$$

• 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 $1 \leq i \leq k$ i $1 \leq j \leq q-1-k$.
 - 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 polinomi definit com $f(x) = a_0 + a_1x + \dots + a_{n-1}x^{n-1}$, amb $a_0, \dots, a_{n-1} \in \mathbb{F}_q$.

Lavors 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,

$$\begin{pmatrix} 1 & 1 & 1 & 1 & \dots & 1 \\ 1 & w & w^2 & w^3 & \dots & w^{(n-1)} \\ 1 & w^2 & w^4 & w^6 & \dots & w^{2(n-1)} \\ 1 & w^3 & w^6 & w^9 & \dots & w^{3(n-1)} \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & w^{n-1} & w^{2(n-1)} & w^{3(n-1)} & \dots & w^{(n-1)(n-1)} \end{pmatrix} \begin{pmatrix} a_0 \\ a_1 \\ \vdots \\ a_{n-1} \end{pmatrix} = \begin{pmatrix} f(1) \\ f(w) \\ \vdots \\ f(w^{n-1}) \end{pmatrix}.$$

► Interpolació polinòmica i matrius de Vandermonde

Teorema 17

- 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 $f_u = a_0 + a_1 x + \dots + a_{n-1} x^{n-1}$ està determinat per la solució del sistema lineal d'equacions

$$\begin{pmatrix} 1 & 1 & 1 & 1 & \dots & 1 \\ 1 & w & w^2 & w^3 & \dots & w^{(n-1)} \\ 1 & w^2 & w^4 & w^6 & \dots & w^{2(n-1)} \\ 1 & w^3 & w^6 & w^9 & \dots & w^{3(n-1)} \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & w^{n-1} & w^{2(n-1)} & w^{3(n-1)} & \dots & w^{(n-1)(n-1)} \end{pmatrix} \begin{pmatrix} a_0 \\ a_1 \\ \vdots \\ a_{n-1} \end{pmatrix} = \begin{pmatrix} u_0 \\ u_1 \\ \vdots \\ u_{n-1} \end{pmatrix}.$$

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.

7.2 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 (RS₄(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 RS₄(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 (RS₄(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:

$$\mathbb{F}_4^2 = \{(0, 0), (1, 0), (\alpha, 0), (\alpha^2, 0), (0, 1), (0, \alpha), (0, \alpha^2), (1, 1), (1, \alpha), (1, \alpha^2), (\alpha, 1), (\alpha, \alpha), (\alpha, \alpha^2), (\alpha^2, 1), (\alpha^2, \alpha), (\alpha^2, \alpha^2)\}$$

- Les paraules són

$$RS_4(2) = \{(0, 0, 0), (1, 1, 1), (\alpha, \alpha, \alpha), (\alpha^2, \alpha^2, \alpha^2), (1, \alpha, \alpha^2), (\alpha, \alpha^2, 1), (\alpha^2, 1, \alpha), (0, \alpha^2, \alpha), (\alpha^2, \alpha, 0), (\alpha, 0, \alpha^2), (\alpha^2, 0, 1), (0, 1, \alpha^2), (1, \alpha^2, 0), (\alpha, 1, 0), (1, 0, \alpha), (0, 1, \alpha)\}.$$

Matriu de control

- Pel **teorema 16**, 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 síndrome 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'anomenen codis Maximum Distance Separable (MDS).
- Els MDS són interessants perquè, donat n i k , garanteixen la màxima capacitat correctora.

Lema 34

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 $0 \leq j_1, \dots, j_{n-k} \leq n - 1$.
- La submatriu amb aquestes columnes té determinant

$$\begin{vmatrix} w^{j_1} & w^{j_2} & \dots & w^{j_{n-k}} \\ w^{2j_1} & w^{2j_2} & \dots & w^{2j_{n-k}} \\ w^{3j_1} & w^{3j_2} & \dots & w^{3j_{n-k}} \\ \vdots & \vdots & \ddots & \vdots \\ w^{(n-k)j_1} & w^{(n-k)j_2} & \dots & w^{(n-k)j_{n-k}} \end{vmatrix} = w^{j_1} w^{j_2} \dots w^{j_{n-k}} \cdot |V_{n-k}(w^{j_1}, w^{j_2}, \dots, w^{j_{n-k}})|.$$

- 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, $d = n - k + 1$.

□

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

$$RS_4(2) = \{(0, 0, 0), (1, 1, 1), (\alpha, \alpha, \alpha), (\alpha^2, \alpha^2, \alpha^2), (1, \alpha, \alpha^2), (\alpha, \alpha^2, 1), (\alpha^2, 1, \alpha), (0, \alpha^2, \alpha), (\alpha^2, \alpha, 0), (\alpha, 0, \alpha^2), (\alpha^2, 0, 1), (0, 1, \alpha^2), (1, \alpha^2, 0), (\alpha, 1, 0), (1, 0, \alpha), (0, 1, \alpha)\}.$$

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 definició 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 -èsima columna de la matriu G definida abans (**G**).

- Per tant, el producte del vector $(a_0, \dots, a_{k-1})$ per la matriu **G** és exactament el vector $(a(1), a(w), a(w^2), \dots, a(w^{n-1}))$.

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

$$RS_q(k) = \{(a(1), a(w), a(w^2), \dots, a(w^{n-1})) : a \in \mathbb{F}_q[x]^{<k}\},$$

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 $u = (u_0, \dots, u_{n-1})$ 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 $i \in \{0, \dots, n-1\}$.
- Per tant, cada u de $\mathbb{F}_q^n$ és del tipus

$$(f(1), f(w), f(w^2), \dots, f(w^{n-1}))$$

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 $u = (u_0, \dots, u_{n-1}) \in \mathbb{F}_q^n$ 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

$$u(x) = u_0 + u_1 x + u_2 x^2 + \dots + u_{n-1} x^{n-1}$$

amb $u_i \in \mathbb{F}_q$.

- Observem que avaluar u a w^i dona

$$\begin{aligned} u(w^i) &= u_0 + u_1 w^i + u_2 w^{i \cdot 2} + \dots + u_{n-1} w^{i(n-1)} \\ &= \begin{pmatrix} 1 & w^i & w^{i \cdot 2} & \dots & w^{i(n-1)} \end{pmatrix} \begin{pmatrix} u_0 \\ u_1 \\ u_2 \\ \vdots \\ u_{n-1} \end{pmatrix} \end{aligned}$$

que, si $i \leq n-k$, és exactament el producte de la fila i -èssima de H (H) pel vector $(u_0, \dots, u_{n-1})^T$.

- Per tant, el producte de H pel vector $(u_0, \dots, u_{n-1})^T$ és igual a

$$(u(w), u(w^2), \dots, u(w^{n-k}))^T.$$

- Per la definició de la matriu de control, podem veure que $RS_q(k)$ és el conjunt de vectors $u = (u_0, \dots, u_{n-1}) \in \mathbb{F}_q^n$ pels quals el polinomi

$$u_0 + u_1 x + \dots + u_{n-1} x^{n-1}$$

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

$$\{(u_0, u_1, \dots, u_{n-1}) \in \mathbb{F}_q^n : u(w) = u(w^2) = \dots = u(w^{n-k}) = 0\}.$$

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 :

$$\begin{aligned} u(\alpha) &= \alpha + \alpha^4 = 0, \\ u(\alpha^2) &= \alpha + \alpha^6 = \alpha + 1 \neq 0 \end{aligned}$$

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

$$g(x) = (x - w) \cdot \dots \cdot (x - w^{n-k}).$$

- 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 $g(x) = (x - w) \cdot \dots \cdot (x - w^{n-k})$.

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	$G = \begin{pmatrix} 1 & 1 & 1 & \dots & 1 \\ 1 & w & w^2 & \dots & w^{n-1} \\ 1 & w^2 & w^4 & \dots & w^{2(n-1)} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & w^{k-1} & w^{(k-1)2} & \dots & w^{(k-1)(n-1)} \end{pmatrix}.$
A partir de la matriu de control	$H = \begin{pmatrix} 1 & w & w^2 & \dots & w^{n-1} \\ 1 & w^2 & w^4 & \dots & w^{2(n-1)} \\ 1 & w^3 & w^6 & \dots & w^{3(n-1)} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & w^{n-k} & w^{(n-k)2} & \dots & w^{(n-k)(n-1)} \end{pmatrix}.$
Com a codi d'avaluació	$RS_q(k) = \{(a(1), a(w), a(w^2), \dots, a(w^{n-1})) : a \in \mathbb{F}_q[x]^{<k}\}.$
Com a codi cíclic primitiu	$g(x) = (x - w)(x - w^2) \dots (x - w^{n-k}),$ $RS_q(k) = \{(u_0, u_1, \dots, u_{n-1}) \in \mathbb{F}_q^n : u(w) = u(w^2) = \dots = u(w^{n-k}) = 0\}.$

Exercici 107

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.176)

Exercici 108

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.177)

Exercici 109

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.179)

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 algorisme 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.

7.3 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 ,

$$\begin{pmatrix} w^{i_1} & w^{i_2} & \dots & w^{i_t} \\ w^{2i_1} & w^{2i_2} & \dots & w^{2i_t} \\ \vdots & \vdots & \ddots & \vdots \\ w^{ti_1} & w^{ti_2} & \dots & w^{ti_t} \end{pmatrix}$$

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

$$\begin{pmatrix} w^{i_1} & w^{i_2} & \dots & w^{i_t} \\ w^{2i_1} & w^{2i_2} & \dots & w^{2i_t} \\ \vdots & \vdots & \ddots & \vdots \\ w^{ti_1} & w^{ti_2} & \dots & w^{ti_t} \end{pmatrix} \begin{pmatrix} e_{i_1} \\ e_{i_2} \\ \vdots \\ e_{i_t} \end{pmatrix} = \begin{pmatrix} u(w) \\ u(w^2) \\ \vdots \\ u(w^t) \end{pmatrix}$$

Exercici 110

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.179)

Exercici 111

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.181)

Exercici 112

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.182)

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

$$\text{rang} \begin{pmatrix} u(w) & \dots & u(w^t) \\ u(w^2) & \dots & u(w^{t+1}) \\ \vdots & \vdots & \vdots \\ u(w^{d-1-t}) & \dots & u(w^{d-2}) \end{pmatrix} = \text{rang} \begin{pmatrix} u(w) & \dots & u(w^t) & u(w^{t+1}) \\ u(w^2) & \dots & u(w^{t+1}) & u(w^{t+2}) \\ \vdots & \vdots & \vdots & \vdots \\ u(w^{d-1-t}) & \dots & u(w^{d-2}) & u(w^{d-1}) \end{pmatrix}$$

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 $x^t + l_{t-1}x^{t-1} + \dots + l_1x + l_0$. Diem que λ_u és el polinomi localitzador d'errors.

3. Trobem les posicions d'error a partir de les arrels de λ_u .
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

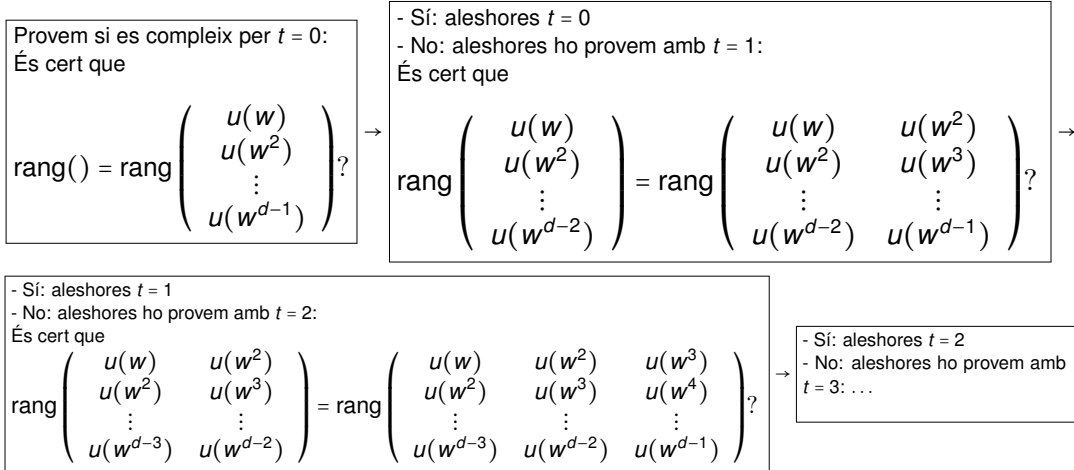
Sigui C un codi cíclic tal que $w, w^2, \dots, w^{d-1}$ són les arrels del polinomi generador de C .

Input: $u \in \mathbb{F}_q^n$

1. Sigui t el mínim enter pel qual

$$\text{rang} \begin{pmatrix} u(w) & \dots & u(w^t) \\ u(w^2) & \dots & u(w^{t+1}) \\ \vdots & \vdots & \vdots \\ u(w^{d-1-t}) & \dots & u(w^{d-2}) \end{pmatrix} = \text{rang} \begin{pmatrix} u(w) & \dots & u(w^{t+1}) \\ u(w^2) & \dots & u(w^{t+2}) \\ \vdots & \vdots & \vdots \\ u(w^{d-1-t}) & \dots & u(w^{d-1}) \end{pmatrix}$$

Això vol dir:



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 113

Considerem el codi RS de l'Exercici 108.

- 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: $u(w) = 2$, $u(w^2) = 9$, $u(w^3) = 8$, $u(w^4) = 10$, $u(w^5) = 1$, $u(w^6) = 0 \dots$
 - Quants errors té la paraula u respecte de C ?
 - Quin és el polinomi localitzador d'errors de u ?
 - Quines són les posicions dels errors de u ?
 - Quins són els valors dels errors de u ?
 - Quina és la paraula corregida?
- 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 w ens dona els següents valors: $v(w) = 9$, $v(w^2) = 8$, $v(w^3) = 5$, $v(w^4) = 12$, $v(w^5) = 4$, $v(w^6) = 8 \dots$
 - Quants errors té la paraula v respecte de C ?
 - Quin és el polinomi localitzador d'errors de v ?
 - Quines són les posicions dels errors de v ?
 - Quins són els valors dels errors de v ?
 - Quina és la paraula corregida?

