1 Exercicis d'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 222222222, 333333333, 444444444, etc.

I.3. Comproveu que si $a \mid b$ i $b \mid c$, aleshores $a \mid c$.

I.4. Comproveu que si $a \mid b$ i existeix d tal que $d \mid a$ i $d \mid b$, aleshores $\frac{a}{d} \mid \frac{b}{d}$.

I.5. Demostreu que si $a \mid b$ i $a \mid c$, aleshores

- $a \mid -b$
- $a \mid b + c$
- $a \mid b - c$

I.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.

(Més endavant veurem l'aplicació d'aquest resultat al càlcul del mcd.)

I.7. Demostreu que si $d > 1$, aleshores d no és divisor de $qd + 1$ per cap enter q.

I.8. Intenteu demostrar per inducció els criteris de divisibilitat del 2, el 5 i el 10. Intenteu demostrar el criteri del 4.

I.9. Demostreu que si $a = bq + r$ amb $0 \leq r < |b|$, aleshores $\mathrm{mcd}(a, b) = \mathrm{mcd}(b, r)$.

I.10.

1. Demostreu que si M és múltiple de a i múltiple de b, aleshores M també és múltiple de $\mathrm{mcm}(a, b)$.

2. Demostreu que, per a qualsevol parella d'enters a, b,

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

I.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
- 2671 i 156

I.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.

I.13. Sabem que donats dos enters a, b *qualssevol*, si d és el $\mathrm{mcd}(a, b)$, aleshores existeixen dos enters més, λ i μ tals que $\lambda a + \mu b = d$. Demostreu amb un contraexemple que no sempre és cert que si existeixen dos enters λ i μ tals que $\lambda a + \mu b = d$, aleshores $d = \mathrm{mcd}(a, b)$.

I.14.

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

I.15.

1. Utilitzeu la identitat de Bézout per demostrar que si $a \mid bc$ i $\mathrm{mcd}(a, b) = 1$, aleshores $a \mid c$.

2. Demostreu que si p és primer i $p \mid ab$ aleshores $p \mid a$ o bé $p \mid b$.

3. Demostreu que si p és primer i $p \mid a_1 \cdot a_2 \cdot \cdots \cdot a_t$, aleshores existeix algun i entre 1 i t tal que $p \mid a_i$.

I.16. Demostreu el Teorema Fonamental de l'Aritmètica.

2 Exercicis d'aritmètica modular

II.1. Demostreu que si $a \equiv b \mod m$ i d divideix m, aleshores $a \equiv b \mod d$.

II.2. Comproveu que a $\mathbb{Z}_2$ es compleix:

- $-a = a$ per tot a,

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

II.3. Comproveu que a $\mathbb{Z}_p$, amb p primer, es compleix que

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

per tot n.

II.4. Calculeu $\mathbb{Z}_m^*$ per $1 < m \leq 12$.

II.5. Calculeu

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

II.6. Comproveu que si la descomposició d'un enter n en producte de primers és $n = p_1^{n_1} \cdot \cdots \cdot p_k^{n_k}$, aleshores

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

II.7. Comproveu que el teorema de Fermat és un cas particular del teorema d'Euler.

II.8.

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.

II.9. Observeu propietats de l'exponenciació a $\mathbb{Z}_m$ a través de les taules

II.10. Comproveu si a $\mathbb{Z}_{18}$ les classes de 3 i 7 tenen ordre, fent servir la definició i fent servir la condició anterior.

II.11. Demostreu que si $a \in \mathbb{Z}_m^*$ i a^{-1} és l'invers de a a $\mathbb{Z}_m$, aleshores $\mathrm{ord}_m(a^{-1}) = \mathrm{ord}_m(a)$.

II.12. Calculeu l'ordre de tots els elements de $\mathbb{Z}_7$ i comproveu que tots els ordres divideixen $\phi(7)$.

II.13. Comproveu que $\mathbb{Z}_8$ no té elements primitius.

II.14.

1. Comproveu que $\mathbb{Z}_{18}$ té elements primitius. a]primitiusz18
2. Quants i quins són els elements primitius de $\mathbb{Z}_{18}$? b]primitiusz18

II.15.

