Problemes: Aritmètica III. Aritmètica polinomial i cossos finits.

III.1. És $x-3$ un divisor de x^4+x^3+x+4 a $\mathbb{Z}_2[x]$?, a $\mathbb{Z}_3[x]$?, a $\mathbb{Z}_5[x]$?, a $\mathbb{Z}_7[x]$?

III.2. (a) Demostreu que $x^n-1 \mid x^m-1$ si i només si $n \mid m$.

(b) Demostreu que $\mathrm{mcd}(x^m-1, x^n-1) = x^d-1$, on $d = \mathrm{mcd}(m,n)$.

III.3. Proveu el Teorema de Wilson (si p és un primer senar, llavors $(p-1)! \equiv -1 \mod p$) de la manera següent:

- Proveu que a $\mathbb{Z}_p[x]$ el polinomi $f(x) = x^{p-1}-1$ factoritza com $f(x) = (x-1)(x-2)\cdots(x-(p-1))$ (useu el teorema de Fermat i el teorema de l'arrel a $\mathbb{Z}_p[x]$.)
- Avalueu $f(0)$.

III.4. Demostreu que x^5+x^2+1 és irreductible a $\mathbb{Z}_2[x]$.

III.5. (a) Demostreu que $p(x) = x^3+2x^2+x+3$ és irreductible a $\mathbb{Z}_5$.

(b) Trobeu l'invers de la classe de $3x^2-2x+1$ a $\mathbb{Z}_5/(p(x))$.

III.6. Digueu si els polinomis x^5 i x^2-1 tenen invers a $\mathbb{Z}_3[x]/(x^2+2x+1)$ i calculeu-lo en cas afirmatiu.

III.7. Trobeu els divisors de zero de $\mathbb{Z}_5[x]/(x^3+2x^2+x+2)$.

III.8. Resoleu, si és possible:

- $(x^3+x+1)f(x) \equiv 1 \mod x^4+x+1$ a $\mathbb{Z}_2[x]$
- $(2x+1)f(x) \equiv 1 \mod 2x^2+2x+2$ a $\mathbb{Z}_3[x]$
- $(x^2+1)f(x) \equiv x^2+x+1 \mod x^4+1$ a $\mathbb{Z}_2[x]$
- $(2x+1)f(x) \equiv 1 \mod 2x^2+2x+1$ a $\mathbb{Z}_3[x]$

III.9. La descomposició dels nombres enters en sumes mínimes de quadrats d'altres enters ha estat un problema clàssic. Es coneix que qualsevol enter descomposa 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.

- Escriviu una rutina que donat un enter en doni la descomposició en una suma de quadrats amb el mínim nombre de termes possibles.
- Demostreu que, en un cos finit, cada element és suma de de dos quadrats.
- Escriviu una rutina que, donat un element d'un cos finit en doni la descomposició com a suma de dos quadrats.