Solució (p.182)

Exercici 114

- Considerem el codi RS de l'exercici 109.
 - Codifiqueu de manera sistemàtica utilitzant el polinomi generador el primer bloc d'informació de la cadena de bits
 $111110001111100011111111111110001010101010101010100011111000 \dots$
 Doneu el resultat també com a cadena de bits.
 - Calculeu alguna síndrome de la paraula codificada.
- Considerem el codi RS de l'exercici 109.
 - Rebem la cadena de bits 00110000000000010100. A quina cadena de símbols correspon?
 - Calculeu totes les síndromes de la paraula rebuda.
 - Quants errors té de símbol la paraula rebuda?
 - Quin és el polinomi localitzador d'errors?
 - Trobeu les posicions dels errors.
 - Calculeu el valor dels errors.
 - Doneu la cadena de bits corregida.
 - Quants errors de bit tenia la paraula enviada?

Solució (p.184)

7.4 Solucions

Solució de l'Exercici 107

1. L'element 2 és primitiu. En efecte, les seves potències són totes diferents fins a exponent $q - 1 = 4$.

$$2^0 = 1, \quad 2^1 = 2, \quad 2^2 = 4, \quad 2^3 = 3, \quad 2^4 = 1.$$

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 3 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:

$0(1111) + 0(1243) = (0000)$	$2(1111) + 3(1243) = (0341)$
$0(1111) + 1(1243) = (1243)$	$2(1111) + 4(1243) = (1034)$
$0(1111) + 2(1243) = (2431)$	$3(1111) + 0(1243) = (3333)$
$0(1111) + 3(1243) = (3124)$	$3(1111) + 1(1243) = (4021)$
$0(1111) + 4(1243) = (4312)$	$3(1111) + 2(1243) = (0214)$
$1(1111) + 0(1243) = (1111)$	$3(1111) + 3(1243) = (1402)$
$1(1111) + 1(1243) = (2304)$	$3(1111) + 4(1243) = (2140)$
$1(1111) + 2(1243) = (3042)$	$4(1111) + 0(1243) = (4444)$
$1(1111) + 3(1243) = (4230)$	$4(1111) + 1(1243) = (0132)$
$1(1111) + 4(1243) = (0423)$	$4(1111) + 2(1243) = (1320)$
$2(1111) + 0(1243) = (2222)$	$4(1111) + 3(1243) = (2013)$
$2(1111) + 1(1243) = (3410)$	$4(1111) + 4(1243) = (3201)$
$2(1111) + 2(1243) = (4103)$	

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.169)

Solució de l'Exercici 108

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 $(x-7)(x-7^2)(x-7^3)(x-7^4) = (x-7)(x-10)(x-5)(x-9) = x^4 + (-7-10-5-9)x^3 + (7 \cdot 10 + 7 \cdot 5 + 7 \cdot 9 + 10 \cdot 5 + 10 \cdot 9 + 5 \cdot 9)x^2 + (-7 \cdot 10 \cdot 5 - 7 \cdot 10 \cdot 9 - 7 \cdot 5 \cdot 9 - 10 \cdot 5 \cdot 9)x + 7 \cdot 10 \cdot 5 \cdot 9 = x^4 + 8x^3 + (5+9+11+11+12+6)x^2 + (-5 \cdot 5 - 5 \cdot 9 - 9 \cdot 9 - 11 \cdot 9)x + 5 \cdot 6 = x^4 + 8x^3 + 2x^2 + (1+7+10+5)x + 4 = x^4 + 8x^3 + 2x^2 + 10x + 4$.

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.170)

Solució de l'Exercici 109

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.170)

Solució de l'Exercici 110

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.

$$\begin{aligned} \begin{pmatrix} 3 & 6 & 5 \\ 2 & 1 & 4 \\ 6 & 6 & 6 \end{pmatrix}^{-1} &= \frac{1}{4 + 4 + 4 - 2 - 2 - 2} \begin{pmatrix} +3 & -2 & +6 \\ -6 & +2 & -3 \\ +5 & -2 & +5 \end{pmatrix}^T \\ &= \frac{1}{6} \begin{pmatrix} 3 & 5 & 6 \\ 1 & 2 & 4 \\ 5 & 5 & 5 \end{pmatrix}^T \\ &= 6 \begin{pmatrix} 3 & 1 & 5 \\ 5 & 2 & 5 \\ 6 & 4 & 5 \end{pmatrix} \\ &= \begin{pmatrix} 4 & 6 & 2 \\ 2 & 5 & 2 \\ 1 & 3 & 2 \end{pmatrix} \end{aligned}$$

Lavors 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.172)

Solució de l'Exercici 111

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 $g(x) = (x - \alpha)(x - \alpha^2) = x^2 + \alpha^4x + \alpha^3$.
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 $(0\alpha^3\alpha^41000)$, que correspon al polinomi $x \cdot g$.
6. Posem esborralls a les posicions primera i segona. Obtenim $(??\alpha^41000)$. El polinomi corresponent a la paraula rebuda, si substituïm els esborralls per zero, és $u(x) = \alpha^4x^2 + x^3$.

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 $(00\alpha^41000) - (0\alpha^300000) = (0\alpha^3\alpha^41000)$.

Torna a l'exercici (p.172)

Solució de l'Exercici 112

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. $g(x) = (x - \alpha)(x - \alpha^2)(x - \alpha^3) = x^3 + \alpha x^2 + \alpha^7x + \alpha^2$.
5. La dimensió serà $n - \text{grau}(g) = 5$.
6. Tenim la paraula amb esborralls $(\alpha\alpha^3\alpha^?000)$. El polinomi corresponent és $u(x) = \alpha x^2 + \alpha^3x + \alpha$. 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 $(x^8 - 1)/g = x^5 + \alpha^5x^4 + \alpha x^3 + \alpha^3x^2 + \alpha^3x + \alpha^2$. El seu recíproc serà el generador del codi dual i és exactament $h^* = \alpha^2x^5 + \alpha^3x^4 + \alpha^3x^3 + \alpha x^2 + \alpha^5x + 1$.

Torna a l'exercici (p.172)

Solució de l'Exercici 113

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 $\text{rang} \begin{pmatrix} 7^{11} \\ 7^4 \\ 7^9 \end{pmatrix} = \text{rang} \begin{pmatrix} 7^{11} & 7^4 \\ 7^4 & 7^9 \\ 7^9 & 7^2 \end{pmatrix} = 1$.

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 resollem $7^5 e_5 = 2 = 7^{11}$, 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 $\text{rang}() \neq \text{rang} \begin{pmatrix} 9 \\ 8 \\ 5 \\ 12 \end{pmatrix}$. Per tant, $t > 0$.

D'altra banda, $\text{rang} \begin{pmatrix} 9 \\ 8 \\ 5 \end{pmatrix} \neq \text{rang} \begin{pmatrix} 9 & 8 \\ 8 & 5 \\ 5 & 12 \end{pmatrix}$, ja que $\text{rang} \begin{pmatrix} 7^4 \\ 7^9 \\ 7^3 \end{pmatrix} \neq \text{rang} \begin{pmatrix} 7^4 & 7^9 \\ 7^9 & 7^3 \\ 7^3 & 7^6 \end{pmatrix}$. Per tant, $t > 1$.

Però $\text{rang} \begin{pmatrix} 9 & 8 \\ 8 & 5 \end{pmatrix} = \text{rang} \begin{pmatrix} 9 & 8 & 5 \\ 8 & 5 & 12 \end{pmatrix}$. 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 resollem 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.175)

Solució de l'Exercici 114

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:

$$\begin{array}{r} \alpha^2 x^6 + \alpha^3 x^5 + \alpha^5 x^4 \\ -(\alpha^2 x^6 + \alpha^5 x^5 + \alpha^2 x^4 + \alpha^3 x^3 + \alpha^5 x^2) \\ \hline \alpha^2 x^5 + \alpha^3 x^4 + \alpha^3 x^3 + \alpha^5 x^2 \\ -(\alpha^2 x^5 + \alpha^5 x^4 + \alpha^2 x^3 + \alpha^3 x^2 + \alpha^5 x) \\ \hline \alpha^2 x^4 + \alpha^5 x^3 + \alpha^2 x^2 + \alpha^5 x \\ -(\alpha^2 x^4 + \alpha^5 x^3 + \alpha^2 x^2 + \alpha^3 x + \alpha^5) \\ \hline \alpha^2 x + \alpha^5 \end{array} \quad \left| \begin{array}{r} x^4 + \alpha^3 x^3 + x^2 + \alpha x + \alpha^3 \\ \hline \alpha^2 x^2 + \alpha^2 x + \alpha^2 \end{array} \right.$$

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:

$$\begin{aligned} u(\alpha) &= \alpha^6 + \alpha^6 + \alpha + \alpha^2 = \alpha^4 \\ u(\alpha^2) &= \alpha^5 + \alpha^4 + \alpha^2 + \alpha^2 = 1 \\ u(\alpha^3) &= \alpha^4 + \alpha^2 + \alpha^3 + \alpha^2 = \alpha^6 \\ u(\alpha^4) &= \alpha^3 + 1 + \alpha^4 + \alpha^2 = 0 \end{aligned}$$

(c) Anomenem t al nombre d'errors. Tenim $\text{rang}() \neq \text{rang} \begin{pmatrix} \alpha^4 \\ 1 \\ \alpha^6 \\ 0 \end{pmatrix}$, per tant, $t > 0$. I tenim $\text{rang} \begin{pmatrix} \alpha^4 \\ 1 \\ \alpha^6 \end{pmatrix} \neq$

$\text{rang} \begin{pmatrix} \alpha^4 & 1 \\ 1 & \alpha^6 \\ \alpha^6 & 0 \end{pmatrix}$, per tant, $t > 1$. Com que $\text{rang} \begin{pmatrix} \alpha^4 & 1 \\ 1 & \alpha^6 \end{pmatrix} = \text{rang} \begin{pmatrix} \alpha^4 & 1 & \alpha^6 \\ 1 & \alpha^6 & 0 \end{pmatrix} = 2$, 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:

$$001100000000000010100$$

$$110100000000110010100$$

TEMA 2

Problemes bàsics

TEMA 2

Problemes bàsics

Índex

1	Aritmètica modular i polinomial, cossos finits	189
2	Codis lineals i cíclics	195
3	Matrius de Vandermonde i codis algebraics	204

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.
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.
3. (a) Trobeu el quocient i el residu per a les següents parelles de valors de dividendes 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.
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) $39x \equiv 18(60)$
5. Quantes solucions tenen aquestes equacions amb congruències? Doneu-ne les solucions.
 - (a) $26x \equiv 3 \pmod{13}$
 - (b) $13x \equiv 3 \pmod{26}$
 - (c) $26x \equiv 0 \pmod{13}$
 - (d) $9x \equiv -3 \pmod{15}$
 - (e) $5x \equiv 4 \pmod{7}$
 - (f) $5x \equiv 7 \pmod{7}$
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 $\text{mcd}(b, c)$?
 - (f) Expresseu $\text{mcd}(b, c)$ 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.
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?
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.
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.
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.
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 anomenau-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.
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?
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.
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.
- (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 .
- (c) Podem deduir si 7 és invertible a $\mathbb{Z}_9$? En cas afirmatiu doneu el seu invers.
- (d) Podem deduir si $2x + 1$ és invertible a $\mathbb{Z}_3[x]/x^2 + 2x + 2$? En cas afirmatiu doneu el seu invers.
- (e) Podem deduir si $x + 2$ és invertible a $\mathbb{Z}_3[x]/x^2 + 2x + 2$? En cas afirmatiu doneu el seu invers.
- (f) Comproveu que tots els inversos que heu trobat són, en efecte, inversos.
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.
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.
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 $\mathbb{Z}_2[x]/f$?
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.
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 $\alpha^2 \left(\frac{\alpha^{20} - \alpha^5 + \alpha}{\alpha^3 - \alpha} \right)$.
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 $\beta^{15} \left(\frac{\beta^2 - \beta^3}{\beta^6 + \beta} \right)$.
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.
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 $\mathbb{F}_{27}$.
23. (a) Quants polinomis mònics hi ha a $\mathbb{Z}_3[x]$ de grau 2?
- (b) Quins són els polinomis irreductibles mònics de $\mathbb{Z}_3[x]$ de grau 2? Justifiqueu la resposta.
- (c) Escolliu un dels polinomis irreductibles de l'apartat anterior i digues-li f . Quants elements té $\mathbb{Z}_3/(f)$?
- (d) Quants elements té $\mathbb{Z}_9$?
- (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.
- (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.
- (g) Doneu un element primitiu de $\mathbb{Z}_3/(f)$ i escriviu totes les seves potències diferents en forma polinomial.
- (h) Doneu un element primitiu de $\mathbb{Z}_9$ i escriviu totes les seves potències diferents.
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) Escriuiu 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.
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.
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.