(a) Calculeu l'invers de 16 a $\mathbb{Z}_{29}$ a]trobainversos

(b) Calculeu l'invers de 258 a $\mathbb{Z}_{2791}$. b]trobainversos

II.16.

1. Expresseu tots els elements no nuls de $\mathbb{Z}_{19}$ com a potències de 2. a]elementsprimitius
2. És possible expressar tots els elements no nuls de $\mathbb{Z}_{23}$ com a potències de 2? b,c]elementsprimitius
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. b,c]elementsprimitius

II.17. Sigui l'anell $\mathbb{Z}_{18}$

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

II.18. 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?

II.19.

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

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

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

II.20.

Calculeu el residu de dividir

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

II.21. Trobeu les classes a $\mathbb{Z}_{100}$ de

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

II.22.

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

3 Exercicis d'aritmètica polinomial i cossos finits

III.1.

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

III.2. Demostreu que el màxim comú divisor de dos polinomis és unívocament definit llevat del producte per constants no nul·les.

III.3. 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 $\mathbb{Z}_2[x]$?

III.4.

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.

III.5.

1. Per què podem afirmar que 2 és un element invertible de $\mathbb{Z}_p$?

2. En general, qui és l'element 2^{-1}, invers de 2 a $\mathbb{Z}_p$, en funció de p?

3. Considerem la taula dels quadrats de tots els elements de $\mathbb{Z}_p$. Per exemple, la taula dels quadrats de $\mathbb{Z}_5$ seria:

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

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

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

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

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

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

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

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

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

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

   Comproveu que 4 i 5 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.

III.6.

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

III.7.

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

III.8.

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 $\mathbb{Z}_2[x]$.

III.9.

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

III.10.

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.

III.11.

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

III.12. Comproveu que, efectivament, les dues condicions de la definició són equivalents. Vegeu el resultat anàleg de les congruències d'enters.

III.13.

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

III.14.

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

III.15.

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.

III.16.

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.

III.17.

Utilitzeu l'Exercici 3 per donar un polinomi que generi $\mathbb{F}_{27}$.

III.18. Demostreu el teorema anterior. Podeu emprar els mateixos arguments que en la demostració del teorema d'Euler.

III.19. 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 $\mathbb{Z}_m$.

III.20.

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 $f(x)$.

III.21.

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.

III.22.

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 $\alpha^2 \left(\frac{\alpha^{20} - \alpha^5 + \alpha}{\alpha^3 - \alpha} \right)$.

III.23.

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

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

Sabem que

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

1. Quins d'aquests polinomis són irreductibles?
2. Quins dels polinomis irreductibles són primitius?

3. Per quins polinomis, en fer quocient a $\mathbb{Z}_3[x]$, s'obté un cos? De quants elements?

4. Per quins dels polinomis anteriors que, en fer quocient, ens donen un cos, podem expressar qualsevol element del cos com a potència de la classe de x en el quocient?

III.24.

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

III.25. Considerem el cos finit $\mathbb{F}_8 = \mathbb{Z}_2[x]/x^3+x+1$. Anomenem α a la classe de x.

1. Doneu la taula d'equivalències de les notacions exponencial i vectorial.

2. Doneu els oposats i els inversos dels elements de $\mathbb{F}_8$.

3. Doneu la taula de les sumes i la taula de les restes de $\mathbb{F}_8$.

4. Doneu la taula de les multiplicacions i la taula de les divisions de $\mathbb{F}_8$.

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

III.26. Considerem el cos finit $\mathbb{F}_9 = \mathbb{Z}_3[x]/x^2+2x+2$. Anomenem α a la classe de x.

1. Doneu la taula d'equivalències de les notacions exponencial i vectorial.

2. Doneu els oposats i els inversos dels elements de $\mathbb{F}_9$.

3. Doneu la taula de les sumes i la taula de les restes de $\mathbb{F}_9$.

4. Doneu la taula de les multiplicacions i la taula de les divisions de $\mathbb{F}_9$.

5. Calculeu $\frac{x^8-1}{x^4+\alpha^6x^3+x^2+\alpha^3x+\alpha^2}$.

III.27.

