Matemáticas Avanzadas (Grado en Ingeniería de Computadores) **Curso 2021-2022**

Práctica 6

EJERCICIOS BÁSICOS

`SAGE` 1. Escribe todos los elementos de $\mathbb{Z}_3[x]$ módulo $x^2 + 2x + 2$, que se suele escribir como $\mathbb{Z}_3[x] / \langle x^2 + 2x + 2 \rangle$.
Luego ejecuta `R = Integers(3)` para definir $\mathbb{Z}_3$ y `R.<x> = PolynomialRing(R)` para definir $\mathbb{Z}_3[x]$, y utiliza el comando `f.quo_rem(g)` para decidir a cuál de ellos es congruente el polinomio $x^8 + 2x^6 + x^5 + x^4 + 2x^3 + 2x^2 + x + 1$.
(Este comando te devuelve, en ese orden, el cociente y el resto de dividir `f` entre `g`).

`SAGE` 2. Ejecuta `R.<x>=QQ[]` para definir $\mathbb{Q}[x]$. Define los polinomios

$$f = 64x^6 - 608/5x^5 + 2264/15x^4 - 328/3x^3 + 788/15x^2 - 40/3x,$$

$$g = 160/3x^5 - 112/3x^4 + 836/15x^3 - 332/15x^2 + 20x$$

y sigue los pasos del algoritmo de Euclides, utilizando el comando `f.quo_rem(g)`, para calcular $\mathrm{mcd}(f, g)$. Comprueba tu resultado usando el comando `f.gcd(g)`.

`SAGE` 3. Ejecuta `R = Integers(7)` para definir $\mathbb{Z}_7$ y `R.<x> = PolynomialRing(R)` para definir $\mathbb{Z}_7[x]$. Define el equivalente a los polinomios del ejercicio anterior pero ahora en $\mathbb{Z}_7[x]$, que serían

$$f = 64x^6 - 608 \cdot 5^{-1}x^5 + 2264 \cdot 15^{-1}x^4 - 328 \cdot 3^{-1}x^3 + 788 \cdot 15^{-1}x^2 - 40 \cdot 3^{-1}x,$$

$$g = 160 \cdot 3^{-1}x^5 - 112 \cdot 3^{-1}x^4 + 836 \cdot 15^{-1}x^3 - 332 \cdot 15^{-1}x^2 + 20x$$

donde lo que antes era la fracción $\frac{a}{b}$ en $\mathbb{Q}$ ahora es el producto $a \cdot b^{-1}$ en $\mathbb{Z}_7$ (que en `SAGE` puede ponerse como `Mod(a*b^(-1),7)`).

Sigue los pasos del algoritmo de Euclides, utilizando el comando `f.quo_rem(g)`, para calcular $\mathrm{mcd}(f, g)$. Comprueba tu resultado usando el comando `f.gcd(g)`. Compara los resultados con los del ejercicio anterior.

`SAGE` 4. En $\mathbb{Q}[x]$, como en el ejercicio 2, factoriza el polinomio f de ese ejercicio con el comando `f.factor()` y haz lo mismo con el polinomio g. Después repite lo mismo en $\mathbb{Z}_7[x]$, con los polinomios correspondientes como en el ejercicio 3, y compara los resultados.

- Los ejercicios básicos son obligatorios y determinarán la calificación de las actividades semanales.
- Los ejercicios de refuerzo se proponen para adquirir mayor destreza.
- Los ejercicios de profundización se proponen para quienes tengan curiosidad.

EJERCICIOS DE REFUERZO

`SAGE` 1. Escribe todos los elementos de $\mathbb{Z}_3[x]$ módulo x^2+2x+1 (que se denota $\mathbb{Z}_3[x]\,/\langle x^2+2x+1\rangle$). Luego ejecuta `R = Integers(3)` para definir $\mathbb{Z}_3$ y `R.<x> = PolynomialRing(R)` para definir $\mathbb{Z}_3[x]$ y utiliza el comando `f.quo_rem(g)` para decidir a cuál de ellos es congruente el polinomio $x^7+2x^6+x^5+x^4+2x^3+2x^2+x+1$.

`SAGE` 2. Escribe todos los elementos de $\mathbb{Z}_5[x]$ módulo x^4+2x+2 (que se denota $\mathbb{Z}_5[x]\,/\langle x^4+2x+2\rangle$). Luego ejecuta `R = Integers(5)` para definir $\mathbb{Z}_5$ y `R.<x> = PolynomialRing(R)` para definir $\mathbb{Z}_5[x]$ y utiliza el comando `f.quo_rem(g)` para decidir a cuál de ellos es congruente el polinomio $x^7+3x^6+4x^5+2x^4+x^3+3x^2+4x+2$.

`SAGE` 3. Ejecuta `R.<x>=QQ[]` para definir $\mathbb{Q}[x]$. Define los polinomios

$$f = x^5+2x^4+x^3+2x^2+3x+1,$$

$$g = x^4+2x^3+x^2+4x+4$$

y sigue los pasos del algoritmo de Euclides, utilizando el comando `f.quo_rem(g)`, para calcular $\mathrm{mcd}(f,g)$. Comprueba tu resultado usando el comando `f.gcd(g)`.

`SAGE` 4. Ejecuta `R = Integers(7)` para definir $\mathbb{Z}_7$ y `R.<x> = PolynomialRing(R)` para definir $\mathbb{Z}_7[x]$. A continuación, haz lo mismo que en el ejercicio anterior. **Nota:** al definir los polinomios puedes usar el comando `a*Mod(b^(-1),7)` para sustituir en $\mathbb{Z}_7$ a la fracción $\frac{a}{b}$ de $\mathbb{Q}$.

`SAGE` 5. En $\mathbb{Q}[x]$, factoriza el polinomio f con el comando `f.factor()` y haz lo mismo con el polinomio g. Después, repite el ejercicio en $\mathbb{Z}_7[x]$.

`SAGE` 6. Calcula 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 $\mathbb{Z}_5[x]$.

EJERCICIOS DE PROFUNDIZACIÓN

1. Estudia 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. Resuelve las siguientes ecuaciones de tipo diofántico:
   (a) $(x^3 + x^2 + 2x + 2) \cdot f(x) + (x^2 + x + 1) \cdot g(x) = x^2 + 2 \quad$ 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 $\mathbb{Q}[x]$.
3. Calcula 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 $\mathbb{Z}_5[x] / \langle x^4 + 3x^2 + 4\rangle$.
4. Encuentra todos los polinomios de grado 2 primos (irreducibles) en $\mathbb{Z}_5[x]$.
5. Construye un cuerpo finito con 4 elementos, dando las tablas de las operaciones de suma y producto. Comprueba que existe un elemento a tal que el cuerpo está formado por los elementos $\{0, a^0, a, a^2\}$.
6. Construye un cuerpo finito con 8 elementos, dando las tablas de las operaciones de suma y producto.
7. Investiga el uso de cuerpos finitos en criptografía y codificación.

`SAGE` 1. Implementa una función que resuelva ecuaciones de tipo diofántico para polinomios.