27. (a) És $\mathbb{Z}_3$ un cos? Per què?
 (b) Comproveu que només hi ha tres polinomis mòncics (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 .
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 determinar 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.
 • $a^5 - a^{11}$
 • $a^3 + a^{18}$
 • $\frac{a^5 - a^{11}}{a^3 + a^{18}} + a^{14}$

2 Codis lineals i cíclics

- Dins de $\mathbb{F}_2^3$ considerem el conjunt de paraules $C = \{(000), (111), (101), (010)\}$.
 - Demostreu que C és un codi lineal.
 - Doneu una matriu generadora de C .
 - Comproveu que totes les paraules de C estan generades per G .
 - Doneu una matriu de control de C .
 - Justifiqueu quina és la distància mínima de C .
 - Comproveu que totes les paraules del codi quan les multipliquem per la matriu de control donen 0.
 - Doneu el codi dual $C^\perp$.
 - Comproveu que les paraules del codi dual quan les multipliquem per la matriu G donen 0.
- Considerem el codi ternari C generat per la matriu

$$\begin{pmatrix} 1 & 1 & 1 & 0 \\ 2 & 0 & 1 & 1 \end{pmatrix}$$

- Quantes paraules té aquest codi?
 - Doneu totes les paraules del codi.
 - Doneu la distància mínima del codi. **Justifiqueu la resposta.**
 - Quina dimensió té el codi dual? **Justifiqueu la resposta.**
 - Doneu dues paraules (no múltiples una de l'altra) del codi dual. **Justifiqueu la resposta.**
 - Quina relació hi ha entre C i $C^\perp$?
 - Trobeu una matriu de control del codi.
 - Corregiu el missatge rebut 212112012222.
- A $\mathbb{Z}_5$ considerem el codi C_1 que té matriu de control

$$\begin{pmatrix} 3 & 1 & 3 & 2 & 1 \\ 4 & 1 & 0 & 4 & 1 \\ 3 & 2 & 2 & 0 & 3 \end{pmatrix}$$

- Doneu una matriu de control de C_1 sistemàtica per la dreta.
- Doneu una matriu generadora de C_1 .
- Quina és la dimensió de C_1 ?
- Quina és la longitud de C_1 ?
- Quina és la distància mínima de C_1 ?
- Quants esborralls es poden corregir?
- Quants errors es poden corregir?
- Corregiu els esborralls de la paraula (324??) i doneu la paraula corregida.
- Rebem la paraula (43031). Escolliu una matriu de control de les anteriors i doneu la síndrome de la paraula rebuda.
- Quants errors hi ha i en quines posicions es troben?
- Quins són els valors dels errors?
- Doneu la paraula corregida.

4. (a) Quants símbols diferents hi ha a $\mathbb{F}_{125}$?
- (b) Quins són els dígitos d'un codi sobre $\mathbb{F}_{125}$?
- (c) Quants dígitos 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?
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.
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.

8. Considerem el codi $\mathcal{C}$ sobre $\mathbb{Z}_3$ donat per les solucions del sistema

$$\begin{cases} x_1 + 2x_3 + x_4 + x_5 + 2x_6 = 0 \\ x_1 + 2x_2 + x_3 + 2x_4 + 2x_6 = 0 \end{cases}$$

- Doneu una matriu G generadora de $\mathcal{C}$.
 - Doneu una matriu H de control de $\mathcal{C}$.
 - Com és el producte GH^T ? I el producte HG^T ? Comproveu-ho.
 - Doneu la longitud i la dimensió de $\mathcal{C}$.
 - Doneu la distància mínima de $\mathcal{C}$.
 - Podem corregir algun esborrall? En cas afirmatiu
 - Digueu quants.
 - Poseu un exemple detallat de correcció d'esborralls.
 En cas negatiu
 - Justifiqueu per què no.
 - Poseu un exemple detallat en què no es corregeixi bé cap esborrall.
 - Rebem la paraula 221220
 - Quina és la seva síndrome?
 - 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.
 - Rebem la paraula 110102
 - Quina és la seva síndrome?
 - 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.
 - Rebem la paraula 022202
 - Quina és la seva síndrome?
 - 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.
 - Rebem la paraula 210120
 - Quina és la seva síndrome?
 - 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.
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.
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 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.
 - (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.
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.
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?
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.
- (b) Quina longitud té?
- (c) Quina dimensió té? Justifiqueu la resposta.
- (d) Demostreu que es tracta d'un codi cíclic.
- (e) Quin és el seu polinomi generador? Justifiqueu la resposta.
- (f) Quin és el seu polinomi de control?
- (g) Doneu una matriu de control de C_2 .
- (h) Quina és la distància mínima de C_2 ? Justifiqueu la resposta.

- (i) Quants errors es poden corregir en una paraula de C_2 ? Justifiqueu la resposta.
- (j) Quina és la síndrome de la paraula (100110)?
- (k) Si té errors expliqueu els passos per corregir-los i doneu la paraula corregida. Si no té errors demostreu que no en té.
- (l) Poseu un exemple de paraula amb dos errors que no es corregeixi de manera correcta.

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.
- (b) Quina longitud té?
- (c) Quina dimensió té? Justifiqueu la resposta.
- (d) Es tracta d'un codi cíclic? Justifiqueu la resposta.
- (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.
- (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.
- (g) Doneu una matriu de control de C_3 .
- (h) Quina és la distància mínima de C_3 ? Justifiqueu la resposta.
- (i) Quants errors es poden corregir en una paraula de C_3 ? Justifiqueu la resposta.
- (j) Quina és la síndrome de la paraula (212021)?
- (k) Si té errors, expliqueu els passos per corregir-los i doneu la paraula corregida. Si no té errors demostreu que no en té.
- (l) Doneu una paraula no nul·la del codi amb dos esborralls i corregiu-los explicant tots els passos.

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?
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.
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 anomenau-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.
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 C sobre $\mathbb{F}_4$ donat per les solucions a $\mathbb{F}_4^3$ del sistema
$$\begin{cases} x_1 + x_2 + x_3 = 0, \\ x_1 + \alpha x_2 + \alpha^2 x_3 = 0. \end{cases}$$
- (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.
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.
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.
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?
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 ,
 - $x^7 + \alpha x + 1$,
 - $x^4 + \alpha^3 x^3 + x^2 + \alpha x + \alpha^3$.
- (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?

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 anomeu-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.
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.

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

$$\det(V_3(1, \alpha^2, \alpha^5)) = (\alpha^2 - 1)(\alpha^5 - 1)(\alpha^5 - \alpha^2).$$
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}	$\alpha^2 + 1$

- (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.
3. (a) Comproveu que el polinomi $x^4 + x + 1$ sobre $\mathbb{Z}_2$
 - i. És irreductible.
 - ii. És primitiu.

- (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.
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.
8. (a) És $\mathbb{Z}_3$ un cos? Per què?
- (b) Comproveu que només hi ha tres polinomis mòncics (coeficient de grau màxim igual a 1) irreducibles de grau 2 a $\mathbb{Z}_3[x]$ i doneu-los.
- (c) Doneu un polinomi mònic $f(x)$ de grau 2 irreducible 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 dígit.
- (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.
9. (a) Construcció d'un cos finit.
- Comproveu que el polinomi $x^3 + x + 1$ és irreducible i primitiu sobre $\mathbb{Z}_2$.
 - Construïu $\mathbb{F}_8$ utilitzant aquest polinomi i doneu-ne una taula exponencial-vectorial.
- (b) Definiu el codi RS primitiu i en sentit estricte, amb longitud 7, capaç de detectar dos errors.
- Doneu-ne el polinomi generador.
 - Doneu-ne el polinomi de control.
 - Doneu-ne la longitud i la dimensió.
 - Doneu-ne una matriu generadora.
 - Doneu-ne una matriu de control.
 - Quants errors podem garantir que podrà corregir?

- (c) Codifiqueu de manera sistemàtica utilitzant el polinomi generador el primer bloc d'informació de la seqüència $01\alpha 01\alpha 01\alpha 01\alpha \dots$.
- (d) En quines posicions és sistemàtica la codificació anterior?
- (e) Corregiu els errors de la primera paraula de la seqüència $\alpha^3 0\alpha^4 \alpha^5 1\alpha 1\alpha^3 10\alpha^5 \alpha^4 \dots$.
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?
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?
12. (a) **Definició d'un codi**
 Anomenarem C a un codi primitiu, de Reed-Solomon, capaç de corregir dos errors, construït sobre el cos $\mathbb{F}_{3^2}$.
- Comproveu que el polinomi $x^2 + x + 2 \in \mathbb{F}_3$ és irreductible i utilitzeu-lo per construir $\mathbb{F}_{3^2}$.
 - Doneu l'equivalència vectorial-exponencial per a cada element de $\mathbb{F}_{3^2}$.
 - Doneu el polinomi generador del codi C .
 - Doneu la longitud, la dimensió i la distància mínima de C .
 - Doneu la matriu de control del codi C .
- (b) **Procés de codificació-descodificació**
 Codificarem la imatge . Tot seguit l'introduïrem en un canal ternari amb soroll additiu i, després, la descodificarem.
- Amb la tècnica de codificació sistemàtica per a codis cíclics, codifiqueu el primer bloc de l'anterior informació usant el codi C .
 - 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:
 $e = (12120000000000000000000000000000 \dots)$.
 Calculeu la paraula que trobarem a la sortida del canal.
 - Calculeu el polinomi localitzador d'errors necessaris per corregir el vector rebut.
 - Doneu la posició i el valor dels errors que cal corregir.
 - Doneu la primera paraula-codi de la codificació de la imatge (cadena de blancs, grisos i negres), després de la correcció d'errors.
 - Quin és el bloc d'informació que es dedueix que s'ha volgut enviar?
13. (a) **Definició d'un codi**
 Anomenarem C a un codi primitiu, de Reed-Solomon, capaç de corregir tres esborralls, construït sobre el cos $\mathbb{F}_{3^2}$.
- Comproveu que el polinomi $x^2 + x + 2 \in \mathbb{F}_3$ és irreductible i utilitzeu-lo per construir $\mathbb{F}_{3^2}$.
 - Doneu l'equivalència vectorial-exponencial per a cada element de $\mathbb{F}_{3^2}$.
 - Doneu el polinomi generador del codi C .
 - Doneu la longitud, la dimensió i la distància mínima de C .

v. Doneu la matriu de control del codi C .

(b) **Procés de codificació-descodificació**

Codificarem la imatge

0	1	0	0	0	1
---	---	---	---	---	---

 2 2 1 2 0 . Tot seguit l'introduïrem 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 .
 - ii. Multipliqueu la paraula obtinguda per la matriu de control. Especifiqueu totes les operacions. Quin és el resultat?
 - iii. El canal pel qual circularà la paraula codificada és un canal ternari en què hi ha un soroll additiu que ens donarà, en dígit, el vector d'error següent:
 $e = (01000000000000000000000000000000 \dots)$.
 Calculeu la paraula en símbols que trobarem a la sortida del canal.
 - iv. Calculeu el polinomi localitzador d'errors.
 - v. Doneu la posició i el valor dels errors que cal corregir.
 - vi. Doneu la primera paraula-codi de la codificació de la imatge (cadena de blancs, grisos i negres), després de la correcció d'errors.
 - vii. Quin és el bloc d'informació que es dedueix que s'ha volgut enviar?
14. (a) Digueu tots els cossos primers i tots els polinomis mòncics 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.
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?

16. (a) Construcció d'un cos finit.
- Comproveu que el polinomi $x^3 + x + 1$ és irreductible i primitiu sobre $\mathbb{F}_2$.
 - Anomenem α a la classe de x dins de $\mathbb{F}_2/(x^3 + x + 1)$. Doneu-ne una taula exponencial-vectorial.
- (b) Definiu un codi RS primitiu sobre el cos de l'apartat anterior capaç de corregir dos errors.
- Quina distància mínima hem d'agafar? Doneu-ne la longitud i la dimensió.
 - Doneu-ne el polinomi generador.
 - Doneu-ne una matriu generadora G a partir del polinomi generador.
 - Doneu una matriu de control H que tingui com a primera fila les potències no nul·les de α .
 - Calculeu el resultat de multiplicar la primera fila de G per la primera fila de H **indicant els càlculs**.
 - Calculeu $G \cdot H^T$.
- (c) Considerem el mateix codi RS que en el problema anterior.
- Codifiqueu de manera sistemàtica utilitzant el polinomi generador el primer bloc d'informació de la cadena de bits
11111000111110001111111111111000101010101010101010100011111000...
Doneu el resultat també com a cadena de bits.
 - Calculeu alguna síndrome de la paraula codificada indicant tots els càlculs intermedis.
- (d) Considerem el mateix codi RS que en els problemes anteriors.
- Rebem la cadena de bits 00110000000000010100. A quina cadena de símbols correspon?
 - Calculeu totes les síndromes de la paraula rebuda.
 - Quants errors té de símbol la paraula rebuda?
 - Quin és el polinomi localitzador d'errors?
 - Trobeu les posicions dels errors.
 - Calculeu el valor dels errors.
 - Doneu la cadena de bits corregida.
 - Quants errors de bit tenia la paraula enviada?
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
- $$011001100001110110100,$$
- $$110001000100111010000.$$
- Quina distància mínima hem d'agafar per al codi RS? Doneu-ne la longitud i la dimensió.
 - A quina cadena de símbols correspon la primera paraula?
 - A quina cadena de símbols correspon la segona paraula?
 - Calculeu totes les síndromes de la primera paraula rebuda i doneu tots els detalls del càlcul.
 - Calculeu totes les síndromes de la segona paraula rebuda i doneu tots els detalls del càlcul.
 - Quants errors té de símbol la primera paraula rebuda?
 - Quants errors té de símbol la segona paraula rebuda?
 - Si alguna o algunes de les paraules té algun error, quin és el polinomi localitzador d'errors?
 - Si alguna de les paraules té algun error, troba les posicions dels errors.
 - Calculeu el valor dels errors.
 - Si alguna o algunes de les paraules té algun error, doneu la cadena de bits corregida.
 - Quants errors de bit tenia la primera paraula enviada?
 - Quants errors de bit tenia la segona paraula enviada?

TEMA 3

Problemes d'aprofundiment

TEMA 3

Problemes d'aprofundiment

Índex

1	Aritmètica entera	213
2	Aritmètica modular	215
3	Aritmètica polinomial i cossos finits	218
4	Caracterització, existència i unicitat dels cossos finits	221
5	Codis lineals	222
6	Codis cíclics	225
7	Codis algebraics	227

1 Aritmètica entera

I.1. 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

I.2. Comproveu que 12345679 és un divisor de 111111111. Deduïu que 12345679 és un divisor de 22222222, 33333333, 44444444, etc.

I.3. Calculeu $(1+x)(1+x^2)(1+x^4)\cdots(1+x^{2^n})$.

I.4. Demostreu que, si $x \neq 1$, aleshores, $\frac{x^m-1}{x-1} = 1+x+x^2+\cdots+x^{m-1}$.

