TEMA 3

Cuerpos finitos.

Ejercicio 1. Calcula el cociente y el resto de dividir $2x^4 + 3x^3 + x^2 + 6x + 1$ entre $3x^2 + 1$ en $\mathbb{Z}_7[x]$ y en $\mathbb{Z}_{10}[x]$.

Ejercicio 2. Comprueba que $x^4 + 1$ es reducible en $\mathbb{Z}_p[x]$ para $p = 2, 3, 5, 7, 11, 13, 17$.

En general se tiene que $x^4 + 1$ es reducible en $\mathbb{Z}_p[x]$ para cualquier número primo.

- Si a es tal que $a^2 \equiv -1 \pmod{p}$ entonces $(x^2 + a)(x^2 - a)$ es una factorización de $x^4 + 1$ en $\mathbb{Z}_p[x]$.
- Si a es tal que $a^2 \equiv 2 \pmod{p}$ entonces $(x^2 + ax + 1)(x^2 - ax + 1)$ es una factorización de $x^4 + 1$ en $\mathbb{Z}_p[x]$.
- Si a es tal que $a^2 \equiv -2 \pmod{p}$ entonces $(x^2 + ax - 1)(x^2 - ax - 1)$ es una factorización de $x^4 + 1$ en $\mathbb{Z}_p[x]$.

Y se tiene que para cualquier primo p, hay en $\mathbb{Z}_p$ una raíz cuadrada de -1, de 2 o de -2.

Ejercicio 3. Sean $p(x) = x^4 + 2x^2 + 2x + 1$, y $q(x) = x^3 + 2x^2 + x + 2$ dos polinomios con coeficientes en $\mathbb{Z}_3$. Sean $r(x) = p(x) \bmod q(x)$ y $s(x) = q(x) \bmod r(x)$.

- Calcula todos los divisores de $p(x)$ (hay 8 en total, cuatro de ellos mónicos), de $q(x)$ (también hay 8) de $r(x)$ (en total 6) y $s(x)$ (hay 4).
- Calcula todos los divisores comunes de $p(x)$ y $q(x)$; de $q(x)$ y $r(x)$; y de $r(x)$ y $s(x)$.
- Calcula el mínimo común múltiplo de $p(x)$ y $q(x)$.

Ejercicio 4. Calcula un máximo común divisor de $a(x)$ y $b(x)$ en los siguientes casos:

1. $a(x) = x^4 + 2x^2 + 1, b(x) = x^4 - 1$ en $\mathbb{Z}_5[x]$.
2. $a(x) = x^4 + 2x^2 + 1, b(x) = x^2 + 2$ en $\mathbb{Z}_3[x]$.

Ejercicio 5. Calcula las raíces en $\mathbb{Z}_5$ del polinomio $x^2 + x + 4$.

Ejercicio 6. Calcula en $\mathbb{Z}_7[x]$ el resto de dividir

1. $x^7 + x^2 + 1$ entre $x - 1$,
2. $x^n + 1$ entre $x - 1$.

Ejercicio 7. Calcula en $\mathbb{Z}_5[x]$ el resto de dividir $x^n + 2$ entre $x + 4$.

Ejercicio 8. Calcula el resto de dividir el polinomio $x^{1321} + 5$ por el polinomio $x + 3$ en el anillo $\mathbb{Z}_7[x]$.

Ejercicio 9. Calcula el cociente y el resto de la división para las siguientes parejas de polinomios considerados en los anillos, $\mathbb{Z}_5[x]$ y $\mathbb{Z}_7[x]$.

1. $p(x) = x^4 - x^2 + 1$, $q(x) = 2x^2 + 1$.
2. $p(x) = x^5 - x^3 + 3x - 5$, $q(x) = x^2 + 5$.
3. $p(x) = x^8 + x^4 + 1$, $q(x) = x^2 - x + 1$.

4. $p(x) = x^5 - x^3 + 3x - 5$, $q(x) = x^2 + 7$.

