

Ejercicio 9

Ana Buendía Ruiz-Azuaga

March 30, 2022

1 Ejercicio 9

1.1 Apartado 1

Toma n tu número publicado para el ejercicio 2. Escribe n en base 2, usa esas cifras para definir un polinomio, $f(x)$, donde tu bit más significativo defina el grado del polinomio n , el siguiente bit va multiplicado por x^{n-1} y sucesivamente hasta que el bit menos significativo sea el término independiente. El polinomio que obtienes es universal en el sentido de que tiene coeficientes en cualquier anillo

Sea $f(x)$ el polinomio que obtienes con coeficientes en \mathbb{Z}

$n = 77770081$

Tenemos que n en base 2 es 100101000101010110101100001, luego

$$f(x) = x^{26} + x^{23} + x^{21} + x^{17} + x^{15} + x^{13} + x^{11} + x^{10} + x^8 + x^6 + x^5 + 1.$$

Toma $g(x) = f(x) \bmod 2$ y halla el menor cuerpo de característica 2 que contenga a todas las raíces de g . ¿Qué deduces sobre la irreducibilidad de $g(x)$ en $\mathbb{Z}_2[x]$?

Definimos $g(x)$ como $g(x) = f(x) \bmod 2$, luego

$$g(x) = x^{26} + x^{23} + x^{21} + x^{17} + x^{15} + x^{13} + x^{11} + x^{10} + x^8 + x^6 + x^5 + 1.$$

El menor cuerpo de característica 2 que contiene a todas las raíces de g es $F_{2^{46}} = F_{2^{2 \cdot 23}}$. Como tenemos que $46 > 26$ entonces $g(x)$ es reducible en $\mathbb{Z}_2[x]$. Además, sabemos que los factores en los que se descomponga g serán de grado un divisor de 46, esto es, 1, 2 o 23.

1.2 Apartado 2

Extrae la parte libre de cuadrados de $g(x)$ y le calculas su matriz de Berlekamp por columnas. Resuelve el s.l. $(B - Id)X = 0$.

Tenemos que el máximo común divisor de g y su derivada es $(g, g') = 1$, luego g es libre de cuadrados. Pasamos por tanto a calcular su matriz de Berlekamp por columnas.

para ello, comenzamos por calcular $x^{2i} \bmod g$ con $0 \leq i < 26$

```

[0] x^2i mod f = 1
[1] x^2i mod f = x^2
[2] x^2i mod f = x^4
[3] x^2i mod f = x^6
[4] x^2i mod f = x^8
[5] x^2i mod f = x^10
[6] x^2i mod f = x^12
[7] x^2i mod f = x^14
[8] x^2i mod f = x^16
[9] x^2i mod f = x^18
[10] x^2i mod f = x^20
[11] x^2i mod f = x^22
[12] x^2i mod f = x^24
[13] x^2i mod f = x^23 + x^21 + x^17 + x^15 + x^13 + x^11 + x^10 + x^8 + x^6 +
    x^5 + 1
[14] x^2i mod f = x^25 + x^23 + x^19 + x^17 + x^15 + x^13 + x^12 + x^10 + x^8 +
    x^7 + x^2
[15] x^2i mod f = x^25 + x^24 + x^22 + x^21 + x^19 + x^18 + x^17 + x^16 + x^15 +
    x^11 + x^10 + x^7 + x^6 + x^4 + x
[16] x^2i mod f = x^22 + x^20 + x^19 + x^16 + x^15 + x^14 + x^10 + x^7 + x^6 +
    x^5 + x^3 + x + 1
[17] x^2i mod f = x^24 + x^22 + x^21 + x^18 + x^17 + x^16 + x^12 + x^9 + x^8 +
    x^7 + x^5 + x^3 + x^2
[18] x^2i mod f = x^24 + x^21 + x^20 + x^19 + x^18 + x^17 + x^15 + x^14 + x^13
    + x^9 + x^8 + x^7 + x^6 + x^4 + 1
[19] x^2i mod f = x^22 + x^20 + x^19 + x^16 + x^13 + x^9 + x^5 + x^2 + 1
[20] x^2i mod f = x^24 + x^22 + x^21 + x^18 + x^15 + x^11 + x^7 + x^4 + x^2
[21] x^2i mod f = x^24 + x^21 + x^20 + x^15 + x^11 + x^10 + x^9 + x^8 + x^5 +
    x^4 + 1
[22] x^2i mod f = x^22 + x^21 + x^15 + x^12 + x^8 + x^7 + x^5 + x^2 + 1
[23] x^2i mod f = x^24 + x^23 + x^17 + x^14 + x^10 + x^9 + x^7 + x^4 + x^2
[24] x^2i mod f = x^25 + x^23 + x^21 + x^19 + x^17 + x^16 + x^15 + x^13 + x^12
    + x^10 + x^9 + x^8 + x^5 + x^4 + 1
[25] x^2i mod f = x^25 + x^24 + x^23 + x^22 + x^21 + x^19 + x^17 + x^16 + x^15
    + x^10 + x^9 + x^2 + x