I.5. Demostreu que, si m és senar i $x \neq -1$, $\frac{x^m+1}{x+1} = 1-x+x^2-x^3+\cdots-x^{m-2}+x^{m-1}$.

I.6. Demostreu que si $2^n + 1$ és primer per algun enter n , aleshores n ha de ser una potència de 2.

I.7. Demostreu que, per a tot enter $n \geq 1$, es compleix

- $6 \mid n(n+1)(n+2)$
- $30 \mid n^5 - n$
- $13 \mid 4^{2n+1} + 3^{n+2}$

I.8. Demostreu que, per tot $n \in \mathbb{Z}$, la suma $\frac{n^5}{5} + \frac{n^3}{3} + \frac{7n}{15}$ és sempre un nombre enter.

I.9. Calculeu quants divisors té 720. Comproveu-ho amb sage.

I.10. Demostreu que si un enter $n > 1$ no és primer, aleshores tots els seus divisors són menors o iguals que $\sqrt{n}$.

I.11. Siguin a, b, c enters.

- (a) Demostreu que, si $a \mid b$, aleshores $ac \mid bc$.
- (b) Demostreu que, si $c \mid a$ i $c \mid b$, aleshores $a \mid b$ implica que $\frac{a}{c} \mid \frac{b}{c}$.

I.12. Siguin a, b, c enters. Demostreu que $\text{mcd}(a, b) = \text{mcd}(a+bc, b)$

I.13. Tenint en compte l'exercici anterior, escriviu en sage una funció que calcula el màxim comú divisor de dos nombres de manera recursiva.

I.14. Escriviu una funció de sage que, donada una parella d'enters, calculi el seu màxim comú divisor i els coeficients de la identitat de Bézout.

I.15. Siguin a, b dos enters i siguin $m = \text{mcd}(a, b)$, $M = \text{mcm}(a, b)$.

- (a) Demostreu que, si c és un múltiple comú de a i b , aleshores $M \mid c$.
- (b) Demostreu que, si d és un divisor comú de a i b , aleshores $d \mid m$.

I.16. Siguin a, b dos enters i siguin $m = \text{mcd}(a, b)$, $M = \text{mcm}(a, b)$. Demostreu que $m \cdot M = a \cdot b$.

I.17. Siguin a, b, c enters amb $c > 0$.

- (a) Demostreu que $\text{mcd}(ac, bc) = c \text{mcd}(a, b)$.

(b) Demostreu que, si $c \mid a$ i $c \mid b$, aleshores $\gcd\left(\frac{a}{c}, \frac{b}{c}\right) = \frac{\gcd(a,b)}{c}$.

I.18. (a) Comproveu que 40191 i 38143 són coprimers.

(b) Demostreu que no existeixen parelles d'enters a i b tals que $a - b = 625$ amb la propietat que el seu màxim comú divisor és parell.

I.19. Considerem els nombres de Fibonacci:

$F_0 = 0, F_1 = 1, F_2 = 1, F_3 = 2, F_4 = 3, F_5 = 5$, etc.,

definitos per la recurrència $F_i = F_{i-1} + F_{i-2}$ per $i \geq 2$.

(a) Demostreu que qualsevol parella de nombres de Fibonacci consecutius són coprimers.

(b) Volem calcular la identitat de Bézout de dos nombres de Fibonacci consecutius F_{i-1}, F_i , per $i \geq 5$.

- Preneu un exemple particular de dos nombres de Fibonacci consecutius F_{i-1}, F_i amb $i \geq 7$ i calculeu-ne la identitat de Bézout.
- Considerem el cas general de dos nombres de Fibonacci consecutius F_{i-1}, F_i amb $i \geq 5$. Qui són els quocients i els residus de la taula de divisions successives en el cas general?
- Quina és la identitat de Bézout de dos nombres de Fibonacci consecutius F_{i-1}, F_i , per $i \geq 5$?

I.20. Busqueu la definició de nombres primers bessons. Construïu una funció amb *sage* que donat n retorni totes les parelles de nombres primers bessons menors que n .

I.21. Construïu les següents funcions amb *sage*

(a) Una funció que, donats un enter positiu b i una llista d'enters positius $a_0, \dots, a_n$ que satisfan $0 \leq a_i < b$ per $0 \leq i \leq n$, retorni l'enter $c = \sum_{i=0}^n a_i b^i$ (en decimal).

(b) Una funció que faci l'operació inversa: Donats dos enters $b > 0$ i $c \geq 0$, calculi els enters $a_0, \dots, a_n$ amb $0 \leq a_i < b$ que satisfan l'equació anterior.

I.22. Els nombres d'Ulam es defineixen de la manera següent:

- $U_1 = 1$
- $U_2 = 2$
- U_i és el menor enter més gran que U_{i-1} i tal que pot ser escrit com $U_j + U_k$ per una única parella i, j amb $1 \leq i < j \leq i-1$.

Els primers nombres d'Ulam són 1, 2, 3, 4, 6, 8, 11, 13.

(a) Demostreu que hi ha un nombre infinit de nombres d'Ulam.

(b) Construïu una funció amb *sage* que donat un enter n retorni els primers n nombres d'Ulam.

(c) Demostreu que a partir de cert punt no hi pot haver tres nombres consecutius que siguin, tots tres, nombres d'Ulam. Quin és el punt a partir del qual es compleix?

(d) Demostreu que donats 5 nombres consecutius, com a molt dos d'ells poden ser d'Ulam.

I.23. Diem que un conjunt de la forma $\mathbb{N}_0 \setminus \{a_1, \dots, a_g\}$ amb $0 < a_1 < a_2 < \dots < a_g$ és un semigrup numèric si és tancat per la suma. Diem que el *gènere* del semigrup és g i, si $g > 0$, el *conductor* és $c = a_g + 1$.

(a) Quin és el nombre n_0 de semigrups de gènere 0? i el nombre n_1 de semigrups de gènere 1? I el nombre n_2 de semigrups de gènere 2?

(b) Demostreu que per tot semigrup numèric de gènere positiu es compleix $c \leq 2g$.

(c) Construïu una funció amb *sage* que donat un enter g calculi el nombre n_g de semigrups de gènere g .

(d) Comproveu experimentalment que, per tot g positiu, $n_g \geq n_{g-1}$ fins a un cert g .

(e) Comproveu experimentalment que, per tot $g > 1$, $n_g \geq n_{g-1} + n_{g-2}$ fins a un cert g .

(f) Comproveu experimentalment que la fracció $\frac{n_{g-1} + n_{g-2}}{n_g}$ tendeix a 1.

(g) Comproveu experimentalment que la fracció $\frac{n_g}{n_{g-1}}$ tendeix al nombre d'or.

NOTA: Les desigualtats $n_g \geq n_{g-1} + n_{g-2}$ i $n_g \geq n_{g-2}$ són a dia d'avui conjectures.

2 Aritmètica modular

- II.1.** (a) Demostreu que el quadrat de qualsevol enter és congruent amb 0 o amb 1 mòdul 4.
 (b) Demostreu que, si x i y són dos enters senars, aleshores $x^2 + y^2$ no és el quadrat de cap enter.
- II.2.** Demostreu els criteris de divisibilitat per 3, per 4, per 5, per 7, per 9 i per 11.
- II.3.** Demostreu que, si $a \equiv b \pmod{m}$, aleshores $\text{mcd}(a, m) = \text{mcd}(b, m)$.
- II.4.** Siguin $a, m \neq 0$.
 (a) Demostreu que si $ab \equiv ac \pmod{am}$, aleshores $b \equiv c \pmod{m}$.
 (b) Demostreu que si $ab \equiv ac \pmod{m}$, aleshores $b \equiv c \pmod{\frac{m}{\text{mcd}(a, m)}}$. (Aquest resultat generalitza l'anterior.)
- II.5.** Demostreu que, si $a \equiv b \pmod{m}$ i $a \equiv b \pmod{n}$ aleshores $a \equiv b \pmod{\text{mcm}(m, n)}$.
- II.6.** Calculeu $\text{mcd}(48m + 11, 42m + 8)$ en funció de m .
- II.7.** Siguin p un primer senar i $a \not\equiv 0 \pmod{p}$.
 (a) Demostreu que $x^2 \equiv a^2 \pmod{p}$ té dues i només dues solucions mòdul p .
 (b) Mostreu amb exemples que si no es compleixen les dues hipòtesis, aleshores el resultat anterior no és cert.
- II.8.** Teorema de Wilson
 (a) Demostreu que, si p és primer, aleshores
- $$(p-1)! \equiv \prod_{\{x \in \{1, \dots, p-1\} : x^2 \equiv 1 \pmod{p}\}} x \pmod{p}$$
- (b) Demostreu que, si p és primer, aleshores
- $$(p-1)! \equiv -1 \pmod{p}$$
- II.9.** Demostreu que, si p és primer, aleshores $\text{mcd}(p, (p-1)!) = 1$.
- II.10.** Siguí p un primer. Demostreu que si $x^2 \equiv -1 \pmod{p}$ té solució, aleshores, o bé $p = 2$, o bé $p \equiv 1 \pmod{4}$.
- II.11.** Siguí n un nombre enter. Demostreu les propietats següents.
 (a) Si n és primer, aleshores $2^n - 2 \equiv 0 \pmod{n}$
 (b) Si n no és divisible per 7, aleshores $n^{12} - 1 \equiv 0 \pmod{7}$.
 (c) $n^{13} - n$ és divisible per 2, 3, 5, 7 i 13.
 (d) Si n és un nombre compost més gran que 5, aleshores $(n-1)! \equiv 0 \pmod{n}$.
- II.12.** Considerem altra vegada els nombres de Fibonacci:
 $F_0 = 0, F_1 = 1, F_2 = 1, F_3 = 2, F_4 = 3, F_5 = 5$, etc.,
 definits per la recurrència $F_i = F_{i-1} + F_{i-2}$ per $i \geq 2$.
 A partir de la Identitat de Bézout de dos nombres de Fibonacci consecutius,
 (a) Podem deduir qui és l'invers de F_{i-1} a $\mathbb{Z}_{F_i}$?
 (b) Podem deduir quant val $F_{i-1}^2 \pmod{F_i}$, per $i \geq 5$?
 (c) Quin és l'ordre de F_{i-1} a $\mathbb{Z}_{F_i}$ per $i \geq 5$?
 (d) Què podem dir de $\phi(F_i)$ per $i \geq 5$?

- II.13.** Els codis de barres van néixer amb la intenció d'identificar productes de manera automàtica. Cada producte va associat a un codi diferent i a una representació pictòrica que es pot escanejar fàcilment. La majoria dels productes que comprem duen un codi de barres creat d'acord amb el EAN-13. El d'EAN-13 consta de 12 dígit que s'assignen de manera única a un producte, i un dígit de control. Aquest darrer dígit no aporta informació sobre el producte, però permet detectar algunes lectures errònies del codi. L'últim dígit es calcula a partir dels 12 anteriors de manera que la suma de totes les xifres en posició senar més el triple de la suma de totes les xifres en posició parell és un múltiple de 10.

Construïu una funció amb sage que detecti si un codi de barres conté algun error.

- II.14.** (a) Demostreu que, si $d \mid n$, aleshores

$$\#\{b : 1 \leq b \leq n, \text{mcd}(b, n) = d\} = \phi(n/d).$$

Construïu una funció amb sage que construeixi el conjunt $\{b : 1 \leq b \leq n, \text{mcd}(b, n) = d\}$ i que calculi quants elements té. Comproveu el resultat que acabeu de demostrar per una varietat de nombres n .

- (b) Demostreu que

$$\sum_{d \mid n} \phi(d) = n.$$

Construïu una funció amb sage que calculi la suma $\sum_{d \mid n} \phi(d)$. Comproveu el resultat que acabeu de demostrar per una varietat de nombres n .

- II.15.** El 1976, Whitfield Diffie i Martin Hellman van presentar un protocol d'intercanvi de claus criptogràfiques que es pot dur a terme a través d'un canal de comunicació insegur, on potser hi ha altres usuaris llegint els missatges intercanviats. A continuació veurem una versió simplificada del protocol. Suposem que Alice i Bob són dues persones que volen obtenir una clau secreta que només sigui coneguda per ells dos.

(A1) Alice tria un nombre primer (gran) p i busca un generador g de $\mathbb{Z}_p^*$.

(A2) Alice tria un enter $0 < x < p$ i calcula $h_A = g^x$.

(A3) Alice envia a Bob p , g i h_A . Alice manté x secreta.

(B1) Bob genera $0 < y < p$ i calcula $h_B = g^y$.

(B2) Bob envia h_B a Alice i calcula $k_B = h_A^y$.

(A4) Alice calcula $k_A = h_B^x$.

Al final del protocol, Alice obté k_A i Bob obté k_B . La seguretat del protocol rau en la dificultat de calcular el logaritme discret. Diem que x és el logaritme de h en base g si $g^x = h$, i escrivim $x = \log_g(h)$.

(a) Comproveu que, si no hi ha errors de transmissió, al final del protocol les claus obtingudes satisfan $k_A = k_B$.

(b) Descriviu un algoritme per calcular el logaritme discret d'un element. Feu una estimació del nombre d'operacions necessàries per calcular el logaritme discret d'un enter de n bits.

(c) Considereu el cas que un atacant té accés a la comunicació i intercepta h_A i h_B . Doneu un algoritme que, amb un ordinador convencional, li permeti obtenir k_A .

(d) Tenint en compte les respostes als dos apartats anteriors, discuteix l'eficiència de l'atac i la possibilitat de dur-lo a terme.

- II.16.** El 1977, Ron Rivest, Adi Shamir i Len Adleman van dissenyar un esquema d'encryptació de clau pública, que amb el temps s'ha anomenat RSA. A continuació veurem una versió simplificada de l'esquema RSA

Suposem que Alice i Bob es volen comunicar. Alice genera una parella de claus (sk_A, pk_A) on pk_A és una clau que es dona a conèixer a tothom, és pública, i sk_A és una clau que Alice ha de mantenir secreta. Quan Bob vol enviar un missatge a Alice, xifrarà el missatge emprant pk_A . Quan Alice rebí el missatge xifrat, el podrà desxifrar emprant sk_A . La seguretat i la correcció de l'esquema es basa en alguns problemes d'aritmètica modular.