Ejercicio 10. Encuentra todos los números primos p tales que $x^2 + 2$ sea un divisor de $x^5 - 10x + 12$ en $\mathbb{Z}_p[x]$.

Ejercicio 11. Halla un máximo común divisor y un mínimo común múltiplo en $\mathbb{Z}_3[x]$, $\mathbb{Z}_5[x]$ de las siguientes parejas de polinomios:

1. $p(x) = x^2 - 1$, $q(x) = x^3 - 3x^2 + 6x - 4$.
2. $p(x) = x^2 + 2x + 1$, $q(x) = x^3 + 7x^2 + 15x + 9$.
3. $p(x) = x^5 + 5x^4 + 4x^3 + 3x^2 + 2x - 1$, $q(x) = x^3 - 3x^2 + 2x - 1$.

Encuentra en cada caso polinomios $u(x)$ y $v(x)$ tales que

$$p(x) \cdot u(x) + q(x) \cdot v(x) = \mathrm{mcd}(p(x), q(x)).$$

Ejercicio 12. Encuentra todas las raíces de $x^2 - 1 \in \mathbb{Z}_8[x]$. Da dos factorizaciones distintas de $x^2 - 1$ como producto de polinomios mónicos.

Ejercicio 13. Comprueba que los polinomios $x^3 + x^2 + x + 1$ y $x^2 + 2x + 1$ determinan la misma aplicación $f : \mathbb{Z}_3 \to \mathbb{Z}_3$.

Ejercicio 14. El polinomio $x^4 - 1$ puede factorizarse en factores lineales en $\mathbb{Z}_5[x]$. Encuentra dicha factorización.

Ejercicio 15. Descompón como producto de irreducibles el polinomio $x^6 - 1$ en $\mathbb{Z}_3[x]$, $\mathbb{Z}_5[x]$ y $\mathbb{Z}_7[x]$.

Ejercicio 16. Sea $A = \mathbb{Z}_2[x]_{x^3+1}$.

1. Calcula las unidades de A, y da, en cada caso, su inverso. ¿Es la suma de dos unidades una unidad? ¿Y el producto?
2. Calcula los divisores de cero[1]. Para cada uno de ellos, encuentra un elemento no nulo de A que al multiplicarlo por él de cero. ¿Es la suma de dos divisores de cero un divisor de cero? ¿Y el producto?.

Ejercicio 17. Sea $A = \mathbb{Z}_5[x]_{x^3+3}$, y $\alpha = [x] \in A$.

- Comprueba que $3\alpha^2 + 3\alpha + 1$ y $2\alpha + 3$ son unidades y calcula sus inversos.
- Comprueba que $3\alpha^2 + 3$ y $4\alpha^3 + \alpha^2 + 3\alpha + 1$ son divisores de cero. Multiplícalos por un elemento no nulo de A para que de cero.

Ejercicio 18. ¿Cuántos elementos tiene $\mathbb{Z}_3[x]_{x^4+x^2+x+1}$? ¿Cuántos de ellos tienen inverso?

Ejercicio 19. Sean $K_1 = \mathbb{Z}_2[x]_{x^4+x+1}$ y $K_2 = \mathbb{Z}_2[x]_{x^4+x^3+x^2+x+1}$. Sean $\alpha = [x]$ y $\beta = [x]$, tomadas respectivamente en K_1 y K_2.

Calcula todas las potencias de α y β, y encuentra un isomorfismo $K_2 \to K_1$.

Ejercicio 20. Demuestra que $x^2 + 1$ es irreducible en $\mathbb{Z}_3[x]$ y que $x^3 + x + 1$ es irreducible en $\mathbb{Z}_2[x]$. Describe todos los elementos, y la aritmética de $\mathbb{Z}_3[x]_{x^2+1}$ y $\mathbb{Z}_2[x]_{x^3+x+1}$.

[1] Dado un anillo conmutativo A y un elemento $a \in A$ se dice que es un divisor de cero si existe $b \in A$, $b \neq 0$, tal que $a \cdot b = 0$

Preguntas test.

