MATEMATICA DISCRETA II-2006
PRACTICO 9 (cuerpos finitos y Reed-Solomon)

I): Dar las tablas de suma y producto de $GF(8)$, tomando el polinomio $1+x+x^3$ para representarlo, y luego repetir, tomando $1+x^2+x^3$.

II): Dar todos los polinomios irreducibles de grado 2,3,4 y 5. (Ayuda: si $p(0) = 0$, entonces x divide a $p(x)$ y no es irreducible, por lo que todos deben tener termino independiente igual a 1. Por otro lado, si $p(1) = 0$, entonces $1+x$ divide a $p(x)$, por lo que para que sea irreducible debe ser $p(1) = 1$, i.e., debe tener un numero IMPAR de terminos no nulos. Los polinomios de grado 2 o 3 que NO sean irreducibles deben tener un factor de grado 1 es decir, o x o $1+x$, por lo tanto basta con las dos condiciones de arriba para encontrarlos. Para los de grado 4, ademas de esas condiciones, hay que ver que no sea producto de dos irreducibles de grado dos, los cuales ya hallaron, asi que eliminan facil y obtienen los irreducibles de grado 4. Para el de 5, ademas de las condiciones anteriores, deben eliminar los que sean productos de irreducibles de grado 2 y grao 3, lo cual tambien hacen a partir de los calculos ya realizados).

III): $1+x+x^4$ es irreducible, y puede ser usado para dar una representacion de $GF(16)$. Si entendemos que "2" esta representado como "0100", (es decir, por el polinomio x), entonces probar que "2" es un elemento primitivo en $(GF(16) - \{0\}, .)$, es decir, que sus potencias dan todos los elementos. (un polinomio irreducible con esta propiedad se dice primitivo)

Con esto se puede construir facilmente la tabla de multiplicar de $GF(16)$. Por ejemplo, probar que "3"."12"="7". Calcular "5"."4", "15"."10" y "6"."11".

IV): En el ejercicio anterior se ve que $1+x+x^4$ es primitivo.

a) Ir al ejericio 1), y decidir si alguno, o ambos de los polinomios usados alli para representar $GF(8)$ es primitivo.

b) Ir al ejercicio 2) y decidir cuales de los polinomios que aparecen alli son primitivos.

V): Sea C el codigo $RS(2^3, 5)$ con generador $g(x) = (1+x)(\alpha+x)(\alpha^2+x)(\alpha^3+x)$ usando $GF(2^3)$ construido con $1+\alpha+\alpha^3$. (conviene hacer el ejercicio 1) antes).

a) Dar n, k, δ y $|C|$.

b) Hallar una matriz generadora para C.

VI): Dar un polinomio generador para un codigo MDS de longitud 31 sobre $GF(32)$ que corrija 3 errores. (i.e., tendrá un (31,25,7)-code). (no hace falta desarrollar el polinomio)

VII): Dar una matriz generadora con la identidad a derecha para un codigo $(8, 4, 5)$ sobre $GF(16)$.