```

Y por tanto, la matriz de Berlekamp B, cuyas filas vienen dadas por los coeficientes de los polinomios calculados resulta:

```

[1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0]
[0 0 1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0]
[0 0 0 0 1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0]
[0 0 0 0 0 0 1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0]
[0 0 0 0 0 0 0 0 1 0 0 0 0 0 0 0 0 0 0 0 0 0 0]
[0 0 0 0 0 0 0 0 0 0 1 0 0 0 0 0 0 0 0 0 0 0 0]
[0 0 0 0 0 0 0 0 0 0 0 0 1 0 0 0 0 0 0 0 0 0 0]
[0 0 0 0 0 0 0 0 0 0 0 0 0 0 1 0 0 0 0 0 0 0 0]
[0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 1 0 0 0 0 0 0]
[0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 1 0 0 0 0]
[0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 1 0 0]

```

```

[0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 1 0 0 0]
[0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 1 0]
[1 0 0 0 0 1 1 0 1 0 1 1 0 1 0 1 0 0 0 1 0 1 0 0]
[0 0 1 0 0 0 0 1 1 0 1 0 1 1 0 1 0 1 0 0 0 1 0 1]
[0 1 0 0 1 0 1 1 0 0 1 1 0 0 0 1 1 1 1 1 0 1 1 0 1]
[1 1 0 1 0 1 1 1 0 0 1 0 0 0 1 1 1 0 0 1 1 0 1 0 0]
[0 0 1 1 0 1 0 1 1 1 0 0 1 0 0 0 1 1 1 0 0 1 1 0 1]
[1 0 0 0 1 0 1 1 1 1 0 0 0 1 1 1 0 1 1 1 1 0 0 1 0]
[1 0 1 0 0 1 0 0 0 1 0 0 0 1 0 0 1 0 0 1 1 0 1 0 0]
[0 0 1 0 1 0 0 1 0 0 0 1 0 0 0 1 0 0 1 0 0 1 1 0 1]
[1 0 0 0 1 1 0 0 1 1 1 1 0 0 0 1 0 0 0 0 1 1 0 0 1]
[1 0 1 0 0 1 0 1 1 0 0 0 1 0 0 1 0 0 0 0 0 1 1 0 0]
[0 0 1 0 1 0 0 1 0 1 1 0 0 0 1 0 0 1 0 0 0 0 1 1 0]
[1 0 0 0 1 1 0 0 1 1 1 0 1 1 0 1 1 0 1 0 1 0 1 0 1]
[0 1 1 0 0 0 0 0 0 1 1 0 0 0 0 1 1 1 0 1 0 1 1 1 1]

```

Ahora que tenemos construida B, vamos a resolver $(B - Id)X = 0$.

El rango de $B - Id$ es 23, luego la dimensión de $V_1 = 26 - 23 = 3$. Por tanto, hay 3 soluciones, que son:

```

[1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0]
[0 1 0 1 1 1 1 0 0 0 1 0 1 0 1 0 1 0 1 1 0 0 0 1 1]
[0 0 1 0 0 1 0 1 0 0 0 0 1 1 0 0 1 1 0 0 1 0 0 0 1]

```

Luego obtenemos los polinomios:

$$f_1(x) = 1$$

$$f_2(x) = x + x^3 + x^4 + x^5 + x^6 + x^{10} + x^{12} + x^{14} + x^{16} + x^{18} + x^{19} + x^{23} + x^{24}$$

$$f_3(x) = x^2 + x^5 + x^7 + x^{12} + x^{13} + x^{16} + x^{17} + x^{20} + x^{25}$$

donde f_2 y f_3 son g-reductores.

1.3 Apartado 3

Aplica Berlekamp si es necesario recursivamente para hallar la descomposición en irreducibles de $g(x)$ en $\mathbb{Z}_2[x]$.

Comenzamos trabajando con f_2 , para el que calculamos $(g, f_2) = h_1$ y $(g, f_2 + 1) = h_2$ y comprobamos que son libres de cuadrados:

$$(g, f_2) = x^2 + x + 1$$

$$(g, f_2 + 1) = x^{24} + x^{23} + x^{19} + x^{18} + x^{16} + x^{14} + x^{12} + x^{10} + x^6 + x^5 + x^4 + x^3 + x + 1$$

Luego tenemos que $g = h_1 \cdot h_2$.

Comprobamos que tanto h_1 como h_2 son libres de cuadrados, pues $(h_1, h'_1) = 1$ y $(h_2, h'_2) = 1$.

El menor cuerpo de característica que contiene las raíces de h_1 es F_{2^2} , y como h_1 tiene grado 2, por tanto es irreducible.

Como h_2 tiene grado 24 y el menor cuerpo de característica 2 que contiene sus raíces es $F_{2^{23}}$, con 23|24, no sabemos si debe ser irreducible. En efecto, tenemos que h_2 tiene 1 como raíz y por tanto descompone como

$$h_2 = (x + 1) \cdot (x^{23} + x^{18} + x^{15} + x^{14} + x^{11} + x^{10} + x^5 + x^3 + 1)$$

Luego la descomposición en irreducibles de g es:

$$g = (x + 1) \cdot (x^2 + x + 1) \cdot (x^{23} + x^{18} + x^{15} + x^{14} + x^{11} + x^{10} + x^5 + x^3 + 1)$$

Hacemos lo análogo con f_3 , considerando $(g, f_3) = h_3$ y $(g, f_3 + 1) = h_4$

$$\begin{aligned} (g, f_3) &= x^{23} + x^{18} + x^{15} + x^{14} + x^{11} + x^{10} + x^5 + x^3 + 1 \\ (g, f_3+1) &= x^3 + 1 \end{aligned}$$

Obteniendo por tanto que $g = h_3 \cdot h_4$

Comprobamos que tanto h_3 como h_4 son libres de cuadrados, pues $(h_3, h'_3) = 1$ y $(h_4, h'_4) = 1$.

