MATEMÀTICA DISCRETA - FIB 7-10-2008

Primer examen parcial Grup 10

Justifiqueu les respostes

1.

1. [0,5 punts] Doneu la definició de polinomi irreductible.
2. [0,5 punts] Digueu per a quins valors de $n \in \mathbb{Z}$ hi ha cossos finits de n elements.
3. [0,5 punts] Digueu quants elements primitius té el cos $\mathbb{F}_{81}$.
4. [1,5 punts] Calculeu l'invers de $\alpha^3 + \alpha + 1$ al cos $\mathbb{F}_2[x]/(x^4 + x^3 + x^2 + x + 1)$, sent $\alpha = \overline{x}$.

2. Sigui $f(x) = x^2 + x + 2$. Considereu el quocient $\mathbb{F}_3[x]/(f(x))$.

1. [1 punt] Comproveu que es tracta d'un cos. Digueu quin cardinal té.
2. [1 punt] Feu la llista dels elements del cos.
3. [1 punt] Esbrineu si el polinomi $f(x)$ és primitiu i en cas afirmatiu doneu la taula de logaritmes.
4. [1 punt] Calculeu l'ordre de cadascun dels elements invertibles del cos.
5. [2 punts] Comproveu que $T = 1 + \alpha$, on $\alpha = \overline{x}$ al cos, és una solució de l'equació
$$(2 + \alpha)T^3 + 2\alpha T^2 + (2 + 2\alpha)T + 1 = 0$$
i trobeu les altres solucions de l'equació.

3. [1 punt] Sigui p un nombre primer. Demostreu que el polinomi $x^p - x$ té p arrels i que aquestes són els elements de $\mathbb{F}_p$.

Solucions

1.

1. Doneu la definició de polinomi irreductible.

   Un polinomi de grau ≥ 1 és irreductible si no es pot obtenir com a producte de dos polinomis de graus estrictament més petits que el d'ell.

2. Digueu per a quins valors de $n \in \mathbb{Z}$ hi ha cossos finits de n elements.

   Per a $n = p^r$, on p és un nombre primer i $r \in \mathbb{Z}$, $r \geq 1$.

3. Digueu quants elements primitius té el cos $\mathbb{F}_{81}$.

   El nombre d'elements primitius és $\phi(81-1) = \phi(80) = \phi(2^4 5) = 2^3 4 = 32$.

4. Calculeu l'invers de $\alpha^3 + \alpha + 1$ al cos $\mathbb{F}_2[x]/(x^4 + x^3 + x^2 + x + 1)$, sent $\alpha = \overline{x}$.

   Sigui $f(x) = x^4 + x^3 + x^2 + x + 1$. L'element $\alpha^3 + \alpha + 1$ és la classe del polinomi $a(x) = x^3 + x + 1$. Mitjançant la identitat de Bezout trobarem aquest l'invers.

$t(x)$	1	0	1	x^2+1
$s(x)$	0	1	$x+1$	x^3+x^2+x
$q(x)$		$x+1$	x^2+1	
$r(x)$	$x^4+x^3+x^2+x+1$	x^3+x+1	x	1

   Aleshores, $a(x)s(x) + f(x)t(x) = 1$. Per tant, $\overline{a(x)(x^3+x^2+x)} = \overline{1}$ a $\mathbb{F}_2[x]/(x^4+x^3+x^2+x+1)$ i l'invers és $\overline{x^3+x^2+x} = \alpha^3 + \alpha^2 + \alpha$.

2. Sigui $f(x) = x^2 + x + 2$. Considereu el quocient $\mathbb{F}_3[x]/(f(x))$.

1. Comproveu que es tracta d'un cos. Digueu quin cardinal té.

   Per tal que el quocient sigui un cos cal que el polinomi $f(x)$ sigui irreductible. Atès que és un polinomi de grau 2 n'hi ha prou en comprovar que no té arrels: $f(0) = f(2) = 2$ i $f(1) = 1$. Per tant, $f(x)$ és irreductible i el quocient $\mathbb{F}_3[x]/(f(x))$ és un cos $\mathbb{F}_q$ amb $q = 3^2 = 9$ elements.

2. Feu la llista dels elements del cos.

   Sigui $\alpha = \overline{x}$, aleshores $\mathbb{F}_9 = \{0, 1, 2, \alpha, \alpha+1, \alpha+2, 2\alpha, 2\alpha+1, 2\alpha+2\}$, són les classes dels residus possibles que s'obtenen en dividir qualsevol polinomi entre $f(x)$.

