Universidad Carlos III de Madrid

***COSEC LAB**· Dpto. Informática*

Universidad Carlos III de Madrid

Problemas fundamentos matemáticos. Cuerpos de Galois

SOLUCIONES

CSI
Curso 2016/2017

Ana Isabel González-Tablas Ferreres

1. **Sea CG(2^8) definido por el polinomio irreducible p(x) = $x^8 + x^4 + x^3 + x + 1$.**
   Sea a(x) = x + 1 y b(x) = $x^7 + x^5 + x^4 + x^3 + x^2 + x + 1$
   Calcule: a(x) * b(x) mod p(x)
2. **Sea CG(2^8) definido por el polinomio irreducible p(x) = $x^8 + x^4 + x^3 + x + 1$.**
   Sea f(x)= $x^6 + x^4 + x^2 + x + 1$ y g(x) = $x^7 + x + 1$
   Calcule: f(x) * g(x) mod p(x)
3. **Sea CG(2^8) definido por el polinomio irreducible p(x) = $x^8 + x^4 + x^3 + x + 1$.**
   Calcule: (02)*(D4) + (03)*(BF) + (5D) + (30) mod p(x)
   Considere que cada dígito (0...9 A B C D E F) se codifica con 4 bits (código hexadecimal).
   Por ejemplo: (02) --> (0000 0011) = x + 1
   Por ejemplo: (BF) --> (1011 1111) = $x^7 + x^5 + x^4 + x^3 + x^2 + x + 1$
   Es decir, cada pareja de dígitos contenida en un paréntesis del cálculo que debe hacer, representa un polinomio de grado 7 o menor que pertenece por tanto al CG(2^8) donde se realiza el cálculo.

2) $CG(2^8)$ $p(x) = x^8 + x^4 + x^3 + x + 1 \Rightarrow (100011011)$

no se aplica $x^8 + x + 1$ porque no está en la lista.

$$\begin{cases} f(x) = x^6 + x^4 + x^2 + x + 1 \Rightarrow (1010111) \\ g(x) = x^7 + x + 1 \Rightarrow (10000011) \end{cases}$$

Hallar $f(x) \cdot g(x)$

$$\begin{array}{r} 1010111 \\ \text{AND}\ 10000011 \\ \hline 1010111 \\ \oplus\ 1010111 \\ \hline 10101110111001 \\ 10001101100000 \\ \hline 00100000011 \\ 10001101100 \\ \hline 00001100000 1 \end{array}$$

x^{13}

$$\begin{array}{r|l} 10101110111001 & 100011011 \\ \hline 10001101100000 & \\ \hline 00100000011 & \\ 10001101100 & \\ \hline 00001100000 1 & \end{array}$$

Solo me fijo en tamaño nomás valor

$$\begin{array}{r|l} 10001101100000 & 100011011 \\ \hline 1001000 & \end{array}$$

$$\boxed{f(x) \cdot g(x) = x^7 + x^6 + 1}$$

1) Mismo $CG(2^8)$ $f(x)$ igual

$a(x) = x + 1 \Rightarrow (11)$

$b(x) = x^7 + x^5 + x^4 + x^3 + x^2 + x + 1 \Rightarrow (10111111)$

$$\begin{array}{r} 10111111 \\ \times\ 11 \\ \hline 10111111 \\ 10111111 \\ \hline 11000001 \\ \oplus\ 100011011 \\ \hline 01101101 0 \end{array}$$

x^8

$$\begin{array}{r|l} 11000001 & 100011011 \\ \hline 1 & \end{array}$$

$$\boxed{a(x) \cdot b(x) = x^7 + x^6 + x^4 + x^3 + x} \quad \text{mod } p(x)$$

3) $CG(2^8)$ $\quad p(x) = x^8+x^4+x^3+x+1 \Rightarrow (100011011)$

$(02)\cdot(D4)+(03)\cdot(BF)+(5D)+(30) \bmod p(x)$

$D4 \Rightarrow 11010100$ $\quad$ $02 \Rightarrow 00000010$ (×)

$11010\,1000$

$BF \Rightarrow 1011\,1111$ $\quad$ $03 \Rightarrow 0000\,0011$

$1011\,1111$ (⊕) 10111111 (+)

$11100000\,1$ (+)

$5D \Rightarrow 0101\,1101$ (+)

$30 \Rightarrow 0011\,0000$

110101000
111000001 (⊕)
010111101
001100000

$000000100 \Rightarrow (x^2)$

Sol: $x^2 \bmod x^8+x^4+x^3+x+1$