- (A1) Alice tria dos nombres primers (grans) p i q . Calcula $N = pq$.
- (A2) Alice tria un enter $0 < e < N$ tal que $\gcd(e, \phi(N)) = 1$. Calcula $d = e^{-1} \bmod \phi(N)$. O sigui, d i e satisfan $ed = 1 \bmod \phi(N)$.
- (A3) Alice publica $pk = (N, e)$ i es guarda $sk = (N, d)$.
- (B1) Si Bob té un missatge $m \in \mathbb{Z}_N^*$ per enviar a Alice i coneix pk , calcula $c = m^e \bmod N$.
- (B2) Bob envia c a Alice.
- (A4) Al rebre c , Alice calcula $m' = c^d \bmod N$. Si no hi ha hagut errors de transmissió, $m' = m$.
- Al final d'aquest protocol, Alice ha rebut m' .
- (a) Comproveu que, si no hi ha errors de transmissió, $m' = m$. O sigui, comproveu que $(m^e)^d = m \bmod N$.
- (b) Algú que interceptés la comunicació, podria arribar a obtenir N , e i c . Dissenyeu un atac que permeti obtenir m .
- (c) Sigui N un enter de n bits. Analitzeu l'eficiència del vostre atac: feu una estimació del nombre d'operacions que es requereixen en funció de n .

II.17. L'operació de desxifratge de RSA requereix calcular $c^d \bmod N$, on habitualment d i N són nombres enters grans. A continuació, veurem una tècnica per realitzar aquesta operació de manera més eficient. Aquesta tècnica s'utilitza en OpenSSL i altres biblioteques. L'usuari que realitza aquesta operació coneix p i q , els nombres primers que satisfan $N = pq$. L'usuari calcula els enters d_p , d_q i q' , definits de la següent manera:

- (a) $d_p = d \bmod p - 1$
- (b) $d_q = d \bmod q - 1$
- (c) q' és l'invers de q mòdul p . Satisfà $q \cdot q' \equiv 1 \bmod p$.

Després, calcula m_1 , m_2 , h i m' de la manera següent:

- (a) $m_1 = c^{d_p} \bmod p$
- (b) $m_2 = c^{d_q} \bmod q$
- (c) $h = q' \cdot (m_1 - m_2) \bmod p$
- (d) $m' = m_2 + h \cdot q \bmod N$

Responen als següents apartats:

- (a) Comproveu que $c^d \equiv c^{d_p} \bmod p$.
- (b) Reduïu m' mòdul p i q i comproveu que

$$\begin{cases} m' \equiv m_1 \bmod p \\ m' \equiv m_2 \bmod q \end{cases}$$

- (c) Aplicant el teorema xinès del residu, raoneu que m' l'únic valor $\bmod N$ que satisfà aquest sistema d'equacions.
- (d) Mostreu que si $c = m^e \bmod N$, aleshores es compleix que $m' = m$.
- (e) Discutiu quin creieu que és el guany computacional que s'obté calculant m d'aquesta manera i no com hem vist a l'exercici anterior (fent el càlcul directament mòdul N).

II.18. Els algoritmes de xifrat i desxifrat dels esquemes basats en RSA requereixen la computació de multiplicacions d'enters de molts dígits. Actualment, els paràmetres més comuns requereixen multiplicacions d'enters de 2048 bits. Aquests enters són grans i, a nivell hardware, no caben en registres convencionals. Per tant, els enters s'han d'emmagatzemar per parts en diferents registres, i les multiplicacions requereixen operacions amb molts registres. Una manera de calcular els productes modulars és amb el mètode de *interleaving*. Aquest mètode descompon la multiplicació en diverses operacions seqüencials simples. L'algoritme és el següent.

Suposem que hem de calcular $ab \bmod n$, on a i b són enters inferiors a n , i b es pot representar amb k bits: $b = \sum_{i=0}^{k-1} b_i 2^i$. Observeu que

$$ab = \sum_{i=0}^{k-1} ab_i 2^i$$

La computació es fa iterativament, començant amb els exponents més alts:

- (a) Calculeu $p_{k-1} = ab_{k-1} \bmod n$
- (b) Calculeu $p_{k-2} = 2p_{k-1} + ab_{k-2} \bmod n$
- (c) Seguiu iterativament, calculant $p_i = 2p_{i+1} + ab_i \bmod n$ fins que $i = 0$, obtenint el resultat.

Comproveu que l'algoritme és correcte. Mostreu que l'algoritme redueix la multiplicació a com a molt k sumes i k multiplicacions per 2. Discutiu la idoneïtat de l'algoritme.

3 Aritmètica polinomial i cossos finits

- III.1. Suposem que p és primer i $a(x), b(x) \in \mathbb{Z}_p[x]$. Demostreu que el màxim comú divisor mònic de $a(x)$ i $b(x)$ és únic.
- III.2. Doneu un exemple de polinomis $a(x), b(x)$ de $\mathbb{Z}_m[x]$ per alguna m tals que el quocient i/o el residu de la divisió de $a(x)$ entre $b(x)$
 - (a) no existeixin,
 - (b) no siguin únics.
- III.3. Comproveu si $x - 5$ divideix $x^4 + x^2 + 1$ a $\mathbb{Z}_2[x]$, a $\mathbb{Z}_3[x]$, a $\mathbb{Z}_5[x]$ i a $\mathbb{Z}_7[x]$.
- III.4. (a) Demostreu que $x^n - 1 \mid x^m - 1$ si i només si $n \mid m$.
 (b) Demostreu que $\text{mcd}(x^m - 1, x^n - 1) = x^d - 1$, on $d = \text{mcd}(m, n)$.
- III.5. Suposem que p és un primer senar. Descomponeu $f(x) = x^{p-1} - 1$ a $\mathbb{Z}_p[x]$ en factors lineals i utilitzeu la factorització per demostrar el Teorema de Wilson (si p és un primer senar, aleshores $(p-1)! \equiv -1 \pmod p$).
- III.6. Calculeu el màxim comú divisor de la següent parella de polinomis, i expresseu-lo com a combinació lineal polinomial dels polinomis inicials.
 - (a) $x^4 + 1$ i $x^2 + 1$, definits a $\mathbb{Z}_2[x]$
 - (b) $x^4 + 1$ i $x^2 + 1$, definits a $\mathbb{Z}_3[x]$
 - (c) $x^5 + x^2 + x + 1$ i $x^3 + 1$, definits a $\mathbb{Z}_2[x]$
 - (d) $x^5 + x^2 + x + 1$ i $x^3 + 1$, definits a $\mathbb{Z}_3[x]$
 - (e) $x^5 + x^2 - x - 1$ i $x^3 - 1$, definits a $\mathbb{Z}_3[x]$
- III.7. Demostreu que $x^5 + x^4 + x^2 + x + 1$ és irreductible a $\mathbb{Z}_2[x]$.
- III.8. (a) Trobeu els divisors de zero de $\mathbb{Z}_3[x]/(x^2 + 2x + 1)$.
 (b) Trobeu els divisors de zero de $\mathbb{Z}_3[x]/(x^3 + 2x^2 + x)$.
- III.9. La descomposició dels nombres enters en sumes mínimes de quadrats d'altres enters és un problema clàssic. Es coneix que qualsevol enter descompondre en suma de quatre quadrats. També se sap que un nombre senar és suma dels quadrats de dos enters si i només si és congruent amb 1 mòdul 4.
 - (a) Escriuiu una rutina que donat un enter en doni la descomposició en una suma de quadrats amb el mínim nombre de termes possibles.
 - (b) Demostreu que, en un cos finit, tot element és suma de dos quadrats.

- (c) Escriu una funció de sage que, donat un element d'un cos finit en doni la descomposició com a suma de dos quadrats.

III.10. L'Advanced Encryption Standard (AES) és un esquema criptogràfic de clau privada que va ser estandaritzat pel National Institute of Standard and Technology (NIST) a finals del segle passat. Des d'aleshores, AES és el principal esquema de clau privada, i el fem servir a diari quan establim comunicacions segures.

L'AES és un esquema de xifratge de bloc: Les dades es divideixen en diversos blocs i, durant part del procés, cada bloc es processa per separat. Per processar cada bloc, es realitzen operacions aritmètiques com productes i sumes en $\mathbb{F}_{128}$, $\mathbb{F}_{2^8}[x]/(x^4+1)$, i $\mathbb{Z}_2^{16}$. A continuació analitzarem l'operació Bytesub. L'operació Bytesub consisteix en dues transformacions. A partir d'un byte a , primer calculem un valor auxiliar $c \in \mathbb{F}_{2^8}$, i finalment calculem $b \in \mathbb{F}_{2^8}$ a partir de c .

- (a) Prenem el cos finit $\mathbb{F}_{2^8} = \mathbb{Z}_2[x]/(m(x))$, on

$$m(x) = 1 + x + x^3 + x^4 + x^8 \in \mathbb{Z}_2[x]$$

és un polinomi irreductible de grau 8. Sigui a un byte d'estat. Aquest byte es pot escriure com

$$a = a_7 a_6 a_5 a_4 a_3 a_2 a_1 a_0,$$

on $a_k \in \{0, 1\}$.

- (b) Aquest element a ara el veurem com un element del cos finit $\mathbb{F}_{2^8}$, fent servir la notació vectorial. O sigui, que a es correspon amb

$$a_7 \alpha^7 + a_6 \alpha^6 + a_5 \alpha^5 + a_4 \alpha^4 + a_3 \alpha^3 + a_2 \alpha^2 + a_1 \alpha + a_0,$$

on $\alpha = [x] \in \mathbb{F}_{2^8}$

- (c) Si $a = 0$, aleshores $c = 0 \in \mathbb{F}_{2^8}$. Si $a \neq 0$, aleshores $c = a^{-1}$. Altre cop, escriurem c en notació vectorial:

$$c = c_7 \alpha^7 + c_6 \alpha^6 + c_5 \alpha^5 + c_4 \alpha^4 + c_3 \alpha^3 + c_2 \alpha^2 + c_1 \alpha + c_0.$$

- (d) Després apliquem la següent transformació afí definida a $\mathbb{Z}_2$, obtenint b , el resultat de Bytesub:

$$b = \begin{bmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \\ b_4 \\ b_5 \\ b_6 \\ b_7 \end{bmatrix} = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 \end{bmatrix} \begin{bmatrix} c_0 \\ c_1 \\ c_2 \\ c_3 \\ c_4 \\ c_5 \\ c_6 \\ c_7 \end{bmatrix} + \begin{bmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 0 \\ 1 \\ 1 \\ 0 \end{bmatrix}$$

i

$$b = b_7 b_6 b_5 b_4 b_3 b_2 b_1 b_0,$$

Donada l'especificació d'aquesta funció, calculeu el resultat d'aplicar-la als següents bytes.

- (a) Calculeu $\text{Bytesub}(a)$ per $a = 00000001$.
 (b) Sigui $a = 00000010$. Comproveu que $\alpha^{-1} = (\alpha^7 + \alpha^3 + \alpha^2 + 1)$ a $\mathbb{F}_{2^8} = \mathbb{Z}_2[x]/(m(x))$, i després calculeu $\text{Bytesub}(a)$.

III.11. L'operació Mixcolumn d'AES també es pot descriure a través d'operacions polinomials. En aquest cas, els blocs d'informació a processar, que tenen 128 bits, es divideixen en quatre columnes de 32 bits, i cada una d'aquestes columnes es veu com un polinomi sobre $\mathbb{F}_{2^8}$:

$$a(X) = a_{0,j} + a_{1,j}X + a_{2,j}X^2 + a_{3,j}X^3 \in \mathbb{F}_{2^8}[X]$$

Com abans, es pren $\mathbb{F}_{2^8} = \mathbb{Z}_2[x]/m(x)$, on

$$m(x) = 1 + x + x^3 + x^4 + x^8 \in \mathbb{Z}_2[x]$$

L'operació que s'executa a Mixcolumn és

$$b(X) = c(X)a(X) \bmod 1 + X^4$$

on $c(X) = '02' + '01'X + '01'X^2 + '03'X^3$ és un polinomi fixat amb coeficients a $\mathbb{F}_{2^8}$, i els coeficients estan escrits en hexadecimal. Com a exemple de codificació hexadecimal, podem veure que '2B' es correspon a la seqüència de bits 00101011, que es correspon al polinomi

$$0\alpha^7 + 0\alpha^6 + 1\alpha^5 + 0\alpha^4 + 1\alpha^3 + 0\alpha^2 + 1\alpha^1 + 1\alpha^0 \in \mathbb{F}_{2^8}$$

Per tant, '2B' es correspon amb $\alpha^5 + \alpha^3 + \alpha + 1 \in \mathbb{F}_{2^8}$.

(a) Comproveu que aquesta operació es pot executar fent la següent operació matricial:

$$\begin{bmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \end{bmatrix} = \begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix} \cdot \begin{bmatrix} a_0 \\ a_1 \\ a_2 \\ a_3 \end{bmatrix}$$

(b) Apliqueu la operació Mixcolumn a la columna determinada per $a_{0,1} = 00$, $a_{1,1} = 01$, $a_{2,1} = 03$, i $a_{3,1} = 10$.

III.12. El 1994, Peter Shor va presentar algoritmes eficients que empen operacions quàntiques per factoritzar nombres enters i per calcular el logaritme discret. Aquest resultat és trascendental per la criptografia perquè, si s'arribessin a construir ordinadors quàntics suficientment potents, gran part de les comunicacions actuals esdevindrien insegures. A continuació presentem un algoritme simplificat per factoritzar $N = pq$, on p i q són primers. Aquest algoritme es pot executar en un ordinador convencional (però llavors no és eficient).