(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.

4 Exercicis d'existència i unicitat de cossos finits

IV.1. 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 $\oplus$.

IV.2. 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 $a \in E \setminus \{0_E\}$.

IV.3. Demostreu que si E és una extensió de F, aleshores E és un espai vectorial sobre F.

IV.4. Què passa en el lema anterior si canviem algun + per −? Indicació: Podeu separar els casos de característica parell i de característica senar.

IV.5. Demostreu que en un cos finit de q elements hi ha exactament $\phi(q-1)$ elements primitius.

IV.6. Comproveu les següents propietats:

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

IV.7. Demostreu que els factors irreductibles de la descomposició de $x^{p^m} - x$ dins de $\mathbb{Z}_p[x]$ són tots diferents.

IV.8. Demostreu que si $f(x) \in \mathbb{Z}_p[x]$ és irreductible a $\mathbb{Z}_p[x]$, aleshores $f(x)$ ha de dividir $x^{p^{\mathrm{grau}(f)}} - x$.

IV.9. Sigui F un cos finit de p^m elements. Si $\gamma \in F$ definim $C_\gamma = \{\gamma, \gamma^p, \gamma^{p^2}, \ldots, \gamma^{p^{s-1}}\}$ 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 $C_\gamma \cap C_{\gamma'} = \varnothing$.
- Demostreu que existeix un subconjunt $\Gamma(F) = \{\gamma_1, \ldots, \gamma_r\} \subseteq F$ tal que F és la unió disjunta de $C_{\gamma_1}, \ldots, C_{\gamma_r}$.
- Demostreu que
$$x^{p^m} - x = \prod_{\gamma \in \Gamma(F)} m_\gamma(x).$$

IV.10. Demostreu que en un cos finit F de p^m elements,

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

IV.11. 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.

IV.12. 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 $\{a, e, i, o\}$.

5 Exercicis de codis lineals

V.1.

Dins de $\mathbb{F}_2^3$ considerem el conjunt de paraules

$$C = \{(000), (111), (101), (010)\}.$$

Demostreu que C és un codi lineal.

V.2.

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

V.3. Quina seria la dimensió del codi
$C = \{(000), (111), (101), (010)\} \subseteq \mathbb{F}_2^3$?

V.4. Quines serien la taxa de transmissió i la codimensió del codi $C = \{(000), (111), (101), (010)\} \subseteq \mathbb{F}_2^3$?

V.5. Doneu una matriu generadora del codi
$C = \{(000), (111), (101), (010)\} \subseteq \mathbb{F}_2^3$.

V.6. Comproveu que les paraules del codi
$C = \{(000), (111), (101), (010)\} \subseteq \mathbb{F}_2^3$ són totes les codificacions possibles amb la matriu

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

V.7.

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

- $(1, 0, 2)$
- $(2, 2, 1)$

V.8.

Considerem el codi ternari de l'Exercici 5 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.

V.9. 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.

V.10.

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.

V.11.

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
$$011111010011001000000000.$$

V.12.

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.

V.13.

Utilitzem el codi dels Exercicis 5 i 5.

Useu la síndrome per descodificar el vector rebut 212121.

V.14.

Utilitzem el codi dels Exercicis 5 i 5.

Useu la síndrome per corregir els vectors rebuts

1. 120102, a]correcsindromegeneral
2. 222222. b]correcsindromegeneral

V.15. 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.

V.16.

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?

6 Exercicis de codis cíclics

VI.1.

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.

VI.2. 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.

VI.3.

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 $n - k$.

VI.4.

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. $G_3 = \begin{pmatrix} 1 & 0 & 0 & 6 & 0 \\ 0 & 1 & 0 & 0 & 6 \\ 0 & 0 & 1 & 2 & 4 \end{pmatrix}$

VI.5.

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

VI.6.

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

VI.7.

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.

VI.8.

Sobre $\mathbb{F}_2$ considerem la matriu

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

1. Demostreu que el codi generat per G és cíclic.
2. Trobeu els polinomis generador i de control.

VI.9. 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.