El menor cuerpo de característica 2 que contiene las raíces de h_3 es $F_{2^{23}}$, y como h_3 tiene grado 23 tenemos que es irreducible.

De nuevo, observamos que h_4 tiene grado 4 y el menor cuerpo de característica 2 que contiene sus raíces es F_{2^2} , luego no sabemos si es irreducible, si lo fuera, tendría un factor de grado 1 y otro de grado 2, y en efecto $h_4 = (x + 1) \cdot (x^2 + x + 1)$, pues 1 es raíz suya, y la descomposición de g en irreducibles resulta:

$$g = (x + 1) \cdot (x^2 + x + 1) \cdot (x^{23} + x^{18} + x^{15} + x^{14} + x^{11} + x^{10} + x^5 + x^3 + 1)$$

1.4 Apartado 4

Haz lo mismo para hallar la descomposición en irreducibles de $f(x)$ mod 3

Nota: En este apartado se va a usar y en lugar de x para los polinomios para que vaya de acuerdo al código implementado.

Tenemos que $h = f \mod 3 = y^{26} + y^{23} + y^{21} + y^{17} + y^{15} + y^{13} + y^{11} + y^{10} + y^8 + y^6 + y^5 + 1$

Tenemos que $(h, h') = 1$, luego h es libre de cuadrados.

El menor cuerpo de característica 3 que contiene las raíces de h es $F_{3^{117}} = F_{3^{3^2 \cdot 13}}$, y como $117 > 26$ tenemos que h es reducible, con factores de grado 1, 3, 9 o 13.

Calculamos ahora la matriz B por columnas, para lo que calculamos de nuevo primero $y^{2^i} \mod h$ con $0 \leq i < 26$:

$$\begin{aligned} [0] \quad x^{2^0} \mod f &= 1 \\ [1] \quad x^{2^1} \mod f &= y^3 \\ [2] \quad x^{2^2} \mod f &= y^6 \\ [3] \quad x^{2^3} \mod f &= y^9 \\ [4] \quad x^{2^4} \mod f &= y^{12} \\ [5] \quad x^{2^5} \mod f &= y^{15} \\ [6] \quad x^{2^6} \mod f &= y^{18} \\ [7] \quad x^{2^7} \mod f &= y^{21} \end{aligned}$$