1. Preneu un enter aleatori $1 \leq a \leq N$. Si no és coprimer amb N , ja podeu descompondre N i ja podeu parar. Si és coprimer amb N , continueu.
2. Trobeu l'ordre d' a : Calculeu potències d' a mòdul N fins que trobeu r que satisfà

$$a^r = 1 \bmod N$$

3. Sabem que $a^r - 1 = 0 \bmod N$, i per tant $a^r - 1 = kN$ per algun k . Si r és imparell, torna al primer pas.
4. Si r és parell, llavors

$$a^r - 1 = (a^{\frac{r}{2}} + 1)(a^{\frac{r}{2}} - 1) = kN$$

Per tant, els factors de N divideixen $(a^{\frac{r}{2}} + 1)$ o $(a^{\frac{r}{2}} - 1)$.

5. Calculeu $x = \gcd(a^{\frac{r}{2}} + 1, N)$
6. Si $x = 1$ o $x = N$, torneu al primer pas. Si $x \neq 1, N$, aleshores x és un divisor de N .
7. Dividiu N per x per obtenir la factorització completa.

El principal avantatge de l'algoritme de Shor és que el segon pas es pot fer de manera eficient amb una operació quàntica que està relacionada amb la transformada de Fourier. En canvi, amb un ordinador convencional és molt costós.

- (a) Feu una estimació de la probabilitat de trobar un $1 \leq a \leq N$ que no és coprimer amb N (pas 1). Expliqueu per què, en aquest cas, ja podem descompondre N .
- (b) Expliqueu per què no es pot donar el cas que els factors de N divideixin $(a^{\frac{r}{2}} - 1)$ (pas 4). Per aquest motiu, en el pas 5 assumim que els factors de N divideixen $(a^{\frac{r}{2}} + 1)$.

- (c) Digueu quins són els possibles ordres dels elements coprimers amb N .
- (d) Feu una estimació dels nombre de Z_N^* que tenen ordre $\phi(N)$. Per aquests casos, feu una estimació del nombre d'exponenciacions necessàries per trobar l'ordre.

L'últim exercici mostra que, en el pitjor cas, els càlculs requerits per trobar l'ordre dels elements és molt costós. Es pot veure que, en general, per quasi tots els elements també és una operació costosa.

III.13. Feu servir l'algoritme anterior per factoritzar $N = 15$.

4 Caracterització, existència i unicitat dels cossos finits

IV.1. Demostreu que si en un cos finit es dona que $\underbrace{1 + \dots + 1}_m = 0$, aleshores m ha de ser un múltiple de la característica.

IV.2. Demostreu que si existeix un morfisme entre dos cossos diferents, aleshores han de tenir la mateixa característica.

IV.3. Demostreu que si un cos finit F té p^m elements, aleshores la característica de F és p .

IV.4. (a) Demostreu que si K , F són cossos finits i K és subcòs de F , aleshores $|F| = |K|^m$ per algun enter positiu m .

(b) Demostreu que $\mathbb{F}_{p^i}$ és subcòs de $\mathbb{F}_{p^j}$ si i només si i divideix j .

IV.5. Sigui p un nombre primer. Feu un gràfic del reticle de subcossos de $\mathbb{F}_{p^{12}}$, $\mathbb{F}_{p^{16}}$, $\mathbb{F}_{p^{20}}$ i $\mathbb{F}_{p^{60}}$.

IV.6. Demostreu que en un cos de característica p tot element té una única arrel p -èssima.

IV.7. Sigui F un cos de cardinal q .

(a) Si β és un element primitiu de F , quin és l'ordre de β^i ?

(b) Si $d \mid q - 1$, quants elements d'ordre d hi ha dins de F ?

(c) Demostreu que hi ha exactament $\phi(q - 1)$ elements primitius.

IV.8. Sigui F un cos de cardinal q . Doneu un mètode per construir una successió $\alpha_1, \alpha_2, \dots, \alpha_k$ d'elements de F^* tal que

$$\text{ord}(\alpha_1) < \text{ord}(\alpha_2) < \dots < \text{ord}(\alpha_k) = q - 1$$

Digueu quin és el valor màxim de k .

IV.9. Demostreu que si p és primer, aleshores $x^2 \equiv -1 \pmod{p}$ té solució si i només si $p = 2$ o si $p \equiv 1 \pmod{4}$.

IV.10. Demostreu que si $p \equiv 1 \pmod{4}$, aleshores $(\frac{p-1}{2})!^2 \equiv -1 \pmod{p}$.

IV.11. (a) Sigui $k \geq 1$. Proveu que a $\mathbb{Z}_p$, o bé k , o bé $-k$, o bé -1 és un quadrat.

(b) Proveu que per a tot primer p el polinomi $x^4 + 1 \in \mathbb{Z}_p[x]$ no és irreductible.

(Indicació: Proveu que sempre té un factor de grau 2.)

IV.12. Comproveu que $x^4 + x^3 + x^2 + x + 1$ és un polinomi irreductible de $\mathbb{Z}_2[x]$ i que no és primitiu. Podeu donar un element primitiu de $\mathbb{Z}_2[x]/(x^4 + x^3 + x^2 + x + 1)$? Podeu donar-los tots?

IV.13. Per quins primers p el conjunt $\mathbb{Z}_p[x]/(x^2 + 1)$ és un cos? I $\mathbb{Z}_p[x]/(x^4 + 1)$?

IV.14. Sigui $F = \mathbb{Z}_3[x]/(x^2 + 1)$ i diem α a la classe de x . Trobeu el polinomi mínim de α i $\alpha + 1$.

IV.15. Sigui $F = \mathbb{Z}_2[x]/(x^4 + x + 1)$ i diem $\alpha = [x]$

- (a) Construïu la taula d'equivalències de F , i calculeu l'ordre de cada element.
- (b) Doneu el polinomi mínim sobre $\mathbb{Z}_2[x]$ de cada element del cos.
- (c) Doneu un isomorfisme explícit entre $\mathbb{Z}_2[x]/(x^4 + x^3 + 1)$ i $\mathbb{Z}_2[x]/(x^4 + x + 1)$.

IV.16. Descomponeu sobre $\mathbb{Z}_2$ el polinomi $x^4 - x$, $x^8 - x$, $x^{16} - x$ i $x^{32} - x$.

IV.17. Sigui p un primer, i sigui $f(x) \in \mathbb{Z}_p[x]$ un polinomi irreductible.

- (a) Demostreu que $f(x)$ divideix $x^{p^{\text{grau}(f)}} - x$.
- (b) Demostreu que $x^{p^n} + x$ no té cap factor irreductible de grau n .

IV.18. L'operació Mixcolumn d'AES també es pot descriure a través d'operacions polinomials. En aquest cas, els blocs d'informació a processar, que tenen 128 bits, es divideixen en quatre columnes de 32 bits, i cada una d'aquestes columnes es veu com un polinomi sobre $\mathbb{F}_{2^8}$:

$$a(X) = a_{0,j} + a_{1,j}X + a_{2,j}X^2 + a_{3,j}X^3 \in \mathbb{F}_{2^8}[X]$$

Com abans, es pren $\mathbb{F}_{2^8} = \mathbb{Z}_2[x]/m(x)$, on

$$m(x) = 1 + x + x^3 + x^4 + x^8 \in \mathbb{Z}_2[x]$$

L'operació que s'executa a Mixcolumn és

$$b(X) = c(X)a(X) \bmod 1 + X^4$$

on $c(X) = '02' + '01'X + '01'X^2 + '03'X^3$ és un polinomi fixat amb coeficients a $\mathbb{F}_{2^8}$, i els coeficients estan escrits en hexadecimal. Com a exemple de codificació hexadecimal, podem veure que '2B' es correspon amb la seqüència de bits 00101011, que es correspon amb el polinomi

$$0\alpha^7 + 0\alpha^6 + 1\alpha^5 + 0\alpha^4 + 1\alpha^3 + 0\alpha^2 + 1\alpha^1 + 1\alpha^0 \in GF(2^8)$$

Per tant, '2B' es correspon amb $\alpha^5 + \alpha^3 + \alpha + 1 \in \mathbb{F}_{2^8}$

- (a) Comproveu que aquesta operació es executa fent la següent operació matricial:

$$\begin{bmatrix} b_0 \\ b_1 \\ b_2 \\ b_3 \end{bmatrix} = \begin{bmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{bmatrix} \cdot \begin{bmatrix} a_0 \\ a_1 \\ a_2 \\ a_3 \end{bmatrix}$$

- (b) Apliqueu la operació Mixcolumn a la columna determinada per $a_{0,1} = 00$, $a_{1,1} = 01$, $a_{2,1} = 03$, i $a_{3,1} = 10$.

5 Codis lineals

V.1. El número internacional normalitzat per a llibres (ISBN) és un identificador únic per a publicacions escrites. Actualment, el format estàndard és l'ISBN-13, però anys enrere l'estàndard era l'ISBN-10 (vegeu el següent exercici). L'ISBN-10 és un número de 10 dígit, i es pot veure com element d'un codi de longitud 10 sobre en el que l'últim element element és redundant. Els nou primers elements són dígit que donen informació sobre l'idioma, l'editorial i el número dins l'editorial. L'últim element es tria de de la següent manera:

Sigui $x_1, \dots, x_9$ els primers 9 dígit, començant per l'esquerra. Aleshores es calcula l'enter $x_{10} \in \{0, \dots, 10\}$ que satisfà

$$\sum_{i=1}^{10} (10 - i)x_i = 0 \pmod{11}$$

Si x_{10} és un enter entre 0 i 9, l'últim element de l'identificador és x_{10} . Si $x_{10} = 10$, aleshores l'últim element és la lletra X.

Per tant, podem veure aquests identificadors com paraules d'un codi sobre $\mathbb{Z}_{11}$ de dimensió 9. Demostreu les següents propietats:

- (a) El codi ISBN és capaç de detectar un error.
- (b) El codi ISBN és capaç de detectar dos errors, si aquests consisteixen en la transposició de dos dígit.
- (c) El codi ISBN és capaç de corregir un esborrall.

V.2. L'ISBN-13 és un identificador que és equivalent al ISBN-10, però té certes diferències. Aquest format es va estandaritzar per tal que aquests identificadors fossin compatibles amb els EAN-13.

En aquest cas, els ISBN-13 són nombres enters decimals de 13 dígit. Els tres primers dígit per l'esquerra són 978, identificant que correspon a un llibre. Els següents 9 dígit són els mateixos que els primers 9 de ISBN-10. L'últim dígit de ISBN-13 és redundant, i es calcula de manera diferent que a ISBN-10.

Segui $x_1, \dots, x_{10}$ els primers 9 dígit, començant per l'esquerra. Aleshores es calcula l'enter $x_{13} \in \mathbb{Z}_{10}$ que satisfà

$$x_1 + 3x_2 + x_3 + 3x_4 + \dots + 3x_{12} + x_{13} = 0 \pmod{10}$$

O sigui, la suma dels dígit en posicions imparells més el triple de la suma dels dígit en posició imparell és un múltiple de 10.

El nou format té l'avantatge que l'identificador és un nombre decimal. Tanmateix, es perden propietats de detecció d'errors. Quins errors detectables amb la codificació ISBN-10 no ho són amb ISBN-13?

V.3. Afegir redundància en els nombres identificadors és una pràctica comuna en molts àmbits, incloent els identificadors de documents personals. A Espanya, el Número d'Identificació Fiscal (NIF) consisteix en un número decimal de 8 dígit seguit d'una lletra. Aquest identificador apareix al DNI. La lletra del NIF es pot veure com un element redundant. Per calcular-la, es redueix mòdul 23 el nombre de 8 dígit, i després s'assigna la lletra d'acord amb la correspondència següent:

A=3; B=11; C=20; D=9; E=22; F=7; G=4; H=18; J=13; K=21; L=19; M=5; N=12; P=8; Q=16; R=1; S=15; T=0; V=17; W=2; X=10; Y=6; Z=14.

Descriviu la capacitat per detectar i corregir errors d'aquest identificador.

- V.4.** (a) Doneu justificadament un polinomi en x que generi $\mathbb{F}_4$.
 (b) Doneu una taula exponencial-vectorial de $\mathbb{F}_4$.
 (c) Digueu 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 donant el resultat també en 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.

V.5. Donat un codi ternari que té per matriu generadora:

$$G = \begin{pmatrix} 1 & 0 & 2 & 0 & 1 \\ 0 & 1 & 0 & a & 2 \end{pmatrix}$$

- (a) Calcula el valor de a de manera que el codi tingui la màxima capacitat correctora.
- (b) Calcula el valor de a pel qual es compleixi que el vector $v = (2, 1, 1, 1, 1)$ sigui una paraula-codi.
- (c) Fes la taula de síndromes per poder portar a terme una descodificació incompleta i digues, pels diferents valors de a , quina és la informació associada al vector rebut $w = (10212)$.

V.6. Considerem el codi binari i lineal definit per les paraules codi:

$$(a_1, a_2, a_3, a_4, a_5, a_1 + a_2 + a_4 + a_5, a_1 + a_3 + a_4 + a_5, a_1 + a_2 + a_3 + a_5, a_1 + a_2 + a_3 + a_4)$$

- (a) Doneu una matriu de control i una matriu generadora d'aquest codi. Trobeu els valors de n, k, d .
- (b) Afegiu a la matriu de control trobada una columna desena i una nova equació, donada per:

$$a_1 + a_2 + a_3 + a_4 + a_5 + a_6 + a_7 + a_8 + a_9 + a_{10} = 0$$

Trobeu la nova matriu generadora. Quant val ara la nova distància mínima?

- (c) Doneu les taules de descodificació via síndrome per aquest segon codi.

V.7. Sigui C un codi lineal sobre $\mathbb{F}_q$ de longitud n i dimensió k . Sigui $1 \leq i \leq n$.

- (a) Demostreu que, a la posició i -èsima de les paraules del codi, o bé totes les paraules tenen un 0, o bé cada element de $\mathbb{F}_q$ apareix amb la mateixa freqüència.
- (b) Si comptem el nombre de paraules del codi en què hi ha un 0 a la posició i -èsima, digueu quantes paraules trobarem.

