Álgebra Efectiva (12/06/2002)

Ejercicio 1: (2 puntos) Sea $k = \mathbb{Z}/\mathbb{Z}\cdot 2$ y $f = Z^9+Z^6+Z^5+Z^4+Z+1 \in k[Z]$.

1).- Hallar el cociente y el resto de la división de $Z^{15}+1$ por f en $k[Z]$.

Sea $\mathcal{C} \subset k^{15}$ el código cíclico de polinomio generador f. Se tiene como dato que $\mathcal{C}$ corrige dos errores.También se tiene como dato los síndromes de algunos errores.

2).- Recibida la palabra $Z^{14}+Z^{12}+Z^9+Z^8+Z^5+Z^2$, hallar la transmitida.

El apartado 2) se calificará triple del 1)

Síndromes	Errores
$Z^6+Z^5+Z^4+Z$	Z^9+1
$Z^7+Z^6+Z^5+Z^2+Z+1$	$Z^{10}+1$
$Z^8+Z^7+Z^6+Z^3+Z^2+1$	$Z^{11}+1$
$Z^8+Z^7+Z^6+Z^5+Z^3+Z$	$Z^{12}+1$
$Z^8+Z^7+Z^5+Z^2$	$Z^{13}+1$
$Z^8+Z^5+Z^4+Z^3$	$Z^{14}+1$

Se da como solución una hoja de cálculo de Maple.

Polinomio dato:

```
> f:=Z^9+Z^6+Z^5+Z^4+Z+1;
```

$$f := Z^9+Z^6+Z^5+Z^4+Z+1$$

Lista formada por cociente y resto de dividir $Z^{15}+1$ entre f

```
> divpolcf(Z^15+1,f);
```

$$[Z^6+Z^3+Z^2+Z+1,\ 0]$$

Esto responde a la primera cuestión del examen. El cociente es el primer elemento de la lista y el resto el segundo, que es cero. Como f divide a $Z^{15}+1$, genera un código cíclico en dimensión 15.

Para responder a la segunda cuestión, escribimos como recordatorio la tabla completa de errores y síndromes. Como los síndromes de los errores se obtienen dividiendo éstos por f y tomando el resto, los nueve primeros son absolutamente obvios: ellos mismos porque el cociente es cero. En el texto del examen se han dado como dato inicial los errores no obvios. De todas formas, aquí los escribimos todos, para mayor claridad.

Comenzamos escribiendo la lista de errores de peso menor o igual que 2

```
> i:='i':le:=[1,seq(1+Z^i,i=1..14)];
```

$$le := [1,\ 1+Z,\ 1+Z^2,\ 1+Z^3,\ 1+Z^4,\ 1+Z^5,\ 1+Z^6,\ 1+Z^7,\ 1+Z^8,\ 1+Z^9,\ 1+Z^{10},\ 1+Z^{11},\ 1+Z^{12},\ 1+Z^{13},\ 1+Z^{14}]$$

Ahora escribimos la lista de sus síndromes:

```
> i:='i':ls:=[seq(divpolcf(le[i],f)[2],i=1..15)];
```

$$ls := [1,\ Z+1,\ Z^2+1,\ Z^3+1,\ Z^4+1,\ Z^5+1,\ Z^6+1,\ Z^7+1,\ Z^8+1,\ Z^6+Z^5+Z^4+Z,\ Z^7+Z^6+Z^5+Z^2+Z+1,\ Z^8+Z^7+Z^6+Z^3+Z^2+1,\ Z^8+Z^7+Z^6+Z^5+Z^3+Z,\ Z^8+Z^7+Z^5+Z^2,\ Z^8+Z^5+Z^4+Z^3]$$

Para que sea más visible, escribimos la lista de síndromes y errores en formato de matriz. Se insiste en que esta lista no hay que calcularla; se daba como dato. A la izquierda están los síndromes, y a la derecha los errores.

```
> M:=linalg[transpose](array([ls,le]));
```

$$M := \begin{bmatrix} 1 & 1 \\ Z+1 & Z+1 \\ Z^2+1 & Z^2+1 \\ Z^3+1 & Z^3+1 \\ Z^4+1 & Z^4+1 \\ Z^5+1 & Z^5+1 \\ Z^6+1 & Z^6+1 \\ Z^7+1 & Z^7+1 \\ Z^8+1 & Z^8+1 \\ Z^6+Z^5+Z^4+Z & Z^9+1 \\ Z^7+Z^6+Z^5+Z^2+Z+1 & Z^{10}+1 \\ Z^8+Z^7+Z^6+Z^3+Z^2+1 & Z^{11}+1 \\ Z^8+Z^7+Z^6+Z^5+Z^3+Z & Z^{12}+1 \\ Z^8+Z^7+Z^5+Z^2 & Z^{13}+1 \\ Z^8+Z^5+Z^4+Z^3 & Z^{14}+1 \end{bmatrix}$$