[8] $x^{2i} \bmod f = y^{24}$
 [9] $x^{2i} \bmod f = 2y^{24} + 2y^{22} + 2y^{18} + 2y^{16} + 2y^{14} + 2y^{12} + 2y^{11} + 2y^9 + 2y^7 + 2y^6 + 2y$
 [10] $x^{2i} \bmod f = 2y^{25} + y^{24} + y^{22} + 2y^{21} + 2y^{19} + y^{18} + 2y^{17} + y^{16} + 2y^{15} + y^{11} + 2y^{10} + y^7 + y^6 + 2y^4 + y$
 [11] $x^{2i} \bmod f = 2y^{25} + y^{24} + y^{23} + y^{22} + y^{21} + 2y^{20} + 2y^{19} + y^{18} + y^{17} + 2y^{16} + y^{15} + 2y^{11} + 2y^{10} + y^8 + 2y^7 + 2y^6 + y^4 + y^2 + 2y$
 [12] $x^{2i} \bmod f = 2y^{25} + 2y^{23} + y^{22} + y^{20} + 2y^{16} + y^{14} + 2y^{13} + 2y^{11} + 2y^{10} + y^9 + y^7 + y^6 + 2y^4 + y^2 + 2y + 2$
 [13] $x^{2i} \bmod f = 2y^{25} + y^{21} + 2y^{16} + 2y^{15} + 2y^{14} + y^{13} + 2y^{12} + y^{11} + y^9 + 2y^8 + y^6 + 2y^5 + 2y^4 + 2y^3 + y^2 + 1$
 [14] $x^{2i} \bmod f = y^{25} + y^{24} + y^{23} + 2y^{18} + y^{16} + y^{14} + y^{13} + 2y^{12} + 2y^{11} + y^{10} + y^9 + 2y^6 + y^5 + y^3 + y^2$
 [15] $x^{2i} \bmod f = 2y^{25} + 2y^{24} + y^{23} + 2y^{22} + y^{21} + 2y^{18} + 2y^{17} + y^{14} + 2y^{13} + 2y^{12} + y^{11} + y^{10} + y^9 + 2y^8 + y^7 + 2y^6 + 2y^2 + 2y + 2$
 [16] $x^{2i} \bmod f = 2y^{24} + y^{22} + y^{21} + 2y^{20} + y^{19} + y^{18} + y^{17} + 2y^{15} + 2y^{14} + y^{13} + 2y^{11} + y^{10} + 2y^7 + y^5 + 2y^4 + 2y^3 + y^2 + y + 2$
 [17] $x^{2i} \bmod f = y^{25} + 2y^{24} + 2y^{23} + 2y^{22} + y^{21} + y^{20} + 2y^{17} + 2y^{16} + y^{13} + y^{12} + y^{11} + 2y^{10} + y^9 + y^8 + y^5 + y^4 + 2y^3 + y$
 [18] $x^{2i} \bmod f = y^{25} + 2y^{24} + y^{23} + y^{22} + y^{21} + 2y^{20} + y^{19} + y^{18} + 2y^{16} + y^{15} + 2y^{14} + 2y^{13} + y^{12} + y^9 + y^8 + y^7 + y^6 + y^5 + y^4 + 2y^2 + y + 1$
 [19] $x^{2i} \bmod f = 2y^{24} + 2y^{22} + y^{19} + 2y^{18} + 2y^{15} + y^{14} + y^{13} + y^{12} + y^{11} + 2y^{10} + 2y^9 + 2y^8 + y^7 + y^5 + y^4 + y^3 + 2y^2 + y + 2$
 [20] $x^{2i} \bmod f = 2y^{25} + y^{24} + 2y^{22} + 2y^{21} + y^{17} + 2y^{16} + y^{15} + 2y^{14} + 2y^{13} + y^{10} + y^9 + y^8 + 2y^7 + 2y^6 + 2y^5 + y^4 + 2y^3 + y$
 [21] $x^{2i} \bmod f = y^{24} + y^{23} + 2y^{22} + y^{20} + y^{16} + y^{15} + 2y^{14} + 2y^{13} + y^{12} + y^9 + y^7 + y^6 + y^4 + y^2 + 2y$
 [22] $x^{2i} \bmod f = 2y^{25} + 2y^{24} + 2y^{22} + 2y^{21} + y^{19} + y^{17} + y^{16} + 2y^{14} + 2y^{13} + y^{11} + 2y^8 + y^6 + 2y^4 + 2y + 2$
 [23] $x^{2i} \bmod f = y^{23} + 2y^{22} + y^{20} + 2y^{19} + y^{18} + y^{15} + 2y^{14} + y^{13} + 2y^{12} + y^{10} + 2y^9 + y^8 + y^7 + y^6 + 2y^4 + 2y^3 + y^2 + y$
 [24] $x^{2i} \bmod f = 2y^{25} + 2y^{22} + y^{18} + y^{17} + y^{16} + y^{15} + 2y^{12} + y^9 + 2y^8 + 2y^7 + y^6 + y^4 + 2$
 [25] $x^{2i} \bmod f = y^{23} + y^{21} + y^{20} + 2y^{19} + y^{18} + y^{17} + y^{13} + 2y^{12} + 2y^{11} + y^9 + y^8 + 2y^7 + 2y^3 + y^2$

Y B, con sus filas formadas por los coeficientes de estos polinomios, resulta:

```

[1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0]
[0 0 0 1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0]
[0 0 0 0 0 0 1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0]
[0 0 0 0 0 0 0 0 1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0]
[0 0 0 0 0 0 0 0 0 0 0 0 1 0 0 0 0 0 0 0 0 0 0 0 0]
[0 0 0 0 0 0 0 0 0 0 0 0 0 0 1 0 0 0 0 0 0 0 0 0 0]
[0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 1 0 0 0 0 0 0 0 0]
[0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 1 0 0 0 0 0 0]
[0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 1 0 0 0 0]
[0 2 0 0 0 0 2 2 0 2 0 2 2 0 2 0 2 0 2 0 0 0 2 0 2 0]
[0 1 0 0 2 0 1 1 0 0 2 1 0 0 0 2 1 2 1 2 0 2 1 0 1 2]
[0 2 1 0 1 0 2 2 1 0 2 2 0 0 0 1 2 1 1 2 2 1 1 1 1 2]

```

```

[2 2 1 0 2 0 1 1 0 1 2 2 0 2 1 0 2 0 0 0 1 0 1 2 0 2]
[1 0 1 2 2 2 1 0 2 1 0 1 2 1 2 2 2 0 0 0 0 1 0 0 0 2]
[0 0 1 1 0 1 2 0 0 1 1 2 2 1 1 0 1 0 2 0 0 0 0 1 1 1]
[2 2 2 0 0 0 2 1 2 1 1 1 2 2 1 0 0 2 2 0 0 1 2 1 2 2]
[2 1 1 2 2 1 0 2 0 0 1 2 0 1 2 2 0 1 1 1 2 1 1 0 2 0]
[0 1 0 2 1 1 0 0 1 1 2 1 1 1 0 0 2 2 0 0 1 1 2 2 2 1]
[1 1 2 0 1 1 1 1 1 1 0 0 1 2 2 1 2 0 1 1 2 1 1 1 2 1]
[2 1 2 1 1 1 0 1 2 2 2 1 1 1 1 2 0 0 2 1 0 0 2 0 2 0]
[0 1 0 2 1 2 2 2 1 1 1 0 0 2 2 1 2 1 0 0 0 2 2 0 1 2]
[0 2 1 0 1 0 1 1 0 1 0 0 1 2 2 1 1 0 0 0 1 0 2 1 1 0]
[2 2 0 0 2 0 1 0 2 0 0 1 0 2 2 0 1 1 0 1 0 2 2 0 2 2]
[0 1 1 2 2 0 1 1 1 2 1 0 2 1 2 1 0 0 1 2 1 0 2 1 0 0]
[2 0 0 0 1 0 1 2 2 1 0 0 2 0 0 1 1 1 1 0 0 0 2 0 0 2]
[0 0 1 2 0 0 0 2 1 1 0 2 2 1 0 0 0 1 1 2 1 1 0 1 0 0]

