Álgebra (Ingeniería Informática) **Curso 2007-2008**

Práctica 4: Anillos de polinomios y cuerpos finitos.

EJERCICIOS BÁSICOS

1. Estudiar si los siguientes polinomios son irreducibles:
   (a) $x^3 + x^2 + 3x + 2$ en $\mathbb{Z}_5[x]$.
   (b) $x^3 + 2x^2 + x + 1$ en $\mathbb{Z}_3[x]$.
   (c) $x^4 + x^2 + 1$ en $\mathbb{Z}_2[x]$.
2. Calcular el máximo común divisor de los siguientes pares de polinomios:
   (a) $f(x) = x^5 + 2x^4 + x^3 + 2x + 1, \quad g(x) = x^3 + x^2 + 2x + 2$ en $\mathbb{Q}[x]$.
   (b) $f(x) = x^5 + 2x^4 + x^3 + 2x^2 + 3x + 1, \quad g(x) = x^4 + 2x^3 + x^2 + 4x + 4$ en $\mathbb{Z}_5[x]$.
3. Resolver las siguientes ecuaciones diofánticas:
   (a) $(x^3 + x^2 + 2x + 2) \cdot f(x) + (x^2 + x + 1) \cdot g(x) = x^2 + 2$ en $\mathbb{Z}_3[x]$.
   (b) $(x^5 - 4x^4 + 9x^3 - 9x^2 + 8x - 5) \cdot f(x) + (x^4 + x^3 - 14x^2 + 41x - 35) \cdot g(x) = x^3 - 4x^2 + 8x - 5$ en $\mathbb{Q}[x]$.
4. Calcular los inversos de los siguientes polinomios en los cuerpos indicados:
   (a) $x^3 + 2x + 1$ en $\mathbb{Z}_3[x]/\langle x^4 + x + 2\rangle$.
   (b) $x^3 + 3x + 4$ en $\mathbb{Z}_5[x]/\langle x^4 + 3x^2 + 4\rangle$.
5. Encontrar todos los polinomios de grado 2 primos (irreducibles) en $\mathbb{Z}_5[x]$.
6. Describir los elementos del cuerpo $\mathbb{Z}_5[x]/\langle x^3 + 2x + 1\rangle$. ¿Cuál es su cardinal?
7. Construir un cuerpo finito con 8 elementos, dando las tablas de las operaciones de suma y producto.

EJERCICIOS DE REFUERZO

1. Estudiar si los siguientes polinomios son irreducibles:
   (a) $x^3 + 4x^2 + 2x + 1$ en $\mathbb{Z}_5[x]$.
   (b) $x^4 + x^3 + x + 1$ en $\mathbb{Z}_2[x]$.
   (c) $x^3 + x^2 + 2x + 2$ en $\mathbb{Z}_3[x]$.
2. Calcular el máximo común divisor de los siguientes pares de polinomios:
   (a) $f(x) = x^5 + x^3 + 2\,x^2 + x + 1, \quad g(x) = x^4 + x^3 + 2\,x^2 + 2\,x$ en $\mathbb{Z}_3[x]$.

(b) $f(x) = x^6 - 5\,x^4 - 2\,x^3 + 5\,x^5 + 11\,x^2 - 17\,x + 7, \quad g(x) = x^5 + 7\,x^4 + 7\,x^3 + x^2 + 14\,x$ en $\mathbb{Q}[x]$.

(c) $f(x) = x^6 + 4x^5 + 2x^3 - 5x^2 + 2x - 9, \quad g(x) = x^3 - 3x^2 + 7$ en $\mathbb{Z}_3[x]$.

(d) $f(x) = x^5 + 7x^4 + 16x^3 + 17x^2 + 13x + 6, \quad g(x) = x^4 + 7x^3 + 16x^2 + 14x + 4$ en $\mathbb{Q}[x]$.

3. Resolver las siguientes ecuaciones diofánticas:

(a) $(x^2 + 2\,x + 1) \cdot f(x) + (x^3 + 2\,x^2 + 1) \cdot g(x) = x^2$ en $\mathbb{Z}_3[x]$.

(b) $(x^3 - 4\,x^2 + 1) \cdot f(x) + (x^4 - x^2 + x) \cdot g(x) = 4\,x - 1$ en $\mathbb{Q}[x]$.

4. Calcular los inversos de los siguientes polinomios en los cuerpos indicados:

(a) $x^3 + x + 2$ en $\mathbb{Z}_3[x]\,/\langle x^4 + 2x + 2\rangle$.

(b) $x^2 + 2x + 4$ en $\mathbb{Z}_5[x]\,/\langle x^3 + x + 4\rangle$.

5. Encontrar todos los polinomios de grado 2 primos (irreducibles) en $\mathbb{Z}_5[x]$.

EJERCICIOS DE PROFUNDIZACIÓN

1. Construir un cuerpo finito con 27 elementos, dando las tablas de las operaciones de suma y producto.

2. Investigar la utilidad de los cuerpos finitos en criptografía. (**Indicación:** puedes comenzar buscando *finite field cryptography* o bien *GF(256) cryptography*).