Control de CTC: 12 de Marzo de 2014

Sean los siguientes polinomios con coeficientes en $\mathbb{Z}/\langle 2\rangle$

$$f := X^6 + X^5 + 1$$

$$g := X^6 + X^3 + X^2 + X + 1$$

$$h := X^6 + X^4 + X^2 + X + 1$$

Se pide:

(i) Deducir razonadamente cuáles son irreducibles y cuáles son primitivos.

(ii) Considérese el anillo/cuerpo $\mathbb{F}_{64} := \mathbb{F}_2[X]/\equiv_f$, y sea $\alpha := [X]_f$. Calcular si existe el inverso de $\alpha^2 + 1$ en ese anillo/ cuerpo.

(iii) Considérese el anillo/cuerpo $\mathbb{F}'_{64} := \mathbb{F}_2[X]/\equiv_h$, y sea $\gamma := [X]_h$. Calcular el orden multiplicativo de γ y también de $\gamma + 1$.

Ejercicio de Evaluación CTC : (1 de dic de 2014).

1. Resolver la ecuación en congruencias $14x \equiv 21 \bmod 91$.
2. Sabiendo que $91 = 7 \times 13$ Calcular $3^{57} \bmod 91$
3. Sea $f = X^6 + X^3 + 1 \in \mathbb{Z}/\langle 2\rangle[X]$, Demostrar que no tiene factores irreducibles en $\mathbb{Z}/\langle 2\rangle[X]$ de grados 1 ni 2. Concluir que f es irreducible en $\mathbb{Z}/\langle 2\rangle[X]$. ¿Es primitivo?
4. Llamemos $\alpha := [X]_f$. Escribir el inverso de $\alpha + 1$ en el cuerpo $\mathbb{F}_f = \mathbb{Z}/\langle 2\rangle[X]/\langle f\rangle$ expresándolo en función de la base

$$B := \{1, \alpha, \alpha^2, \alpha^3, \alpha^3, \alpha^4, \alpha^5\}$$

de $\mathbb{F}_f$ como $\mathbb{Z}/\langle 2\rangle$ -espacio vectorial.

Control CTC : (15 de Diciembre 2014).

1. Sea el polinomio $f \in \mathbb{F}_2[X]$, $f = X^6 + X^3 + 1$. Se pide:

   (i) Demostrar que f es irreducible ¿ Es f primitivo?

   (ii) En el cuerpo $\mathbb{F}_{64} = \mathbb{F}_2[X]/\langle f \rangle$ llamamos $\alpha := X \bmod f$. Calcular el inverso de $\alpha^3 + \alpha$ expresándolo en funcion de la base $B := \{1, \alpha, \alpha^2, \alpha^3, \alpha^4, \alpha^5\}$ de $\mathbb{F}_{64}$ como $\mathbb{F}_2$ espacio vectorial.

   (iii) Calcular el orden de α^3 en el grupo multiplicativo $\mathbb{F}_{64}^*$.

   (iv) Calcular el polinomio mínimo de α^3 sobre $\mathbb{F}_2$

   (iv) Descomponer en factores irreducibles sobre $\mathbb{F}_2[X]$ el siguiente polinomio $g := X^6 + X^5 + X^4 + X^3 + 1$

2. Calcular las soluciones en congruencias de a) $16x \equiv 12 \mathrm{m}od 24$, b) $x^2 \equiv 23 \mathrm{m}od 77$

Ejercicio de Evaluación CTC : (10 de Abril de 2013).

1. Resolver la ecuación en congruencias $x^2 \equiv 58 \bmod 77$.
2. Sabiendo que $91 = 7 \times 13$ Calcular $3^{57} \bmod 91$
3. Sea $f = X^3 - X - 1 \in \mathbb{Z}/\langle 3 \rangle[X]$, ¿Es f es irreducible en $\mathbb{Z}/\langle 3 \rangle[X]$? ¿ Es primitivo?.
4. Continuación de 3.: Llamemos $\alpha := [X]_f$. Escribir el inverso de $\alpha + 1$ en el cuerpo $\mathbb{F}_f = \mathbb{Z}/\langle 3 \rangle[X]/\langle f \rangle$ expresándolo en función de la base
   $$B := \{1, \alpha, \alpha^2\}$$
   de $\mathbb{F}_f$ como $\mathbb{Z}/\langle 3 \rangle$ -espacio vectorial. Calcular el orden de α^4 en el grupo multiplicativo $\mathbb{F}_f \setminus \{0\}$.