```

Como (B-Id) tiene rango 22, entonces $26 - 22 = 4$ tendremos 4 soluciones.
Y resolvemos el sistema (B-Id)X=0, obteniendo como soluciones:

```

[1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0]
[0 2 0 1 1 1 1 2 1 1 0 1 1 0 1 0 2 2 0 0 1 1 2 0 1 0]
[0 0 1 2 0 2 1 0 2 0 1 1 2 1 0 1 0 1 2 1 1 2 2 2 0 0]
[0 0 0 0 1 2 0 1 0 1 2 0 1 0 1 2 2 2 2 1 0 0 2 0 0 1]

```

Que son los siguientes polinomios:

$$f_1 = 1$$

$$f_2 = 2*y + y^3 + y^4 + y^5 + y^6 + 2*y^7 + y^8 + y^9 + y^{11} + y^{12} + y^{14} + 2*y^{16} + 2*y^{17} + y^{20} + y^{21} + 2*y^{22} + y^{24}$$

$$f_3 = y^2 + 2*y^3 + 2*y^5 + y^6 + 2*y^8 + y^{10} + y^{11} + 2*y^{12} + y^{13} + y^{15} + y^{17} + 2*y^{18} + y^{19} + y^{20} + 2*y^{21} + 2*y^{22} + 2*y^{23}$$

$$f_4 = y^4 + 2*y^5 + y^7 + y^9 + 2*y^{10} + y^{12} + y^{14} + 2*y^{15} + 2*y^{16} + 2*y^{17} + 2*y^{18} + y^{19} + 2*y^{22} + y^{25}$$

Calculamos los mcd correspondientes a f_2 , siendo $h_1 = (g, f_2)$, $h_2 = (g, f_2 + 1)$ y $h_3 = (g, f_2 + 2)$:

$$(g, f_2) = y^3 + 2*y^2 + 1$$

$$(g, f_2+1) = y^{13} + 2*y^{12} + y^{11} + y^{10} + 2*y^9 + 2*y^8 + 2*y^7 + y^5 + y^4 + y^2 + 2$$

$$(g, f_2+2) = y^{10} + 2*y^9 + 2*y^8 + y^5 + 2*y^4 + y^3 + y^2 + 2$$

Obtenemos por tanto que $h = h_1 \cdot h_2 \cdot h_3$, siendo estos tres polinomios libres de cuadrados, y como el mínimo cuerpo de característica 3 que contiene las raíces de h_1 es F_{3^3} , coincidiendo 3 con su grado, se tiene que es irreducible. Análogamente se tiene que para h_2 es $F_{3^{13}}$ y su grado es 13, y por tanto es irreducible. Mientras para h_3 es F_{3^9} , siendo 9 distinto de su grado, por lo que es reducible y es fácil comprobar que tiene 1 como raíz simple, luego se descompone en $h_3 = (x + 2) \cdot (y^9 + 2y^7 + 2y^6 + 2y^5 + 2y^3 + y + 1)$, luego la descomposición de h en irreducibles es:

$$h = (y^3 + 2y^2 + 1) \cdot (y^{13} + 2y^{12} + y^{11} + y^{10} + 2*y^9 + 2*y^8 + 2*y^7 + y^5 + y^4 + y^2 + 2) \cdot (y + 2) \cdot (y^9 + 2y^7 + 2y^6 + 2y^5 + 2y^3 + y + 1)$$

Para f_3 , siendo $h_4 = (g, f_3)$, $h_5 = (g, f_3 + 1)$ y $h_6 = (g, f_3 + 2)$:

$$\begin{aligned}
(g, f_3) &= y^{16} + y^{15} + 2y^{14} + y^{13} + y^{11} + y^{10} + 2y^7 + 2y^6 + \\
&\quad 2y^5 + 2y^3 + 2y^2 + 2 \\
(g, f_{3+1}) &= y^9 + 2y^7 + 2y^6 + 2y^5 + 2y^3 + y + 1 \\
(g, f_{3+2}) &= y + 2
\end{aligned}$$

