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)

Solución: **$x^7 + x^6 + x^4 + x^3 + x$**

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)

Solución: **$x^7 + x^6 + 1$**

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.

Solución: **(04) = (0000 0100) = x^2**