

Ejercicio 8

David García Curbelo

Preámbulo

Toma tu número $n = 191871308917122834687961459636870046909$ 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.

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 $\mathbb{Z}_2[x]$?*

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 $f(x)$*
(mod 3)

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