V.8. Diem que un codi binari és de *Hamming* de paràmetre m si la seva matriu de control té per columnes tots els vectors binaris no nuls de longitud m .

- (a) Doneu la matriu de control del codi de Hamming de paràmetre 3.
- (b) Determineu la longitud, la dimensió i la distància mínima d'un codi de Hamming de paràmetre m .

V.9. En aquest exercici analitzem dues operacions que permeten obtenir altres codis lineals, que són *puncturing* i *shortening*. Sigui C un codi lineal de longitud n , dimensió k i distància mínima $d \geq 2$.

- (a) El codi obtingut per *shortening* C a la posició i ($1 \leq i \leq n$) és el codi que obtenim en separar totes les paraules que tenen un 0 a la posició i -èsima i en posteriorment eliminar aquesta posició en totes les paraules del conjunt separat.
- (b) El codi obtingut per *puncturing* C a la posició i ($1 \leq i \leq n$) és el codi que obtenim eliminant la coordenada i de les paraules del codi.

Per cadascuna d'aquestes operacions, què podem dir de la longitud, la dimensió, la distància mínima, les matrius generadores i les matrius de control del codi obtingut?

V.10. Així com a l'exercici anterior hem vist maneres de reduir un codi lineal, en aquest exercici veiem una manera d'extendre'l. Si C és un codi binari de longitud n , definim el codi estès C' com:

$$C' = \{(c_1, c_2, \dots, c_n, c_{n+1}) : (c_1, c_2, \dots, c_n) \in C, \sum_{i=1}^{n+1} c_i = 0\}$$

Si C és un codi lineal de matriu generadora G i matriu de control H , trobeu, en funció d'aquestes, la matriu generadora i de control del codi C' . Si C té distància mínima d , trobeu la distància mínima de C' .

V.11. Sigui C un codi lineal binari de longitud n i dimensió k . Demostreu que si C té una paraula codi de pes imparell, llavors les paraules codi de pes parell formen un altre codi de longitud n i dimensió $k - 1$.

V.12. Sigui C un codi lineal sobre $\mathbb{F}_q$ de longitud n i dimensió k , amb matriu generadora G . Demostreu que si G no té cap columna tot zeros, llavors la suma de tots els pesos de totes les paraules codi és

$$n \cdot (q - 1) \cdot q^{k-1}.$$

V.13. Sigui $\mathbb{F}_{q^2}$ un cos finit amb q^2 elements. El *producte hermític* de dos vectors $\mathbf{x} = (x_1, \dots, x_n)$ i $\mathbf{y} = (y_1, \dots, y_n)$ de $\mathbb{F}_{q^2}^n$ es defineix com

$$\langle \mathbf{x}, \mathbf{y} \rangle_H = \sum_{i=1}^n x_i y_i^q.$$

Aquest producte és una *forma sesquilineal*, és a dir:

$$\langle a\mathbf{x}, \mathbf{y} \rangle_H = a\langle \mathbf{x}, \mathbf{y} \rangle_H, \quad \langle \mathbf{x}, a\mathbf{y} \rangle_H = a^q \langle \mathbf{x}, \mathbf{y} \rangle_H.$$

Verifiqueu aquestes propietats.

(a) Sigui $C \subseteq \mathbb{F}_{q^2}^n$ un codi lineal. El codi *dual hermític* de C es defineix com

$$C^{\perp_H} = \{ \mathbf{y} \in \mathbb{F}_{q^2}^n : \langle \mathbf{x}, \mathbf{y} \rangle_H = 0 \text{ per a tot } \mathbf{x} \in C \}.$$

Demostreu que $C^{\perp_H}$ és un codi lineal i que $\dim C + \dim C^{\perp_H} = n$.

(b) Sigui $q = 2$ i $\mathbb{F}_4 = \{0, 1, \alpha, \alpha^2\}$ amb $\alpha^2 = \alpha + 1$. Calculeu $\langle (1, \alpha), (1, \alpha) \rangle_H$ i determineu tots els vectors ortogonals a $(1, \alpha)$ sota aquest producte.

V.14. L'*interleaving* (o entrelaçat) és una tècnica que consisteix a reordenar els símbols de diverses paraules de codi per reduir l'impacte d'errors agrupats. Donades t paraules del codi $\mathbf{c}^{(1)}, \dots, \mathbf{c}^{(t)} \in \mathbb{F}_q^n$ a enviar, la tècnica d'interleaving de bloc consisteix en escriure les paraules per files en una matriu

$$M = \begin{pmatrix} c_1^{(1)} & c_2^{(1)} & \dots & c_n^{(1)} \\ c_1^{(2)} & c_2^{(2)} & \dots & c_n^{(2)} \\ \vdots & \vdots & \ddots & \vdots \\ c_1^{(t)} & c_2^{(t)} & \dots & c_n^{(t)} \end{pmatrix},$$

i enviar la informació en blocs d'informació determinat per les columnes. O sigui, enviaríem les paraules $(c_1^1, c_1^2, \dots, c_1^t)$, després $(c_2^1, c_2^2, \dots, c_2^t)$, i així successivament.

(a) Suposem que hem codificat tres missatges amb un codi de distància mínima 3, obtenint tres paraules binàries de longitud 7:

$$\mathbf{c}^{(1)} = (1, 1, 1, 0, 0, 0, 0), \quad \mathbf{c}^{(2)} = (1, 0, 0, 1, 1, 0, 0), \quad \mathbf{c}^{(3)} = (0, 1, 0, 1, 0, 1, 0).$$

Mostreu com queden les paraules transmeses després d'aplicar interleaving de bloc.

(b) Ara compararem la capacitat per corregir errors i esborralls amb les dues estratègies d'enviament de missatges: enviant una paraula després de l'altra o aplicar l'interleaving de bloc. Pels següents casos, discutiu en quin cas es pot recuperar el missatge.

- Hi ha hagut un problema de transmissió i el receptor ha deixat de rebre 2 bits consecutius.
- Hi ha hagut un error de transmissió i el receptor ha rebut la informació amb 3 errors consecutius.
- Hi ha hagut un problema de transmissió i el receptor ha deixat de rebre 6 bits consecutius.
- Hi ha hagut un problema de transmissió i el receptor ha deixat de rebre bits consecutius.

Justifiqueu per què l'interleaving és una pràctica útil quan és probable que els errors es produeixin en ràfegues. Discutiu si aporta algun avantatge quan els errors són uniformement distribuïts.

6 Codis cíclics

VI.1. Considerem el conjunt C de paraules binàries de longitud n i pes parell.

- Demostreu que C és un codi lineal.
- Quina és la distància mínima de C ? Per què?

- (c) Quants errors pot corregir C ? I quants esborralls?
 - (d) Si es rep la paraula $000 \dots 001?10$, podríeu dir justificadament quin dígit correspon a l'esborrall?
 - (e) Demostreu que C és un codi cíclic.
 - (f) Doneu-ne el polinomi generador i una matriu generadora.
 - (g) Doneu-ne el polinomi de control i una matriu de control.
 - (h) Quin és el codi dual?
- VI.2.** (a) Descomponeu $x^7 - 1$ en factors irreductibles sobre el cos $\mathbb{F}_2$ i determineu tots els codis cíclics binaris de longitud 7.
- (b) Quants codis cíclics ternaris hi ha de longitud 8?
- (c) Suposem que $x^n - 1$ és el producte de t polinomis irreductibles diferents sobre $\mathbb{F}_q$. Quants codis cíclics de longitud n hi ha sobre $\mathbb{F}_q$?
- VI.3.** (a) Demostreu que $(x + y)^p = x^p + y^p$ a $\mathbb{F}_{p^n}$.
- (b) Quants codis cíclics 5-aris de longitud 10 hi ha? Descriviu detalladament de quina forma són els seus polinomis generadors.
- (c) Quants codis cíclics 5-aris de longitud 10 i dimensió 6 hi ha? Justifiqueu-ho.
- VI.4.** (a) Demostreu que $\frac{x^n - 1}{x - 1} = x^{n-1} + x^{n-2} + \dots + 1$.
- (b) Quins són els codis cíclics binaris de dimensió 1? I els de codimensió 1?
- VI.5.** Considerem un codi cíclic C de longitud n , dimensió k i distància mínima d , i amb polinomi generador $g(x)$.
- (a) Suposem que existeixen m posicions seguides d'una paraula no nul·la de C fora de les qual tots els valors són 0. Demostreu que necessàriament $m \geq n - k + 1$.
 - (b) Demostreu que una paraula no nul·la de C tindrà, com a màxim, $k - 1$ posicions nul·les seguides.
 - (c) Suposem que existeixen $n - k + 1$ posicions seguides d'una paraula no nul·la fora de les quals tots els valors són 0. Demostreu que en aquest cas els valors en aquestes posicions són els coeficients d'un polinomi que és un múltiple escalar de $g(x)$.
 - (d) Doneu una demostració alternativa de la fita de Singleton per codis cíclics.
 - (e) Demostreu que, en una matriu generadora sistemàtica en les primeres posicions, l'última fila conté els coeficients del polinomi $g(x)/g_0$, on g_0 és el coeficient constant de $g(x)$.
 - (f) En una matriu generadora sistemàtica en les últimes posicions, la primera fila conté els coeficients del polinomi $g(x)$. Demostreu-ho de tres maneres diferents: pel mètode dels pivots, pel sistema de codificació sistemàtica a través de la divisió de polinomis i pels primers apartats.
 - (g) Demostreu que els únics codis cíclics binaris separables a màxima distància són el codi de repetició i el de paritat.
- VI.6.** Descriviu tots els codis ternaris cíclics de longitud 18.
- VI.7.** Sigui $n > 2$ un enter positiu.
- (a) Doneu dos codis lineals binaris que siguin MDS. Un de distància mínima 2, i un altre de distància mínima n .
 - (b) Comproveu que aquests codis són únics, i que un és el dual de l'altre.
 - (c) Comproveu que aquests codis són cíclics, i doneu el polinomi generador de cada un.
- VI.8.** (a) És la intersecció de dos codis cíclics (de la mateixa longitud i definits sobre el mateix alfabet) un codi cíclic? I la unió?
- (b) Donats dos codis cíclics de longitud n amb polinomis generadors $g_1(x)$ i $g_2(x)$, descriviu el màxim codi cíclic contingut pels dos.

- (c) Donats dos codis cíclics de longitud n amb polinomis generadors $g_1(x)$ i $g_2(x)$, descriu el mínim codi cíclic que els conté tots dos.
- (d) Concreteu els dos apartats anteriors pel cas de codis ternaris cíclics de longitud 18.
- VI.9.** Sabem que el polinomi $x - 1$ divideix $x^{q-1} - 1$ a $\mathbb{F}_q$ per tot q . Per tant, ha de ser el polinomi generador d'un codi cíclic primitiu de $\mathbb{F}_q$.
- (a) Doneu-ne una matriu generadora en forma de cascada i una de control.
- (b) Quin és el seu codi dual?
- VI.10.** Un codi lineal C s'anomena *auto-ortogonal* si $C \subseteq C^\perp$, i *auto-dual* si $C = C^\perp$. Doneu un exemple d'un codi binari auto-ortogonal que no sigui autodual.
- VI.11.** El *codi de Golay binari* $\mathcal{G}_{23}$ és un codi lineal binari de longitud 23, dimensió 12 i distància mínima 7. És un codi *perfecte*, ja que les esferes de radi 3 al voltant dels vectors del codi particionen $\mathbb{F}_2^{23}$. Aquest codi va ser presentat per Marcel Golay el 1949 i ha tingut molta repercussió en el món de les telecomunicacions. És cíclic i el seu polinomi generador, que és
- $$g(x) = x^{11} + x^{10} + x^6 + x^5 + x^4 + x^2 + 1.$$
- (a) Comproveu que aquest polinomi divideix $x^{23} + 1$. Comproveu també que el polinomi $g^*(x)$ també divideix $x^{23} + 1$.
- (b) Doneu una matriu generadora i una matriu de control d'aquest codi.
- VI.12.** El *codi de Golay binari estès* és el codi binari que s'obté extenent el codi $\mathcal{G}_{23}$, i es denomina $\mathcal{G}_{24}$.
- (a) Trobeu els paràmetres d'aquest codi.
- (b) Escriviu una matriu generadora de $\mathcal{G}_{24}$ extenent la de $\mathcal{G}_{23}$ amb una columna adicional.
- (c) Comproveu que $\mathcal{G}_{24} = \mathcal{G}_{24}^\perp$.
- VI.13.** Sigui q una potència de primer i sigui n un enter tal que $\text{mcd}(n, q) = 1$. Sigui α una arrel primitiva d'ordre n en una extensió $\mathbb{F}_{q^m}$ de $\mathbb{F}_q$. Per enters $b \geq 1$ i $\delta \geq 1$, el *codi BCH cíclic* de longitud n , $\text{BCH}(n, q, b, \delta)$, és el codi cíclic amb polinomi generador

$$g(x) = \text{lcm}(m_{\alpha^b}(x), m_{\alpha^{b+1}}(x), \dots, m_{\alpha^{b+\delta-2}}(x)),$$

on $m_\beta(x) \in \mathbb{F}_q[x]$ denota el *polinomi mínim* de l'element $\beta \in \mathbb{F}_{q^m}$ sobre $\mathbb{F}_q$. El paràmetre δ s'anomena distància de disseny, i és una fita inferior de la distància mínima del codi.

- (a) Expliqueu per què $g(x)$ divideix $x^n - 1$.
- (b) Sigui $q = 2$ i $n = 15$. El cos $\mathbb{F}_{2^4}$ conté un element α d'ordre 15. Trobeu el polinomi generador del codi BCH binari amb distància de disseny $\delta = 3$.

