Ejercicio 9

David García Curbelo

Preámbulo

Toma tu número $n = 45352609$ de la lista publicada 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.

Tenemos que $n_2 = 10101101000000011010100001$, luego tenemos definido el polinomio

$$f(x) = x^{25} + x^{23} + x^{21} + x^{20} + x^{18} + x^{11} + x^{10} + x^9 + x^7 + x^5 + 1$$

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

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

El menor cuerpo de característica 2 que contenga a todas las raíces de g es $F_{2^{280}} = F_{2^{8 \cdot 5 \cdot 7}}$. Ahora, como 280 es mayor estricto que el grado del polinomio, entonces sabemos que $g(x)$ es irreducible en $\mathbb{Z}_2[x]$.

Apartado II. ***Extrae la parte libre de cuadrados de*** $g(x)$ ***y le calculas su matriz de Berlekamp por columnas. Resuelve el s.l.*** $(B - Id)X = 0$**.**
Sabemos que el propio polinomio $g(x)$ es libre de cuadrados. Tenemos que x^{2i} con $0 \leq i \leq 25$ en módulo $f(x)$ tenemos

1. 1
2. x^2
3. x^4
4. x^6
5. x^8
6. x^{10}
7. x^{12}
8. x^{14}
9. x^{16}
10. x^{18}
11. x^{20}
12. x^{22}
13. x^{24}
14. $x + x^6 + x^8 + x^{10} + x^{11} + x^{12} + x^{19} + x^{21} + x^{22} + x^{24}$
15. $x + x^3 + x^6 + x^{11} + x^{13} + x^{14} + x^{19} + x^{22} + x^{23}$
16. $1 + x^3 + x^7 + x^8 + x^9 + x^{10} + x^{11} + x^{13} + x^{15} + x^{16} + x^{18} + x^{20} + x^{23} + x^{24}$
17. $1 + x + x^2 + x^6 + x^7 + x^8 + x^{10} + x^{11} + x^{13} + x^{15} + x^{17} + x^{19} + x^{23} + x^{24}$
18. $1 + x + x^2 + x^3 + x^4 + x^5 + x^6 + x^7 + x^{10} + x^{13} + x^{15} + x^{17} + x^{18} + x^{20} + x^{21} + x^{22} + x^{23} + x^{24}$
19. $1 + x + x^2 + x^3 + x^4 + x^{15} + x^{17} + x^{18}$
20. $x^2 + x^3 + x^4 + x^5 + x^6 + x^{17} + x^{19} + x^{20}$
21. $x^4 + x^5 + x^6 + x^7 + x^8 + x^{19} + x^{21} + x^{22}$
22. $x^6 + x^7 + x^8 + x^9 + x^{10} + x^{21} + x^{23} + x^{24}$
23. $1 + x + x^5 + x^6 + x^7 + x^{10} + x^{11} + x^{18} + x^{19} + x^{20} + x^{22} + x^{24}$
24. $x + x^2 + x^3 + x^6 + x^7 + x^9 + x^{10} + x^{11} + x^{13} + x^{19} + x^{20}$
25. $x^3 + x^4 + x^5 + x^8 + x^9 + x^{11} + x^{12} + x^{13} + x^{15} + x^{21} + x^{22}$
26. $x^5 + x^6 + x^7 + x^{10} + x^{11} + x^{13} + x^{14} + x^{15} + x^{17} + x^{23} + x^{24}$

Obtenemos así las filas de la matriz de Berlekamp a partir de los coeficientes de estos polinomios:

$$\begin{pmatrix}
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 & 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 & 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 & 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 & 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 & 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 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 0 \\
0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 0 \\
1 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 1 & 0 \\
1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 \\
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 1 & 1 & 0 \\
1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 \\
1 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 & 0 & 1 & 0 \\
0 & 1 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0
\end{pmatrix}$$

El rango de $M - Id$ es 25. Por tanto habrá una única solución. Resolvemos el sistema $(M - Id)X = 0$ y obtenemos la solución siguiente:

$$\{1, 1, 1, 1, 1, 0, 1, 0, 1, 0, 0, 1, 1, 1, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 1, 0\}$$

Y esto nos lleva al polinomio g-reductor siguiente:

$$g_1(x) = 1 + x + x^2 + x^3 + x^4 + x^6 + x^8 + x^{11} + x^{12} + x^{13} + x^{15} + x^{16} + x^{19} + x^{20} + x^{22} + x^{23} + x^{24}$$

Apartado III. ***Aplica Berlekamp si es necesario recursivamente para hallar la descomposición en irreducibles de*** $g(x)$ ***en*** $\mathbb{Z}_2[x]$***.***
Vemos que el máximo común divisor de los polinomios $g_1(x)$ y $g(x)$ es 1. Por lo tanto, $g(x)$ es irreducible, en $\mathbb{Z}_2[x]$.

Apartado IV. ***Haz lo mismo para hallar la descomposición en irreducibles de*** $f(x) \pmod 3$

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