3. Esbrineu si el polinomi $f(x)$ és primitiu i en cas afirmatiu doneu la taula de logaritmes.

   Un polinomi és primitiu si és irreductible (el nostre ho és) i la classe $\overline{x}$ és un element primitiu del cos quocient, en aquest cas de $\mathbb{F}_3[x]/(f(x))$. Cal, per tant, comprovar que l'ordre de $\alpha = \overline{x}$ és $q - 1 = 8$. N'hi ha prou en comprovar que l'ordre de α no és ni 1, ni 2, ni 4. Atès que $\alpha \neq 1$, no té ordre 1.

$$\alpha^2 = 2\alpha + 1 \neq 1,$$
$$\alpha^4 = (2\alpha+1)^2 = \alpha^2 + \alpha + 1 = 2\alpha + 1 + \alpha + 1 = 2 \neq 1.$$

   Per tant, l'odre de α és 4 i el polinomi és primitiu.

   Per escriure la taula de logaritmes ens cal primer calcular les potències de α.

$$\begin{array}{ll}
\alpha^1 = \alpha & \alpha^5 = 2\alpha \\
\alpha^2 = 2\alpha + 1 & \alpha^6 = 2\alpha^2 = 2(2\alpha+1) = \alpha + 2 \\
\alpha^3 = 2\alpha^2 + \alpha = 2\alpha + 2 & \alpha^7 = \alpha^2 + 2\alpha = \alpha + 1 \\
\alpha^4 = 2\alpha^2 + 2\alpha = 2(2\alpha+1) + 2\alpha = 2 & \alpha^8 = 1
\end{array}$$

Aleshores

β	α	$2\alpha+1$	$2\alpha+2$	2	2α	$\alpha+2$	$\alpha+1$	1
$\log_\alpha \beta$	1	2	3	4	5	6	7	8

4. Calculeu l'ordre de cadascun dels elements invertibles del cos.

Recordem que $\operatorname{ord}(\beta^k) = \operatorname{ord}(\beta)/\operatorname{mcd}(\operatorname{ord}(\beta), k)$. Aplicant aquesta fórmula per a $\beta = \alpha$ i usant la taula de logaritmes, és té:

β	α	$2\alpha+1$	$2\alpha+2$	2	2α	$\alpha+2$	$\alpha+1$	1
$\operatorname{ord}(\beta)$	8	4	8	2	8	4	8	1

5. Comproveu que $T = 1 + \alpha$, on $\alpha = \overline{x}$ al cos, és una solució de l'equació

$$(2+\alpha)T^3 + 2\alpha T^2 + (2+2\alpha)T + 1 = 0$$

i trobeu les altres solucions de l'equació.

Per veure que $\beta = 1 + \alpha$ satisfà l'equació podem substituir directament β a l'equació i comprovar que dóna zero. Una altra manera és dividir el polinomi $g(T) = (2+\alpha)T^3 + 2\alpha T^2 + (2+2\alpha)T + 1$ entre $T - \beta$, comprovar que el residu dóna zero i obtenir, a més, el quocient que és el polinomi del que hem de cercar les altres arrels de $g(T)$. Aplicant Ruffini:

$$\begin{array}{c|cccc} & \alpha+2 & 2\alpha & 2\alpha+2 & 1 \\ & & 2\alpha & 1 & 2 \\ \hline \alpha+1 & \alpha+2 & \alpha & 2\alpha & \boxed{0} \end{array}$$

es té $g(T) = (T-\beta)((2+\alpha)T^2 + \alpha T + 2\alpha)$.

Cal ara trobar les solucions de $(2+\alpha)T^2 + \alpha T + 2\alpha = 0$. Estudiem si el discriminant és o no un quadrat al cos $\mathbb{F}_9$:

$$d = \alpha^2 - 4(2+\alpha)2\alpha = 2 = \alpha^4 = (\alpha^2)^2.$$

El discriminant és un quadrat diferent de zero, per tant hi ha dues solucions:

$$T = \frac{-\alpha \pm \sqrt{d}}{2(2+\alpha)} = (-\alpha \pm \alpha^2)2\alpha^2 = \begin{cases} 2\alpha + 1 = \alpha^2 \\ 2\alpha = \alpha^5 \end{cases}$$

usant que $2^{-1} = 2$ i $(2+\alpha)^{-1} = (\alpha^6)^{-1} = \alpha^{8-6}$.

Aleshores, les solucions de l'equació de l'enunciat són: $\alpha + 1$, $2\alpha + 1$ i 2α.

3. Sigui p un nombre primer. Demostreu que el polinomi $x^p - x$ té p arrels i que aquestes són els elements de $\mathbb{F}_p$.

Com aplicació del teorema del residu, tot polinomi de grau ≥ 1 té en un cos, com a molt, tantes arrels com el grau. Per tant, el polinomi $g(x) = x^p - x$ té com a molt p arrels a $\mathbb{F}_p$. El teorema de Fermat assegura que $a^{p-1} = 1$, per a tot $a \in \mathbb{F}_p^*$, per tant, $a^p - a = 0$ per a tot $a \in \mathbb{F}_p$. Aleshores, tot element de $\mathbb{F}_p$ és una arrel de $g(x)$ i, com el cos té p elements, el polinomi $g(x)$ té exactament p arrels totes a $\mathbb{F}_p$.