7 Codis algebraics

- VII.1.** Sigui $\alpha_1, \dots, \alpha_n$ elements diferents d'un cos finit $\mathbb{F}_q$. Considereu la següent matriu de control.

$$H = \begin{pmatrix} 1 & \alpha_1 & \alpha_1^2 & \dots & \alpha_1^{n-1} \\ 1 & \alpha_2 & \alpha_2^2 & \dots & \alpha_2^{n-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \alpha_{n-k} & \alpha_{n-k}^2 & \dots & \alpha_{n-k}^{n-1} \end{pmatrix}$$

- (a) Quina és la distància mínima del codi determinat per una matriu H d'aquest tipus?
- (b) Sigui α un element primitiu de $\mathbb{F}_q$. Quins valors de n i $\alpha_1, \dots, \alpha_{n-k}$ prendries per tal d'obtenir la matriu de control d'un codi Reed Solomon primitiu?

VII.2. Sigui H una matriu de control com la de l'exercici anterior, on $\alpha_1, \dots, \alpha_n$ són elements diferents d'un cos finit $\mathbb{F}_q$ amb $n \leq q-1$. Sigui C el codi associat a la matriu de control H .

(a) Sigui $(c_0, \dots, c_{n-1})$ una paraula del codi determinat per C . Considereu ara el polinomi

$$c(x) = c_0 + c_1x + c_2x^2 + \dots + c_{n-1}x^{n-1}$$

Quant val $c(\alpha_i)$? Quant val $c(\alpha_i)$ per $1 \leq i \leq n-k$?

(b) Trobeu un polinomi mònic que divideix tots els polinomis associats a paraules del codi.

(c) Sigui $g(x)$ el polinomi definit a l'apartat anterior. Justifiqueu que tota paraula del codi està associada a un polinomi $p(x)g(x)$, on $p(x)$ és un polinomi de grau inferior a k .

VII.3. Sigui $n < q-1$ i $k \leq n$. Considereu els elements $\alpha_1, \dots, \alpha_n \in \mathbb{F}_q$, tots ells diferents, i el següent conjunt:

$$C = \{(p(\alpha_1), p(\alpha_2), \dots, p(\alpha_n)) : p \in \mathbb{F}_q[x]^{<k}\}.$$

(a) C és un codi lineal. Per què?

(b) Quin és el mínim pes de les paraules no nul·les d'aquest codi?

(Ajuda: Quantes arrels pot tenir un polinomi de grau $< k$?).

(c) Justifiqueu per què és un codi MDS.

(d) Doneu una matriu generadora d'aquest codi.

Els codis considerats als exercicis anteriors també se'ls anomena codis de Reed-Solomon, en algunes referències. Nosaltres, a teoria i als problemes, ens restringim al cas de codis RS primitius.

VII.4. Sigui $F = \mathbb{F}_q = \{\alpha_1, \alpha_2, \dots, \alpha_q\}$ i sigui $F^{<k}$ el conjunt de polinomis amb coeficients a F i grau menor que k . Considerem el conjunt

$$RS^{ext} = \{(p(\alpha_1), p(\alpha_2), \dots, p(\alpha_q), p_{k-1}) : p = p_0 + p_1x + \dots + p_{k-1}x^{k-1} \in \mathbb{F}_q^{<k}\}.$$

(a) Demostreu que RS^{ext} és un codi de longitud $n = q+1$, dimensió k i distància mínima $n-k+1$.
INDICACIÓ: p té grau menor que $k-1$ si i només si $p_{k-1} = 0$.

(b) Construïu un codi sobre $\mathbb{F}_3$ de longitud 4, dimensió 2 i distància mínima igual a 3. Comproveu que totes les paraules tenen pes 3.

VII.5. Suposem que q és potència de primer i $n < q$. Suposem que els elements $\alpha_1, \dots, \alpha_n \in \mathbb{F}_q$ són tots diferents i suposem que $v_1, \dots, v_n \in \mathbb{F}_q$ són no nuls (i no necessàriament diferents entre ells). El codi de Reed-Solomon generalitzat de dimensió k respecte $\alpha_1, \dots, \alpha_n, v_1, \dots, v_n$ es defineix de la manera següent:

$$GRS_{\alpha_1, \dots, \alpha_n, v_1, \dots, v_n}(k) = \{(v_1p(\alpha_1), v_2p(\alpha_2), \dots, v_np(\alpha_n)) : p \in \mathbb{F}_q^{<k}\}.$$

(a) Comproveu que $GRS_{\alpha_1, \dots, \alpha_n, v_1, \dots, v_n}(k)$ és un codi de longitud n , dimensió k i distància mínima igual a $n-k+1$.

(b) Comproveu que existeixen $v'_1, \dots, v'_n$ tals que

$$GRS_{\alpha_1, \dots, \alpha_n, v_1, \dots, v_n}^\perp(k) = GRS_{\alpha_1, \dots, \alpha_n, v'_1, \dots, v'_n}(n-k).$$

VII.6. Sigui C un codi de Reed-Solomon de dimensió k .

(a) Comproveu que $C^\perp$ és un codi cíclic.

(b) Qui és el polinomi generador de $C^\perp$?

(c) Quina és la distància de disseny de $C^\perp$? Per què?

(d) Comproveu que $C^\perp$ és un codi MDS.

VII.7. Sigui $\mathbb{F}_{q^2}$ un cos finit amb q^2 elements. El producte hermitic de dos vectors $\mathbf{x} = (x_1, \dots, x_n)$ i $\mathbf{y} = (y_1, \dots, y_n)$ de $\mathbb{F}_{q^2}^n$ es defineix com

$$\langle \mathbf{x}, \mathbf{y} \rangle_H = \sum_{i=1}^n x_i y_i^q.$$

- (a) Verifiqueu que aquest producte satisfà aquestes propietats:

$$\langle a\mathbf{x}, \mathbf{y} \rangle_H = a\langle \mathbf{x}, \mathbf{y} \rangle_H, \quad \langle \mathbf{x}, a\mathbf{y} \rangle_H = a^q \langle \mathbf{x}, \mathbf{y} \rangle_H.$$

- (b) Per a un codi lineal $C \subseteq \mathbb{F}_{q^2}^n$, definim el codi *dual hermític* com

$$C^{\perp_H} = \{ \mathbf{y} \in \mathbb{F}_{q^2}^n : \langle \mathbf{x}, \mathbf{y} \rangle_H = 0 \text{ per a tot } \mathbf{x} \in C \}.$$

Demostreu que $C^{\perp_H}$ és un codi lineal i que $\dim C + \dim C^{\perp_H} = n$.

- (c) Sigui $q = 2$ i $\mathbb{F}_4 = \{0, 1, \alpha, \alpha^2\}$ amb $\alpha^2 = \alpha + 1$. Calculeu $\langle (1, \alpha), (1, \alpha) \rangle_H$ i determineu tots els vectors ortogonals a $(1, \alpha)$ sota aquest producte.

VII.8. Sigui $\mathbb{F}_2^m$ l'espai de tots els vectors binaris de longitud m . Denotem per $\mathcal{P}_{r,m}$ el conjunt de tots els polinomis en m variables $x_1, \dots, x_m$ sobre $\mathbb{F}_2$ de grau total com a màxim r . El *codi de Reed-Muller* $\text{RM}(r, m)$ és el conjunt de totes les avaluacions d'aquests polinomis en tots els punts de $\mathbb{F}_2^m$:

$$\text{RM}(r, m) = \{ (f(v))_{v \in \mathbb{F}_2^m} : f \in \mathcal{P}_{r,m} \}.$$

Cada codi té longitud $n = 2^m$ i és un subespai de $\mathbb{F}_2^n$.

- (a) Mostreu que $\text{RM}(0, m)$ és el codi de repetició i que $\text{RM}(m, m) = \mathbb{F}_2^{2^m}$.
 (b) Demostreu que $\dim \text{RM}(r, m) = \sum_{i=0}^r \binom{m}{i}$.
 (c) Determineu els paràmetres (longitud, dimensió i distància mínima) de $\text{RM}(1, 3)$.
 (d) Mostreu que $\text{RM}(r, m)^\perp = \text{RM}(m - r - 1, m)$.

VII.9. L'esquema de Shamir és un esquema criptogràfic en què es generen fragments d'un secret. Pertany a la família dels *esquemes de compartició de secrets*. Aquest esquema es va presentar el 1979 i és un dels més coneguts i emprats. En aquests esquemes hi ha un participant que té el secret, que anomenem repartidor, i n participants que reben un fragment del secret. Està definit sobre cossos finits que tinguin més elements que el nombre de participants, $|\mathbb{F}| > n$, i depèn d'un paràmetre $t < n$

- (a) Input: $s \in \mathbb{F}$
 (b) Per compartir el secret s , el repartidor pren $t - 1$ elements $a_1, \dots, a_t \in \mathbb{F}$ uniformement a l'atzar.
 (c) El repartidor defineix el polinomi

$$p(x) = s + a_1 x + \dots + a_t x^t$$

- (d) A cada participant, el repartidor li envia una evaluació polinomi. O sigui, el repartidor tria $x_1, \dots, x_n \in \mathbb{F}$ diferents i diferents de zero, i envia $p(x_i)$ al participant i .

Ara analitzarem aquest esquema fent servir eines de codis lineals. Considerem el codi

$$C = \{ (s, s_1, \dots, s_n) : \text{on } s_1, \dots, s_n \text{ són possibles fragments de } s \}.$$

Observeu que a l'esquema de Shamir $p(0) = s$. Per tant, un cop fixats $x_1, \dots, x_n$, el codi definit abans és equivalent a

$$C = \{ (p(0), p(x_1), \dots, p(x_n)) : \text{on } p \text{ és un polinomi de grau } t \}.$$

- (a) El conjunt C és un codi lineal? Quin?
 (b) Descriu l'esquema de Shamir matricialment: trobeu una matriu M per la qual els fragments es poden obtenir com $(s, a_1, \dots, a_n)M$.
 (c) Per què els conjunts de tamany $t + 1$ poden recuperar el secret? Què en podem dir dels de tamany t ?

- VII.10.** Sigui $\mathbb{F}_{2^m}$ un cos finit i $L = (\alpha_1, \dots, \alpha_n)$ una llista d'elements distints de $\mathbb{F}_{2^m}$. Sigui $g(x) \in \mathbb{F}_{2^m}[x]$ un polinomi tal que $g(\alpha_i) \neq 0$ per a tot i . El codi de Goppa binari definit per L i $g(x)$ és:

$$\Gamma(L, g) = \left\{ \mathbf{c} = (c_1, \dots, c_n) \in \mathbb{F}_2^n : \sum_{i=1}^n \frac{c_i}{x - \alpha_i} \equiv 0 \pmod{g(x)} \right\}.$$

Aquests codis es fan servir en l'esquema de xifratge de clau pública de McEliece. És un esquema que compleix la funció de l'esquema de RSA, però la seva seguretat rau en problemes de la teoria de codis.

- (a) Expliqueu per què aquest conjunt és un subespai de $\mathbb{F}_2^n$.
- (b) Doneu una matriu de control d'aquest codi.
- (c) Mostreu que si $\text{grau}(g) = t$, aleshores la distància mínima del codi satisfà $d \geq 2t + 1$.
- VII.11.** L'esquema de xifrat McEliece és un esquema de clau pública, i compleix la mateixa funció que l'esquema RSA, vist anteriorment. Va ser proposat per Robert McEliece el 1978, i la construcció es basa en codis de Goppa. Es pot considerar que va ser el punt de partida de la criptografia basada en codis. Durant molts anys no s'ha tingut en compte a nivell pràctic perquè les claus públiques són molt grans, comparades amb les de RSA. Però recentment s'ha reconsiderat el seu ús pràctic perquè RSA és vulnerable a atacs quàntics. El 2025 el NIST ha estandaritzat l'esquema HQC. És un esquema basat en codis i la seva seguretat es basa en els mateixos problemes que l'esquema de McEliece.
- La idea central de la seguretat de l'esquema de McEliece, i de la majoria d'esquemes de clau pública basats en codis, és la següent. Sigui A una matriu, m un vector, e un vector de pes petit, i

$$c = mA + e$$

Un problema clàssic de la teoria de codis és el següent: Es pot recuperar m a partir de c i A eficientment? En general sabem que si A és la matriu generadora d'un codi *bones* capacitats correctores, aleshores és eficient. Per exemple, els codis Reed-Solomon i els codis de Goppa. Tanmateix, si A és una matriu aleatòria, no hi ha cap mètode eficient, en general.

Suposem que un adversari intercepta c , i sap que e té pes t . Assumim que també coneix B . Suposeu que intentem trobar m fent servir correcció d'errors a partir de la síndrome. O sigui, calculem una matriu de control corresponent a A , calculem la síndrome de c , i busquem el vector e' que té la mateixa síndrome que c . Feu una estimació del nombre de càlculs necessaris per trobar e .

- VII.12.** A continuació presentem una versió simplificada de l'esquema de McEliece. Suposem que Alice vol rebre missatges de manera segura. Aleshores generarà una clau pública, i una de privada (com a RSA)
- (a) Alice tria
- Una matriu aleatòria S que és invertible.
 - La matriu generadora d'un codi de Goppa A .
- (b) Alice publica $B = SA$, una matriu que sembla aleatòria. Tanmateix, manté A i S com a claus privades.
- (c) Si Bob vol enviar un missatge m a Alice, envia

$$c = mB + e$$

Per algú que escolti la conversa, en principi serà difícil obtenir m a partir de c i B .

- (d) Ara bé, com que

$$c = mB + e = (mS)A + e,$$

Alice pot calcular $m' = mS$ fent servir les propietats de correcció d'errors dels codis de Goppa, i llavors calcular $m = m' S^{-1}$. Això es pot fer perquè S és invertible.

Discutiu l'eficiència dels algorismes de xifrat i desxifrat.

Aquest llibre s'ha elaborat com a material docent per a l'assignatura Computació Algebraica del Grau en Enginyeria Matemàtica i Física de la Universitat Rovira i Virgili. El seu objectiu és proporcionar a l'estudiant una base sòlida dels conceptes algebraics fonamentals necessaris per a l'estudi posterior d'altres estructures algebraiques i per a l'estudi de les matemàtiques aplicades a la computació i a les comunicacions digitals.