Problemes: Aritmètica IV. Existència i unicitat dels cossos finits.

IV.1. Demostreu que si en un cos finit es dona que $\underbrace{1+\cdots+1}_{m}=0$, aleshores m ha de ser un múltiple de la característica.

IV.2. Demostreu que si K, F són dos cossos tals que existeix $f: K \to F$ un morfisme d'anells, aleshores K, F tenen la mateixa característica.

IV.3. (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.4. Demostreu que si un cos finit F té p^m elements, aleshores la característica de F és p.

IV.5. Demostreu que en un cos finit de p^m elements, tot element té una única arrel p-èssima.

IV.6. Feu un gràfic del reticle de subcossos de $\mathbb{F}_{p^{16}}$, $\mathbb{F}_{p^{20}}$ i $\mathbb{F}_{p^{60}}$.

IV.7. (a) Un cos de 16 elements, quina característica té? pot tenir un subcòs amb 8 elements? i un subcòs amb 4 elements?

(b) Proveu que un cos amb 125 elements té un únic subcòs diferent d'ell mateix.

IV.8. Si K és un cos de característica 0, aleshores $\mathbb{Q} \hookrightarrow K$, i per tant és clar que K ha de ser infinit. Podeu donar un exemple d'un cos amb característica p primer i que sigui infinit?

IV.9. Suposem que $\mathbb{F}_q$ és el cos de cardinal q.

(a) Si β és un element primitiu de $\mathbb{F}_q$, quin és l'ordre de β^i?

(b) Si $d \mid q-1$, quants elements d'ordre d hi ha a $\mathbb{F}_q$? Feu una comprovaciuó amb `sage`.

IV.10. Demostreu que en un cos K amb p^n elements hi ha exactament $\phi(p^n-1)$ elements primitius, on ϕ és la funció d'Euler.

IV.11. Trobeu tots els elements primitius del cos $F = \mathbb{Z}_3[x]/(x^2+1)$ i expresseu-los com a potència de $\beta = \alpha + 1$.

IV.12. Demostreu que al cos $\mathbb{Z}_2[x]/(x^4+x^3+x^2+x+1)$ l'element $\alpha = [x]$ no és primitiu i que, en canvi, $\alpha + 1$ sí que ho és.

IV.13. Construïu una successió $\alpha_1, \alpha_2, \dots, \alpha_k$ d'elements de $\mathbb{F}_q^*$ tal que

$$\mathrm{ord}(\alpha_1) < \mathrm{ord}(\alpha_2) < \cdots < \mathrm{ord}(\alpha_k) = q-1$$

IV.14. Considerem el cos $K = \mathbb{Z}_2[x]/(x^4+x+1)$ i l'element $\alpha = [x]$.

(a) Construïu una taula d'equivalències.

(b) Useu el fet que α és un element primitiu de K i la taula d'equivalències per respondre les qüestions següents:

i. Trobeu les arrels quadrades de $\alpha + 1$ i de α^3 a K.

ii. Trobeu les arrels cúbiques de $\alpha^3+\alpha^2$ i de α^2+1 a K.
iii. Trobeu les arrels cinquenes de $\alpha^2+\alpha+1$ a K.

IV.15. Sigui K un cos finit amb q elements i m un natural.

(a) Demostreu que tot element $a \in K$ té com a màxim m arrels m-èssimes a K.

(b) Demostreu que si m és coprimer amb $q-1$, aleshores els elements de K tenen una única arrel m-èssima a K.

(c) Demostreu que si m no és coprimer amb $q-1$, aleshores hi ha elements de K que no tenen arrel m-èssima.

(d) Demostreu que si m no és coprimer amb $q-1$ i un element de K té arrel m-èssima, aleshores té exactament $\mathrm{mcd}(m, q-1)$ arrels m-èssimes a K.

(Indicació: expresseu els elements de K com a potències d'un element primitiu.)

IV.16. Demostreu que si p és primer, aleshores $x^2 \equiv -1 \mod p$ té solució si i només si $p=2$ o si $p \equiv 1 \mod 4$.

IV.17. Demostreu que, si $p \equiv 1 \mod 4$, llavors $(\frac{p-1}{2})!^2 \equiv -1 \mod p$.

IV.18. (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.19. Per quins primers p és $\mathbb{Z}_p[x]/(x^2+1)$ un cos? I $\mathbb{Z}_p[x]/(x^4+1)$?

IV.20. Sigui $K = \mathbb{Z}_2[x]/(x^3+x+1)$ i $\alpha = [x]$. Calculeu el polinomi mínim de $\alpha+1$, és a dir, trobeu un polinomi irreductible mònic $f(x) \in \mathbb{Z}_2[x]$ tal que $f(\alpha+1)=0$.

IV.21. (a) Construïu la taula d'equivalències del cos $\mathbb{Z}_2[x]/(x^4+x+1)$.

(b) Useu la taula anterior per calcular el polinomi irreductible sobre $\mathbb{Z}_2[x]$ de cada element del cos.

IV.22. Considerem el cos $F = \mathbb{Z}_2[x]/(x^4+x+1)$ i diem $\alpha = [x]$. Trobeu el polinomi irreductible sobre $\mathbb{Z}_2$ dels elements $\alpha+1$, α^3+1, $\alpha^2+\alpha$ de F.

IV.23. Considerem el cos $K = \mathbb{Z}_2[x]/(x^4+x+1)$, com en un exercici anterior.

(a) Comproveu que tots els elements de K anul·len el polinomi $x^{16}-x$.

(b) A partir de la taula d'equivalències, trobeu totes les arrels del polinomi x^4-x a K i proveu que formen un subcòs de K amb 4 elements.

(c) Doneu un isomorfisme explícit del subcòs de quatre elements de l'apartat anterior al cos $\mathbb{Z}_2[x](x^2+x+1)$

IV.24. (a) Trobeu un element de $\mathbb{Z}_2[x](x^4+x+1)$ que sigui arrel del polinomi x^4+x^3+1.

(b) Doneu un isomorfisme explícit de $\mathbb{Z}_2[x]/(x^4+x^3+1)$ a $\mathbb{Z}_2[x]/(x^4+x+1)$.

IV.25. Descomponeu sobre $\mathbb{Z}_2$ el polinomi $x^{16}-x$.

IV.26. Demostreu que per a tot primer p el polinomi $(x^{p^2}-x)(x^{p^3}-x)$ és un divisor de $(x^{p^6}-x)(x^p-x)$ a $\mathbb{Z}_p[x]$. Demostreu que el quocient

$$\frac{(x^{p^6}-x)(x^p-x)}{(x^{p^2}-x)(x^{p^3}-x)}$$

és un polinomi sobre $\mathbb{Z}_p$ que descompon en producte de polinomis irreductibles de grau 6.

IV.27. 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.28. Demostreu que si $n > 1$ i p és un primer senar, aleshores el polinomi $x^{p^n} + x$ no té cap factor irreductible de grau n.