Ahora comienza la resolución de la segunda parte del problema. La palabra recibida es:

```
> pr:=Z^14+Z^12+Z^9+Z^8+Z^5+Z^2;
```

$$pr := Z^{14}+Z^{12}+Z^9+Z^8+Z^5+Z^2$$

Calculamos la lista de cociente y resto de la división de esta palabra por f. Su síndrome es el resto, segundo elemento de la lista:

```
> divpolcf(pr,f);
```

$$[Z^5+Z^3+Z^2+Z+1,\ Z^8+Z^7+Z^2+1]$$

Así pues, el síndrome es $Z^8+Z^7+Z^2+1$, que no está en la primera columna de la matriz. Por tanto, hemos de hallar el producto de Z por la palabra recibida y su síndrome.

> `pr1:=expand(Z*pr);`

$$pr1 := Z^{15} + Z^{13} + Z^{10} + Z^9 + Z^6 + Z^3$$

Como antes, hallamos la lista de cociente y resto de su división por f. El síndrome será el segundo elemento de la lista:

> `divpolcf(pr1,f);`

$$[Z^6 + Z^4 + Z^3 + Z^2 + Z + 1,\ Z^8 + Z^6 + Z^5 + Z^4 + Z^3 + 1]$$

El síndrome es $Z^8 + Z^6 + Z^5 + Z^4 + Z^3 + 1$, que tampoco está en la primera columna de la matriz. Así pues, procedemos a multiplicarla por Z^2 y hacer lo mismo:

> `pr2:=expand(Z^2*pr);`

$$pr2 := Z^{16} + Z^{14} + Z^{11} + Z^{10} + Z^7 + Z^4$$

> `divpolcf(pr2,f);`

$$[Z^7 + Z^5 + Z^4 + Z^3 + Z^2 + Z + 1,\ Z^7 + 1]$$

En este caso el síndrome, $Z^7 + 1$, sí está en la primera columna. Corresponde al error $Z^7 + 1$, como es lógico. Así pues, corregimos la palabra pr2:

> `pr2c:=pr2+(Z^7+1) mod 2;`

$$pr2c := Z^{16} + Z^{14} + Z^{11} + Z^{10} + Z^4 + 1$$

Para obtener la palabra original, hemos de multiplicar la corregida de pr2 por Z^{13} (porque hemos multiplicado por Z^2) y tomar el resto de dividir por $Z^{15} + 1$

> `prc:=expand(Z^13*pr2c);`

$$prc := Z^{29} + Z^{27} + Z^{24} + Z^{23} + Z^{17} + Z^{13}$$

La lista de cociente y resto de dividir por $Z^{15} + 1$ es:

> `divpolcf(prc,Z^15+1);`

$$[Z^{14} + Z^{12} + Z^9 + Z^8 + Z^2,\ Z^{14} + Z^{13} + Z^{12} + Z^9 + Z^8 + Z^2]$$

Por tanto, la palabra emitida es el resto, o sea $Z^{14} + Z^{13} + Z^{12} + Z^9 + Z^8 + Z^2$.

Ejercicio 2: (3 puntos)
A) Resolver la ecuación de recurrencia $f_{n+3} + f_{n+2} - f_{n+1} - f_n = (-1)^n, \quad n \geq 0$ con $f_0 = 0, f_1 = 0, f_2 = 1$.
B) Calcular la función generatriz de la ecuación de recurrencia anterior.

A) $x^3 + x^2 - x - 1 = (x-1)(x+1)^2$, luego

$$f_n^{(h)} = A + [B + Cn](-1)^n.$$

La solución particular de la ecuación no homogénea la buscamos de la forma $f_n^{(p)} = Dn^2(-1)^n$. Sustituyendo se tiene:

$$D(n+3)^2(-1)^{n+3} + D(n+2)^2(-1)^{n+2} - D(n+1)^2(-1)^{n+1} - Dn^2(-1)^n = (-1)^n$$

$$D(-1)^n[(-1)^3(n^2+6n+9)+(-1)^2(n^2+4n+4)-(-1)(n^2+2n+1)-n^2] = (-1)^n$$
$$-4D = 1, \quad D = -(1/4).$$

Por tanto $f_n^{(p)} = -(1/4)n^2(-1)^n$.

La solución general es

$$f_n = f_n^{(h)}+f_n^{(p)} = -(1/4)n^2(-1)^n+A+[B+Cn](-1)^n = A+[B+Cn-(1/4)n^2](-1)^n.$$

$$f_0 = 0 = A + B$$
$$f_1 = 0 = A - [B + C - (1/4)]$$
$$f_2 = 1 = A + [B + 2C - 1]$$

De donde $A = -B = 3/8, \quad C = 1$, $f_n = (3/8)+[-(3/8)+n-(1/4)n^2](-1)^n$.