Obtenemos por tanto que $h = h_4 \cdot h_5 \cdot h_6$, siendo todos ellos libres de cuadrados, y como el mínimo cuerpo de característica 3 que contiene las raíces de h_5 es F_{3^9} , coincidiendo 9 con su grado, se tiene que es irreducible. Análogamente se tiene que para h_6 es F_{3^1} , y por tanto es irreducible. Mientras para h_4 es $F_{3^{39}}$, mayor de su grado, y por tanto aplicamos el algoritmo de nuevo a este polinomio:

$$\begin{aligned}
[0] \quad x^{2i} \bmod f &= 1 \\
[1] \quad x^{2i} \bmod f &= y^3 \\
[2] \quad x^{2i} \bmod f &= y^6 \\
[3] \quad x^{2i} \bmod f &= y^9 \\
[4] \quad x^{2i} \bmod f &= y^{12} \\
[5] \quad x^{2i} \bmod f &= y^{15} \\
[6] \quad x^{2i} \bmod f &= 2y^{15} + 2y^{11} + y^{10} + y^9 + 2y^7 + y^6 + y^3 + 2y + 2 \\
[7] \quad x^{2i} \bmod f &= y^{15} + 2y^{14} + y^{13} + y^{12} + y^{11} + y^{10} + y^7 + 2y^4 + \\
&\quad y^3 + y + 1 \\
[8] \quad x^{2i} \bmod f &= y^{14} + 2y^{13} + y^{12} + y^{11} + y^9 + 2y^8 + 2y^7 + 2y^5 + \\
&\quad 2y^2 + y + 1 \\
[9] \quad x^{2i} \bmod f &= y^{15} + y^{14} + 2y^{13} + y^{10} + 2y^7 + 2y^6 + 2y^4 + \\
&\quad y^2 + y + 1 \\
[10] \quad x^{2i} \bmod f &= 2y^{15} + 2y^{12} + 2y^{10} + y^8 + 2y^5 + 2y^4 + y^3 + \\
&\quad y^2 \\
[11] \quad x^{2i} \bmod f &= 2y^{13} + 2y^{11} + 2y^{10} + 2y^9 + 2y^8 + y^5 + 2y^3 + \\
&\quad y + 1 \\
[12] \quad x^{2i} \bmod f &= y^{15} + y^{14} + 2y^{12} + y^{10} + y^8 + 2y^7 + y^6 + 2y^5 + \\
&\quad y^4 + 2y^2 + 2 \\
[13] \quad x^{2i} \bmod f &= y^{14} + 2y^{13} + 2y^{12} + y^{10} + 2y^9 + y^6 + y^5 + y^4 + \\
&\quad 2y^2 + 1 \\
[14] \quad x^{2i} \bmod f &= 2y^{15} + y^{12} + y^{11} + 2y^{10} + y^9 + 2y^8 + 2y^6 + y^4 + \\
&\quad y^2 + y + 1 \\
[15] \quad x^{2i} \bmod f &= 2y^{15} + y^{14} + 2y^{13} + y^{12} + 2y^{10} + y^9 + 2y^7 + 2y^6 + \\
&\quad y^5 + y^4 + y + 1
\end{aligned}$$

Y obtenemos la matriz:

$$\begin{bmatrix}
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\
2 & 2 & 0 & 1 & 0 & 0 & 1 & 2 & 0 & 1 & 1 & 2 & 0 & 0 & 0 & 2 \\
1 & 1 & 0 & 1 & 2 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 1 & 2 & 1 & 1 \\
1 & 1 & 2 & 0 & 0 & 2 & 0 & 2 & 2 & 1 & 0 & 1 & 1 & 2 & 1 & 0 \\
1 & 1 & 1 & 0 & 2 & 0 & 2 & 2 & 0 & 0 & 1 & 0 & 0 & 2 & 1 & 1 \\
0 & 0 & 1 & 1 & 2 & 2 & 0 & 0 & 1 & 0 & 2 & 0 & 2 & 0 & 0 & 2
\end{bmatrix}$$

```

[1 1 0 2 0 1 0 0 2 2 2 2 0 2 0 0]
[2 0 2 0 1 2 1 2 1 0 1 0 2 0 1 1]
[1 0 2 0 1 1 1 0 0 2 1 0 2 2 1 0]
[1 1 1 0 1 0 2 0 2 1 2 1 1 0 0 2]
[1 1 0 0 1 1 2 2 0 1 2 0 1 2 1 2]

```

Como rango de (B-Id) es 14, tenemos que $16-14=2$ soluciones que tenemos. Las soluciones son:

```

[1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0]
[0 1 0 2 0 2 2 0 1 1 1 2 2 1 2 0]

```

Luego obtenemos el polinomio $f_5 = y + 2y^3 + 2y^5 + 2y^6 + y^8 + y^9 + y^{10} + 2y^{11} + 2y^{12} + y^{13} + 2y^{14}$.

Calculamos ahora los mcd asociados a f_5 , llamando $h_{10} = (g, f_5)$, $h_{11} = (g, f_5 + 1)$ y $h_{12} = (g, f_5 + 2)$:

```

(g, f5) = y^13 + 2*y^12 + y^11 + y^10 + 2*y^9 + 2*y^8 + 2*y^7 + y^5 + y^4 + y^2 + 2
(g, f5+1) = 1
(g, f5+2) = y^3 + 2*y^2 + 1

