COMBINATÓRIA E TEORIA DE CÓDIGOS
Ficha 3

10/3/2008

Exercícios 3.1 - 3.14 + 4.1 - 4.7 (R. Hill)

Problema 1. (Construção do Corpo $G\mathbb{F}\left(2^4\right)$)

a) Verifique que o polinómio $x^4 + x + 1$ é irredutível em $\mathbb{F}_2[x]$;

b) Construa então $G\mathbb{F}\left(2^4\right) = \mathbb{F}_2[x]/x^4+x+1$, idenficando os seus elementos e esboçando as respectivas tabelas de adição e multiplicação;

c) É capaz de identificar o elemento primitivo daquele corpo?

Problema 2. Seja $I(p,n)$ o número de polinómios mónicos irredutíveis de grau n em $\mathbb{F}_p[x]$.

a) Mostre que

$$I(p,2) = \binom{p}{2};$$

b) Mostre que

$$I(p,3) = \frac{p\left(p^2-1\right)}{3}.$$

***c)** Há uma fórmula geral para $I(p,n)$. Se quiser investigue e procure descobrir tal fórmula e como é obtida. Isto permite, entre outras coisas, mostrar que se tem sempre $I(p,n) > 0$ e como tal que se podem construir corpos finitos de qualquer ordem $q = p^n$ (p primo).

Problema 3. Considere o espaço vectorial $(G\mathbb{F}(q))^n$

a) Designando por $\begin{bmatrix} n \\ k \end{bmatrix}_q$ o número de subspaços de dimensão k de $(G\mathbb{F}(q))^n$:

(i) Mostre que

$$\begin{bmatrix} n \\ k \end{bmatrix}_q = \frac{(q^n-1)\left(q^{n-1}-1\right)\cdots\left(q^{n-k+1}-1\right)}{(q^k-1)(q^{k-1}-1)\cdots(q-1)};$$

(ii) Mostre que

$$\begin{bmatrix} n \\ k \end{bmatrix}_q = \begin{bmatrix} n-1 \\ k-1 \end{bmatrix}_q + q^k \begin{bmatrix} n-1 \\ k \end{bmatrix}_q;$$

(iii) Justifique que

$$\lim_{q\to 1} \begin{bmatrix} n \\ k \end{bmatrix}_q = \binom{n}{k};$$

b) (i) Calcule o número de matrizes quadradas não singulares $n \times n$ com entradas num corpo finito $G\mathbb{F}(q)$;

(ii) Qual será então a probabilidade $P(q,n)$ de uma matriz quadrada $n \times n$ sobre $G\mathbb{F}(q)$ ser não singular?

(*)(iii) Para q fixo, mostre que

$$\lim_{n\to\infty} P(q,n) = c(q)$$

existe e $0 < c(q) < 1$. (Para $q = 2$, $c(2) \simeq 0,2887$)