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 $\mathbb{Z}_2[x]$. Por tanto,

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

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