```

Obtenemos los polinomios h_{10}, h_{11}, h_{12} y todos ellos son libres de cuadrados e irreducibles, pues el mínimo cuerpo de característica 3 que contiene las raíces de h_{10} es $F_{3^{13}}$, a h_{11} es F_{3^1} y a h_{12} es F_{3^3} . Por tanto $h_4 = h_{10} \cdot h_{11} \cdot h_{12}$ es su descomposición en irreducibles y la de h queda como:

$$h = (y^3 + 2y^2 + 1) \cdot (y^{13} + 2y^{12} + y^{11} + y^{10} + 2y^9 + 2y^8 + 2y^7 + y^5 + y^4 + y^2 + 2) \cdot (y + 2) \cdot (y^9 + 2y^7 + 2y^6 + 2y^5 + 2y^3 + y + 1)$$

Finalmente, para f_4 , considerando $h_7 = (g, f_4)$, $h_8 = (g, f_4 + 1)$ y $h_9 = (g, f_4 + 2)$:

```

(g, f4) = y + 2
(g, f4+1) = y^22 + 2*y^21 + y^19 + y^18 + y^17 + 2*y^15 + y^14 + 2*y^13 + y^12 +
2*y^11 + 2*y^10 + y^9 + 2*y^8 + y^7 + 2*y^6 + 2*y^5 + y^4 + 2*y^3 + y^2 + 2*y + 2
(g, f4+2) = y^3 + 2*y^2 + 1

```

Obtenemos por tanto que $h = h_7 \cdot h_8 \cdot h_9$, siendo estos libres de cuadrados, y como el mínimo cuerpo de característica 3 que contiene las raíces de h_7 es F_{3^1} , coincidiendo 1 con su grado, se tiene que es irreducible. Análogamente se tiene que para h_9 es F_{3^3} , y por tanto es irreducible. Mientras para h_8 es $F_{3^{117}}$, con 117 mayor de su grado, y por tanto aplicamos el algoritmo de nuevo a este polinomio.

De nuevo, se obtiene:

```

[0] x^2i mod f = 1
[1] x^2i mod f = y^3
[2] x^2i mod f = y^6
[3] x^2i mod f = y^9
[4] x^2i mod f = y^12
[5] x^2i mod f = y^15
[6] x^2i mod f = y^18
[7] x^2i mod f = y^21

```


[8] $x^{2i} \bmod f = y^{20} + y^{18} + y^{15} + 2y^{14} + y^{13} + y^{12} + y^{11} + y^{10} + 2y^9 + y^8 + y^7 + y^6 + y^5 + 2y^4 + y^3 + y^2 + 2y + 1$
 [9] $x^{2i} \bmod f = 2y^{21} + 2y^{20} + y^{19} + 2y^{18} + y^{17} + 2y^{16} + y^{15} + y^{14} + y^{13} + 2y^{12} + y^{10} + y^9 + y^8 + 2y^7 + y^5 + 2y^4 + y^3 + 2y + 1$
 [10] $x^{2i} \bmod f = 2y^{21} + y^{20} + y^{18} + y^{17} + 2y^{15} + y^{13} + 2y^{12} + 2y^{11} + 2y^{10} + y^8 + 2y^6 + 2y^4 + y^3 + y^2 + 2$
 [11] $x^{2i} \bmod f = 2y^{21} + 2y^{20} + y^{19} + 2y^{18} + 2y^{17} + 2y^{16} + y^{15} + y^{13} + 2y^{12} + 2y^{11} + 2y^{10} + 2y^8 + y^7 + 2y^6 + y^4 + y^3 + 2y^2$
 [12] $x^{2i} \bmod f = 2y^{21} + 2y^{20} + y^{18} + 2y^{15} + 2y^{14} + 2y^{13} + y^{12} + y^{10} + 2y^9 + 2y^7 + 2y^6 + 2y^5 + y^2 + 2$
 [13] $x^{2i} \bmod f = 2y^{19} + y^{16} + y^{14} + y^{12} + y^{10} + y^8 + 2y^7 + y^4 + y^3 + 2y^2 + 2y + 1$
 [14] $x^{2i} \bmod f = 2y^{21} + 2y^{19} + y^{18} + 2y^{17} + y^{14} + y^{12} + y^{10} + y^9 + 2y^8 + 2y^7 + y^5 + y^2 + 2y + 2$
 [15] $x^{2i} \bmod f = y^{20} + y^{19} + 2y^{17} + 2y^{15} + 2y^{14} + 2y^{13} + y^{12} + 2y^9 + 2y^8 + y^6 + 2y^5 + y^4 + 1$
 [16] $x^{2i} \bmod f = 2y^{21} + y^{20} + 2y^{18} + 2y^{15} + 2y^{14} + y^{13} + y^{12} + 2y^{11} + y^{10} + y^5 + 2y^4 + 2y^3 + 2y^2 + 2$
 [17] $x^{2i} \bmod f = y^{20} + y^{19} + 2y^{18} + y^{17} + 2y^{16} + 2y^{12} + y^{11} + 2y^{10} + y^9 + y^7 + y^5 + y^4 + y^3 + 2y^2$
 [18] $x^{2i} \bmod f = y^{21} + 2y^{19} + y^{17} + y^{16} + 2y^{10} + 2y^9 + 2y^8 + y^6 + 2y^4 + y^3 + 2y^2 + 2$
 [19] $x^{2i} \bmod f = 2y^{21} + 2y^{20} + 2y^{19} + 2y^{18} + y^{17} + 2y^{13} + y^{12} + 2y^{11} + y^9 + y^7 + y^6 + 2y^5 + 2y^3 + 2y^2 + y$
 [20] $x^{2i} \bmod f = y^{20} + 2y^{18} + 2y^{17} + y^{16} + 2y^{15} + y^{14} + y^{13} + y^{12} + 2y^{11} + 2y^{10} + y^6 + y^3 + y$
 [21] $x^{2i} \bmod f = y^{20} + 2y^{19} + 2y^{16} + y^{15} + 2y^{14} + 2y^{13} + 2y^{11} + y^9 + y^4 + 2y + 1$

