MA-31A Elementos de Álgebra **19 de Noviembre, 2005**

Control 3

Prof. Cátedra: M. Kiwi *Prof. Auxiliar: H. Castro, J. Soto*

Tiempo 4.5 hrs. Ma31a Elementos de Álgebra

Problema 1:

Un polinomio $L(x) = \sum_{i=0}^{n} \alpha_i x^{q^i}$ a coeficientes en un extensión $\mathbb{F}_{q^m}$ de $\mathbb{F}_q$ se llama q–polinomio o polinomio linearizado sobre $\mathbb{F}_{q^m}$

(i).- (0.6 pts) Sea $\mathbb{F}$ una extensión de $\mathbb{F}_{q^m}$. Pruebe que $L(\beta+\gamma) = L(\beta) + L(\gamma)$ y $L(c\beta) = cL(\beta)$ para todo $\beta, \gamma \in \mathbb{F}$ y $c \in \mathbb{F}_q$. Concluya que $L : \mathbb{F} \to \mathbb{F}$ es una transformación $\mathbb{F}_q$-lineal y que el conjunto de las raíces de L es un sub–espacio vectorial de $\mathbb{F}$ sobre $\mathbb{F}_q$.

(ii).- (1.0 pts) Sea L no nulo y suponga que la extensión finita $\mathbb{F}$ de $\mathbb{F}_{q^m}$ contiene todas las raíces de $L(x)$. Pruebe que todas las raíces de $L(x)$ tienen multiplicidad igual a una misma potencia de q.

Indicación: Considere "la derivada" de $L(x)$.

Suponga que desea determinar las raíces de L en una extensión finita $\mathbb{F}$ de $\mathbb{F}_{q^m}$. Sea $\{\beta_1, \ldots, \beta_s\}$ una base de $\mathbb{F}$ sobre $\mathbb{F}_q$.

(iii).- (0.6 pts) Pruebe que existe $C = (c_{j,k})_{j,k}$ matriz a coeficientes en $\mathbb{F}_q$ tal que

$$L(\beta_j) = \sum_{k=1}^{s} c_{j,k}\beta_k\,, \qquad 1 \le j \le s\,,$$

y que el problema de encontrar raíces en $\mathbb{F}$ del polinomio afín $A(x) = L(x) - \alpha$ con $\alpha \in \mathbb{F}_{q^m}$ se reduce al problema de encontrar soluciones de un sistema lineal (homógeneo si $\alpha = 0$)

Sea γ raíz del polinomio irreducible $x^4 + x^3 + x^2 - x - 1 \in \mathbb{F}_3[x]$. Luego, $\mathbb{F}_{81} = \mathbb{F}(\gamma)$. Deseamos encontrar las raíces en $\mathbb{F}_{81}$ de $L(x) = x^9 - x^3 - \gamma^{10}x$.

(iv).- (0.6 pts) Probar que $\Gamma = \{1, \gamma, \gamma^2, \gamma^3\}$ es base de $\mathbb{F}_{81}$ como espacio vectorial sobre $\mathbb{F}_3$.

(v).- (1.0 pts) Verificar que $x^2 + x - 1 \in \mathbb{F}_3[x]$ es irreducible y que $\gamma^{10} = -1 + \gamma + \gamma^2 - \gamma^3$. Probar que γ^{10} es raíz en $\mathbb{F}_{81}$ del polinomio $x^2 + x - 1$.

(vi).- (1.0 pts) Verifique que la matríz $[L]_{\Gamma,\Gamma}$ es

$$\begin{pmatrix} 1 & & -1 & 1 \\ -1 & -1 & & \\ -1 & -1 & & \\ 1 & -1 & 1 & -1 \end{pmatrix},$$

y exprese las 9 raíces en $\mathbb{F}_{81}$ de L como combinación lineal de Γ.

El hecho que encontrar raíces de polinomios linearizados sea simple (pues corresponde a encontrar soluciones de sistemas lineales) sugiere la siguiente estrategía para encontrar una raíz en $\mathbb{F}$ de $P \in \mathbb{F}_{q^m}[x]$, donde $\mathbb{F}$ es extensión finita de $\mathbb{F}_{q^m}$:

- Encontrar un polinomio afín $A(x)$ sobre $\mathbb{F}_{q^m}$ múltiplo de $P(x)$.
- Encontar todas las raíces de $A(x)$ en $\mathbb{F}$.
- Evaluar P en las raíces de A para localizar las raíces de P.

(vii).- (0.6 pts) Para $0 \leq i < n$, sea $R_i(x) \in \mathbb{F}_{q^m}[x]$ el resto de la división de x^{q^i} por $P(x)$, donde n denota el grado de P. Pruebe que existen escalares α_i's no todos nulos, tales que

$$\sum_{i=0}^{n-1} \alpha_i R_i(x)$$

es un polinomio constante e indique como determinar un conjunto de tales escalares.

(viii).- (0.6 pts) Describa un procedimiento basado en (i)-(vii) para encontrar una raíz en $\mathbb{F}$ de un polinomio $P \in \mathbb{F}_{q^m}[x]$, donde $\mathbb{F}$ es una extensión finita de $\mathbb{F}_{q^m}$.