MATEMÀTICA DISCRETA - FIB 7-10-2008

Primer examen parcial Grup 20

A cada un dels apartats següents cal justificar clarament les respostes.

1. Trobeu tots els polinomis irreductibles de grau 2 i de grau 3 a $\mathbb{F}_2[x]$.
2. Proveu que el polinomi $f(x) = x^6 + x + 1$ és irreductible a $\mathbb{F}_2[x]$.
3. Expliqueu per què el conjunt $\mathbb{F}_{64} = \mathbb{F}_2[x]/f(x)$ de les classes de congrüència mòdul $f(x)$ és un cos, i per què té exactament 64 elements.
4. Proveu que el polinomi $f(x)$ és primitiu.
5. Sigui α la classe de x mòdul $f(x)$. Quin és l'ordre de α a $\mathbb{F}_{64}^*$? I els ordres de $\alpha^3, \alpha^4, \alpha^6, \alpha^9$? [Recordeu que l'ordre d'un element a de $\mathbb{F}_q^*$ és el mínim $k > 0$ tal que $a^k = 1$.]
6. Quants elements primitius (és a dir, d'ordre 63) hi ha a $\mathbb{F}_{64}^*$?
7. Expresseu α^{25} com un polinomi en α de grau més petit que 6. Calculeu el seu invers a $\mathbb{F}_{64}$.
8. Trobeu una arrel quadrada de α i proveu que no en té més.