Y la matriz resulta:

```

[1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0]
[0 0 0 1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0]
[0 0 0 0 0 0 1 0 0 0 0 0 0 0 0 0 0 0 0 0 0]
[0 0 0 0 0 0 0 0 0 1 0 0 0 0 0 0 0 0 0 0 0]
[0 0 0 0 0 0 0 0 0 0 0 0 1 0 0 0 0 0 0 0 0]
[0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 1 0 0 0 0 0]
[0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 1 0 0 0]
[0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 1 0]
[1 2 1 1 2 1 1 1 1 2 1 1 1 1 2 1 0 0 1 0 1]
[1 2 0 1 2 1 0 2 1 1 1 0 2 1 1 1 2 1 2 1 2]
[2 0 1 1 2 0 2 0 1 0 2 2 2 1 0 2 0 1 1 0 1]
[0 0 2 1 1 0 2 1 2 0 2 2 2 1 0 1 2 2 2 1 2]
[2 0 1 0 0 2 2 2 0 2 1 0 1 2 2 2 0 0 1 0 2]
[1 2 2 1 1 0 0 2 1 0 1 0 1 0 1 0 1 0 0 2 0]
[2 2 1 0 0 1 0 2 2 1 1 0 1 0 1 0 0 2 1 2 0]
[1 0 0 0 1 2 1 0 2 2 0 0 1 2 2 2 0 2 0 1 1]
[2 0 2 2 2 1 0 0 0 0 1 2 1 1 2 2 0 0 2 0 1]
[0 0 2 1 1 1 0 1 0 1 2 1 2 0 0 0 2 1 2 1 1]
[2 0 2 1 2 0 1 0 2 2 2 0 0 0 0 0 1 1 0 2 0]

```

```
[0 1 2 2 0 2 1 1 0 1 0 2 1 2 0 0 0 1 2 2 2 2]
[0 1 0 1 0 0 1 0 0 0 2 2 1 1 1 2 1 2 2 0 1 0]
[1 2 0 0 1 0 0 0 0 1 0 2 0 2 2 1 2 0 0 2 1 0]
```

Como rango de (B-Id) se tiene 20, entonces $22-20=2$ soluciones, que son:

```
[1 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0]
[0 0 2 1 1 1 1 1 1 1 0 1 0 0 1 0 2 0 2 1 2 0]
```

Luego obtenemos el polinomio $f_6 = 2 * y^2 + y^3 + y^4 + y^5 + y^6 + y^7 + y^8 + y^9 + y^{11} + y^{14} + 2 * y^{16} + 2 * y^{18} + y^{19} + 2 * y^{20}$

Consideramos $h_{13} = (g, f_6)$, $h_{14} = (g, f_6 + 1)$ y $h_{15} = (g, f_6 + 2)$:

```
(g, f6) = 1
(g, f6+1) = y^13 + 2*y^12 + y^11 + y^10 + 2*y^9 + 2*y^8 + 2*y^7 +
y^5 + y^4 + y^2 + 2
(g, f6+2) = y^9 + 2*y^7 + 2*y^6 + 2*y^5 + 2*y^3 + y + 1
```

Obtenemos los polinomios h_{13}, h_{14}, h_{15} y todos ellos son libres de cuadrados e irreducibles, pues el mínimo cuerpo de característica 3 que contiene las raíces de h_{13} es $F_{3^{13}}$, de h_{14} es $F_{3^{13}}$ y de h_{15} es F_{3^9} . Por tanto $h_8 = h_{13} \cdot h_{14} \cdot h_{15}$ es su descomposición en irreducibles y la de h queda como:

$$h = (y^3 + 2y^2 + 1) \cdot (y^{13} + 2y^{12} + y^{11} + y^{10} + 2 * y^9 + 2 * y^8 + 2 * y^7 + y^5 + y^4 + y^2 + 2) \cdot (y + 2) \cdot (y^9 + 2y^7 + 2y^6 + 2y^5 + 2y^3 + y + 1)$$

1.5 Apartado 5

¿ Qué deduces sobre la reducibilidad de $f(x)$ en $\mathbb{Z}[x]$?

Como g descompone en $\mathbb{Z}_2[x]$ en 3 polinomios irreducibles de grados 1, 2 y 23, y en $\mathbb{Z}_3[x]$ en 4 polinomios irreducibles de grados 1, 3, 9 y 13, tenemos que las factorizaciones no son incompatibles y por tanto no podemos asegurar que g sea irreducible en $\mathbb{Z}[x]$, ya que podría descomponer en un polinomio de grado 1 y otro de grado 25.

Pese a esto, lo he comprobado y el polinomio en efecto es irreducible.