Ejercicio 21. ¿Cuál de los siguientes anillos es un cuerpo?

a) $\mathbb{Z}_7[x]$.

b) $\mathbb{Z}_5[x]_{x^2-1}$.

c) $\mathbb{Z}_2[x]_{x^2+1}$.

d) $\mathbb{Z}_3[x]_{x^2+1}$.

Ejercicio 22. ¿Cuál de los siguientes grupos de polinomios de $\mathbb{Z}_7[x]$ es múltiplo de x^2-1?

a) $x^{2n}+1$ para $n \geq 1$.

b) $x^{4n}+x^{2n}-2$ para $n \geq 1$.

c) $x^{2n}-x^n-1$ para $n \geq 1$.

d) $x^{2n}-2x^n+1$ para $n \geq 1$.

Ejercicio 23. Dados $p(x)=x^4+x^3+x^2+x$ y $q(x)=x^5+x^2+x+1$ dos polinomios con coeficientes en $\mathbb{Z}_2$, el máximo común divisor de $p(x)$ y $q(x)$ vale:

a) x^2+1.

b) x^2+x.

c) $x^4+x^3+x^2+x$.

d) 1.

Ejercicio 24. Sea $A=\mathbb{Z}_5[x]_{x^4+3x^3+3x^2+x+2}$, y sea $p(x)=x^2+1 \in A$. Entonces:

a) $p(x)$ no tiene inverso en A, pues $x^4+3x^3+3x^2+x+2$ tiene a $x=1$ como raíz.

b) $p(x)$ no tiene inverso en A, pues x^2+1 no es irreducible.

c) $p(x)$ tiene inverso en A y vale $2x^3+x^2+4x+1$.

d) $p(x)$ tiene inverso en A y vale x^3+x^2+4x+2.

Ejercicio 25. Determina cuál de los siguientes anillos es un cuerpo:

1. $\mathbb{Z}_3[x]_{x^2+1}$.
2. $\mathbb{Z}_5[x]_{x^2+1}$.
3. $\mathbb{Z}_{11}[x]_{x^2+1}$.
4. $\mathbb{Z}_{13}[x]_{x^2+1}$.

Ejercicio 26. Sea $A=\mathbb{Z}_2[x]_{x^4+x+1}$, y $p(x)=x^3+x^2+x+1 \in A$. Entonces:

a) $p(x)$ no tiene inverso, ya que no es irreducible.

b) $p(x)$ tiene inverso, y vale x^3+x+1.

c) $p(x)$ no tiene inverso, pues $p(1)=0$.

d) $p(x)$ tiene inverso y vale x^3.

Ejercicio 27. En el cuerpo $A = \mathbb{Z}_2[x]_{x^3+x+1}$ el elemento $x^2 + x + 1$ es igual a:

a) x^4.

b) x^5.

c) x^6.

d) x^7.

Ejercicio 28. Sea $p(x) = x^5 + x^4 + x^3 + 4x^2 + 3 \in \mathbb{Z}_5[x]$. Entonces $p(x)$ es igual a:

a) $(x+2)^2 \cdot (x+3) \cdot (x+4)^2$.

b) $(x+2)^2 \cdot (x+3)^2 \cdot (x+4)$.

c) $(x+2) \cdot (x+3)^2 \cdot (x+4)^2$.

d) $(x+2)^2 \cdot (x+3) \cdot (x+4)$.

Ejercicio 29. Sea el anillo $A = \mathbb{Z}_3[x]_{x^4+2x+1}$. Entonces:

a) A es un cuerpo con 3^4 elementos.

b) A es un anillo con 4^3 elementos que no es un cuerpo y en el que el inverso de $[x^2 + x + 1]$ vale $[x^2 + 2x]$.

c) A es un cuerpo en el que el inverso de $[x]$ es $[2x^3 + 1]$.

d) A no es un cuerpo, pero el elemento $[x^2 + x + 1]$ tiene inverso y vale $[2x^2 + x]$.