VI.10.

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.

7 Exercicis de codis algebraics

VII.1.

A $\mathbb{F}_7$,

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

VII.2.

A $\mathbb{F}_9 = \mathbb{Z}_3[x]/x^2 + 2x + 2$, anomenem α a la classe de x.

1. Calculeu la matriu de Vandermonde de rang 4 de $\alpha, \alpha^3, \alpha^5, \alpha^7$.
2. Calculeu el seu determinant per menors.
3. Calculeu el seu determinant fent servir el lema i comproveu que coincideixen.

VII.3.

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

- Per menors.
- Pel resultat del lema.

VII.4.

1. Comproveu que $\omega = 2$ 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 $2, 2^2, \ldots, 2^{n-k}$.

VII.5.

1. Quins ordres poden tenir els elements de $\mathbb{Z}_{13}$?

2. Comproveu que $\omega = 7$ és un element primitiu de $\mathbb{Z}_{13}$.

3. Doneu una taula d'equivalències de les potències de ω.

4. Volem construir un codi C de Reed-Solomon primitiu sobre $\mathbb{Z}_{13}$ capaç de corregir dos errors, basat en l'element primitiu $\omega = 7$. 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 $\omega = 7$. 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 $\omega = 7$. Doneu les 3 primeres files d' H.

VII.6.

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 $G \cdot H^T$.

VII.7.

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.

VII.8.

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.

VII.9.

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?

VII.10.

Considerem el codi RS de l'Exercici 7.

1. Considerem la paraula $u = (3, 12, 0, 1, 1, 5, 3, 10, 1, 9, 1, 11)$. Si avaluem el polinomi $u(x) = 11x^{11} + x^{10} + 9x^9 + x^8 + 10x^7 + 3x^6 + 5x^5 + x^4 + x^3 + 12x + 3$ en les primeres potències de ω ens dona els valors següents: $u(\omega) = 2,\ u(\omega^2) = 9,\ u(\omega^3) = 8,\ u(\omega^4) = 10,\ u(\omega^5) = 1,\ u(\omega^6) = 0\ldots$

   (a) Quants errors té la paraula u respecte de C?

   (b) Quin és el polinomi localitzador d'errors de u?

   (c) Quines són les posicions dels errors de u?

   (d) Quins són els valors dels errors de u?

   (e) Quina és la paraula corregida?

2. Considerem la paraula $v = (11, 11, 4, 0, 12, 1, 2, 2, 8, 5, 1, 11)$. Si avaluem el polinomi $v(x) = 11x^{11} + x^{10} + 5x^9 + 8x^8 + 2x^7 + 2x^6 + x^5 + 12x^4 + 4x^2 + 11x + 11$ en les primeres potències de a ens dona els següents valors: $v(\omega) = 9,\ v(\omega^2) = 8,\ v(\omega^3) = 5,\ v(\omega^4) = 12,\ v(\omega^5) = 4,\ v(\omega^6) = 8\ldots$

   (a) Quants errors té la paraula v respecte de C?

   (b) Quin és el polinomi localitzador d'errors de v?

   (c) Quines són les posicions dels errors de v?

   (d) Quins són els valors dels errors de v?

   (e) Quina és la paraula corregida?

VII.11.

1. Considerem el codi RS de l'exercici 7.

   (a) Codifiqueu de manera sistemàtica utilitzant el polinomi generador el primer bloc d'informació de la cadena de bits
   $11111000111110001111111111111000101010101010101010101000111111000\ldots$
   Doneu el resultat també com a cadena de bits.

   (b) Calculeu alguna síndrome de la paraula codificada.

2. Considerem el codi RS de l'exercici 7.

(a) Rebem la cadena de bits 00110000000000010100. A quina cadena de símbols correspon?

(b) Calculeu totes les síndromes de la paraula rebuda.

(c) Quants errors té de símbol la paraula rebuda?

(d) Quin és el polinomi localitzador d'errors?

(e) Trobeu les posicions dels errors.

(f) Calculeu el valor dels errors.

(g) Doneu la cadena de bits corregida.

(h) Quants errors de bit tenia la paraula enviada?