COMBINATÓRIA E TEORIA DE CÓDIGOS
Exercise List 3

5/3/2011

Exercises 3.1 - 3.14 + 4.1 - 4.6 (R. Hill)

Problem 1. (The field $\mathbb{F}_{2^4}$)

a) Show that the polynomial $x^4 + x + 1$ is irreducible in $\mathbb{F}_2[x]$.

b) Define $\mathbb{F}_{2^4} = \mathbb{F}_2[x]/\langle x^4+x+1\rangle$ by identifiying its elements and by sketching the addition and multiplication tables.

c) Find a primitive element in $\mathbb{F}_{2^4}$.

Problem 2. Let $I(p, n)$ be the number of irreducible monic polynomials of degree n in $\mathbb{F}_p[x]$.

a) Show that

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

b) Show that

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

***c)** There is a general formula for $I(p, n)$. If you are interested in that, try to find that formula and how to prove it. It allows us to show that $I(p, n) > 0$ for all primes p and for all positive integers n and, as a consequence, we can built finite fields of orders $q = p^n$.

Problem 3.

Consider the vector space $(\mathbb{GF}(q))^n$

a) Denote by $\begin{bmatrix} n \\ k \end{bmatrix}_q$ the number of k dimentional subspaces of $(\mathbb{GF})(q))^n$:

(i) Show that

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

(ii) Show that

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

(iii) Justify that

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

b) **(i)** Determine the number of nonsingular $n \times n$ square matrices with entries in a finite field $\mathbb{GF}(q)$;

(ii) What's the probability $P(q,n)$ of a $n \times n$ matrix over $\mathbb{GF}(q)$ being nonsingular?

(*)**(iii)** For q fixed, show that

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

exists and $0 < c(q) < 1$. (For $q = 2$, $c(2) \simeq 0,2887$.)