Curso 2017-18. Convocatoria extraordinaria 2.

Dados los polinomios,

$$p(x) = 1 + 8x - 5x^2 - 6x^3 \quad \text{y} \quad q(x) = -2 + 8x^2.$$

Se pide:

a) Utilizar el algoritmo de Euclides en $\mathbb{Z}_7[x]$, para calcular un máximo común divisor, $d(x)$, de $p(x)$ y $q(x)$.

b) ¿Existe otro polinomio que sea máximo común divisor de $p(x)$ y $q(x)$ en $\mathbb{Z}_7[x]$? Razonar la respuesta.

c) Expresar $d(x)$ (obtenido en el apartado a), como combinación de $p(x)$ y $q(x)$ en $\mathbb{Z}_7[x]$ (Identidad de Bezout); esto es, calcular $\lambda(x)$ y $\mu(x)$ en $\mathbb{Z}_7[x]$ tales que $d(x) = \lambda(x)\,p(x) + \mu(x)\,q(x)$.

$p(x) = -6x^3 - 5x^2 + 8x + 1 = x^3 + 2x^2 + x + 1$

$q(x) = 8x^2 - 2 = x^2 + 5$

$x^3 + 2x^2 + x + 1 = p(x)$ | $x^2 + 5 = q(x)$

$-x^3 \qquad -5x$ | $x + 2 = q_1(x)$

$2x^2 - 4x + 1 =$

$= 2x^2 + 3x + 1$

$-2x^2 \qquad -10$

$3x - 9 = 3x - 2 = 3x + 5 = r_1(x)$

a 7

5

$\bar{a} = \bar{5}$

$-6 = ?$

$\bar{6} + \bar{1} = \bar{0} = \bar{7}$

$-\bar{6} = \bar{1}$

$p(x) = q(x) \cdot q_1(x) + r_1(x)$

$q(x) = q_1(x) \cdot q_2(x)$

$x^2 + 5 \quad | \; 3x + 5$

$5x + 1 = q_2(x)$

$-15x^2 - 25x$

$-14x^2 - 25x + 5 =$

$= -4x + 5 =$

$= 3x + 5$

$-3x - 5$

$0 = r_2(x)$

$d(x) = (p(x), q(x)) = r_1(x) = 3x + 5$

$\frac{x^2}{3x} = 3^{-1} \cdot x = 5x$

$3^{-1} = ?$

$3 \cdot 5 = 15 = 1$

$3^{-1} = 5$

Curso 2017-18. Convocatoria extraordinaria 2.

Dados los polinomios,

$$p(x) = 1 + 8\,x - 5\,x^2 - 6\,x^3 \quad \text{y} \quad q(x) = -2 + 8\,x^2.$$

Se pide:

a) Utilizar el algoritmo de Euclides en $\mathbb{Z}_7[x]$, para calcular un máximo común divisor, $d(x)$, de $p(x)$ y $q(x)$.

b) ¿Existe otro polinomio que sea máximo común divisor de $p(x)$ y $q(x)$ en $\mathbb{Z}_7[x]$? Razonar la respuesta.

c) Expresar $d(x)$ (obtenido en el apartado a), como combinación de $p(x)$ y $q(x)$ en $\mathbb{Z}_7[x]$ (Identidad de Bezout); esto es, calcular $\lambda(x)$ y $\mu(x)$ en $\mathbb{Z}_7[x]$ tales que $d(x) = \lambda(x)\,p(x) + \mu(x)\,q(x)$.

b) Si $\exists d'(x) \in \mathbb{Z}_7[x]$ t.q $d'(x) = (p(x), q(x)) \Rightarrow d'(x) \sim d(x)$ en $\mathbb{Z}_7[x]$

$d(x)$

$\Leftrightarrow \exists u \in \mathcal{U}(\mathbb{Z}_7[x])$ t.q $d'(x) = d(x) \cdot u$

$\mathcal{U}(\mathbb{Z}_7) = \mathbb{Z}_7 - \{\bar{0}\} = \{\bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}, \bar{6}\}$

$d_1(x) = d(x) \cdot 1 = 1(3x+5) = d(x)$

$d_2(x) = d(x) \cdot 2 = 2(3x+5) = 6x + 10 = 6x + 3$

$d_3(x) = d(x) \cdot 3 = 3(3x+5) = 9x + 15 = 2x + 1$

$d_4(x) = d(x) \cdot 4 = 4(3x+5) = 12x + 20 = 5x + 6$

$d_5(x) = d(x) \cdot 5 = 5(3x+5) = 15x + 25 = x + 4$

$d_6(x) = d(x) \cdot 6 = 6(3x+5) = 18x + 30 = 4x + 2$

Curso 2017-18. Convocatoria extraordinaria 2.

Dados los polinomios,

$$p(x) = 1 + 8x - 5x^2 - 6x^3 \quad \text{y} \quad q(x) = -2 + 8x^2.$$

Se pide:

a) Utilizar el algoritmo de Euclides en $\mathbb{Z}_7[x]$, para calcular un máximo común divisor, $d(x)$, de $p(x)$ y $q(x)$.

b) ¿Existe otro polinomio que sea máximo común divisor de $p(x)$ y $q(x)$ en $\mathbb{Z}_7[x]$? Razonar la respuesta.

c) Expresar $d(x)$ (obtenido en el apartado a), como combinación de $p(x)$ y $q(x)$ en $\mathbb{Z}_7[x]$ (Identidad de Bezout); esto es, calcular $\lambda(x)$ y $\mu(x)$ en $\mathbb{Z}_7[x]$ tales que $d(x) = \lambda(x)\,p(x) + \mu(x)\,q(x)$.

c) $\mathbb{Z}$: $d = (a,b) \Rightarrow \exists u, v \in \mathbb{Z}$ $d = au + bv$ (I. Bezout)

$\mathbb{Z}_7[x]$: $d(x) = (p(x), q(x)) \Rightarrow \exists \lambda(x), \mu(x) \in \mathbb{Z}_7[x]$ t.q.

$$d(x) = \lambda(x) \cdot p(x) + \mu(x) \cdot q(x)$$

Del Algoritmo de Euclides $p(x) = q(x) \cdot q_1(x) + r_1(x)$

$$d(x) = r_1(x) = p(x) - q(x) \cdot q_1(x) = 1 \cdot p(x) + (-q_1(x)) \cdot q(x)$$

Tomo $\lambda(x) = 1 \in \mathbb{Z}_7[x]$

$\mu(x) = -q_1(x) = -(x+2) = 6x + 5 \in \mathbb{Z}_7[x]$