B)

$$F(x) = \sum_{n\geq 0} f_n x^n =$$

$$= (3/8)\sum_{n\geq 0} x^n - (3/8)\sum_{n\geq 0}(-x)^n + \sum_{n\geq 0} n(-x)^n - (1/4)\sum_{n\geq 0} n^2(-x)^n =$$

$$= \frac{3}{8}\frac{1}{1-x} - \frac{3}{8}\frac{1}{1+x} + \frac{x}{(1+x)^2} + \frac{1}{4}\frac{x(1-x)}{(1+x)^3}$$

Ejercicio 3: (1 punto) Probar que si a y b son primos entre sí, entonces se verifica que m.c.d(ab,n)=m.c.d(a,n) · m.c.d(b,n), para todo n $\in \mathbb{Z}$.

Sean d=m.c.d.(ab,n), d_1=m.c.d.(a,n), d_2=m.c.d.(b,n). Es fácil ver que m.c.d.(d_1, d_2)=1. Pongamos

$$d = \alpha ab + \beta n$$
$$d_1 = \alpha_1 a + \beta_1 n$$
$$d_2 = \alpha_2 b + \beta_2 n.$$

$$d_1 \mid a \mid ab, \quad d_1 \mid n \quad \Rightarrow d_1 \mid d.$$

$$d_2 \mid b \mid ab, \quad d_2 \mid n \quad \Rightarrow d_2 \mid d.$$

Como m.c.d.(d_1, d_2)=1, se tiene que $d_1 d_2 \mid d$.

Recíprocamente: $d_1 d_2 = \alpha_1\alpha_2 ab + (\alpha_1\beta_2 a + \beta_1\alpha_2 b + \beta_1\beta_2 n)n$,

$$d \mid ab, \quad d \mid n \quad \Rightarrow \quad d \mid d_1 d_2.$$

Ejercicio 4: (1 punto) Sean $a, b, c \in \mathbb{Z}$, $1 \leq a \leq b \leq c$. Calcular todas las soluciones de

$$\begin{array}{rcll} a & \equiv & b & (mod \quad c) \\ b & \equiv & c & (mod \quad a) \\ c & \equiv & a & (mod \quad b) \end{array}$$

De la primera congruencia se tiene que $c \mid (b-a)$, luego $a = b$, pues $b - a < c$. Las dos congruencias restantes son iguales a

$$a \equiv c \pmod{a},$$

por tanto $a \mid (c-a)$, luego $a \mid c$. Solución: $a = b \mid c$.

Ejercicio 5: (1 punto)
A) Probar que $Q_{n+1}(0,1,\ldots,1) = F_n$.
B) Calcular $Q_{n+1}(\underbrace{0,\ldots,0}_{s},\underbrace{1,\ldots,1}_{r})$, $\quad r+s=n+1$.

A)$Q_{n+1}(0,1,\ldots,1) = 0.Q_n(1,\ldots,1) + Q_{n-1}(1,\ldots,1) = F_n$.
B)$Q_{r+s}(\underbrace{0,\ldots,0}_{s},\underbrace{1,\ldots,1}_{r}) = 0.Q_{r+s-1}(\underbrace{0,\ldots,0}_{s-1},\underbrace{1,\ldots,1}_{r}) + Q_{r+s-2}(\underbrace{0,\ldots,0}_{s-2},\underbrace{1,\ldots,1}_{r}) =$
$Q_{r+s-2}(\underbrace{0,\ldots,0}_{s-2},\underbrace{1,\ldots,1}_{r})$
$Q_{r+s-2}(\underbrace{0,\ldots,0}_{s-2},\underbrace{1,\ldots,1}_{r}) = 0.Q_{r+s-3}(\underbrace{0,\ldots,0}_{s-3},\underbrace{1,\ldots,1}_{r}) + Q_{r+s-4}(\underbrace{0,\ldots,0}_{s-4},\underbrace{1,\ldots,1}_{r}) =$
$Q_{r+s-4}(\underbrace{0,\ldots,0}_{s-4},\underbrace{1,\ldots,1}_{r})$.

Distinguimos dos casos: $s = 2k, s = 2k+1$. Supongamos $s = 2k$. Después de k pasos tenemos que

$$Q_{r+s}(\underbrace{0,\ldots,0}_{s},\underbrace{1,\ldots,1}_{r}) = Q_{r+s-2k}(\underbrace{1,\ldots,1}_{r}) = Q_r(\underbrace{1,\ldots,1}_{r}) = F_{r+1}.$$

Supongamos $s = 2k+1$. Después de k pasos tenemos que

$$Q_{r+s}(\underbrace{0,\ldots,0}_{s},\underbrace{1,\ldots,1}_{r}) = Q_{r+s-2k}(0,\underbrace{1,\ldots,1}_{r}) = Q_{r+1}(0,\underbrace{1,\ldots,1}_{r}) = F_r.$$