ALGEBRA EFECTIVA **Examen final** **10-06-2003**

Apellidos **Nombre**

Ejercicio 1: (3.75 puntos)(5 CUESTIONES INDEPENDIENTES)
a) Probar que $c \cdot m.c.d.(a,b) = \quad m.c.d.(ac,bc)$.
b) Sea n un entero que no es múltiplo de 2 ni de 5. Calcular los valores de n para que $10^n - 1$ sea múltiplo de n.
c) Probar que si m.c.d.$(a,b) = d$ y $\alpha a + \beta b = d$, entonces m.c.d.$(\alpha, \beta) = 1$.
d) Probar que si $n > 2$ es impar y el orden de 2 en $\mathbb{Z}/\mathbb{Z}n$ es $n-1$, entonces n es primo.
e) Probar que si $a|bc$ y m.c.d.$(a,b)|c$, entonces $a|c^2$.

Ejercicio 2: (1.5 puntos) Se considera el cuerpo $K = (\mathbb{Z}/\mathbb{Z}\cdot 3)[x]/(x^3 + 2\,x^2 + 1)$ de 27 elementos. Se recuerda que todos los elementos de K deberán escribirse como un polinomio en x de grado 2, a lo más. Se pide:
1) Calcular el orden de $x + 2$.
2) Calcular $1/(x+1)$.

Ejercicio 3: (2.75 puntos) Se considera el cuerpo $K = (\mathbb{Z}/\mathbb{Z}\cdot 2)[x]/(x^3 + x + 1)$ de 8 elementos. Los polinomios de $K[Z]$ se escribirán en forma de suma potencias **decrecientes** de Z con sus correspondientes coeficientes entre paréntesis. Se considera el código cíclico en $K[Z]/(Z^7 - 1)$ de polinomio generador

$$F = Z^4 + \left(x^2 + x + 1\right) Z^3 + Z^2 + \left(x^2 + x\right) Z + x^2 + x + 1$$

y sea

$$p_1 = Z^6 + \left(x^2 + x\right) Z^5 + \left(x^2 + x\right) Z^4 + xZ^3 + (x+1)\,Z^2 + x$$

una palabra recibida en un proceso de transmisión. Se sabe que el código es de Reed-Solomon, con respecto a una cierta raíz primitiva. Para ayudar a resolver el problema se incluye al final una parte de la tabla completa de síndromes y errores (que tiene 301 elementos). Se pide

1. Calcular la dimensión del código. ¿Cuántos errores corrige?
2. Calcular la palabra recibida p.
3. Decodificar p, es decir, hallar la palabra de información correspondiente, o sea el polinomio $q \in K[Z]$ tal que $p = q\,F$.
4. Explicar con menos de 20 palabras por qué este problema se podría haber resuelto sin necesidad de dar la parte de la tabla.

$$\left[\begin{array}{cc}
\mathit{Sindromes} & \mathit{Errores} \\
(x+1)\,Z^3 + x & (x+1)\,Z^3 + x \\
x^2 Z^3 + x & x^2 Z^3 + x \\
(x^2+1)\,Z^3 + x & (x^2+1)\,Z^3 + x \\
(x^2+x)\,Z^3 + x & (x^2+x)\,Z^3 + x \\
(x^2+x+1)\,Z^3 + x & (x^2+x+1)\,Z^3 + x \\
(x^2+x+1)\,Z^3 + Z^2 + (x^2+x)\,Z + 1 + x^2 & Z^4 + x \\
(x^2+1)\,Z^3 + xZ^2 + (x^2+x+1)\,Z + 1 + x^2 + x & xZ^4 + x \\
xZ^3 + (x+1)\,Z^2 + Z & (x+1)\,Z^4 + x \\
Z^3 + x^2 Z^2 + (x^2+1)\,Z + 1 + x & x^2 Z^4 + x \\
(x^2+x)\,Z^3 + (x^2+1)\,Z^2 + (x+1)\,Z + x^2 & (x^2+1)\,Z^4 + x
\end{array}\right]$$