CONJUNTOS Y NÚMEROS. Curso 2012-2013. **HOJA 6.**

1) Hallar el cociente $C(X)$ y el resto $R(X)$ que resultan de dividir el polinomio
$$P(X) = 3X^5 + 2X^3 + X + 1 \quad \text{por el} \quad Q(X) = 3X^2 + 1.$$
Hacer primero esa división en $\mathbb{Q}[X]$, y luego en $\mathbb{Z}_5[X]$.

2) Sean P, $Q \in \mathbb{Q}[X]$. Probar que P y Q son *coprimos* si y sólo si $P + Q$, $P \cdot Q$ también lo son.

3) Calcular el máximo común divisor $D(x)$ de los polinomios
$$P(X) = X^5 - 5X^3 + 4X, \quad Q(X) = X^3 - 2X^2 - 5X + 6.$$
Encontrar dos polinomios $A(X)$ y $B(X)$ tales que $A(X) \cdot P(X) + B(X) \cdot Q(X) = D(X)$.

4) Encontrar polinomios $A(X)$ y $B(X)$ tales que $A(X)(X^2 + 2X - 2) + B(X)(X^2 + X - 1) = 1$.

5) Hallar un polinomio $P(X) \in \mathbb{Q}[X]$ tal que $X^2 + 1$ divida a $P(X)$, y $X^3 + 1$ divida a $P(X) - 1$, siendo el grado de P el mínimo posible.

6) (a) Hallar un polinomio $P(X)$, del mínimo grado posible, que cumpla las siguientes condiciones:
$$P(X + 1) - P(X) = X\,, \quad P(0) = 1.$$
(b) Para cada $Q(X) \in \mathbb{R}[X]$, probar por inducción sobre $n = \mathit{grado}(Q)$, que algún $P(X)$ de grado $n + 1$ cumple:
$$Q(X) = P(X + 1) - P(X).$$
Indicación: los coeficientes de Q son **función lineal** *de los de P, y sólo es $Q = 0$ si $gr(P) = 0$.*

(c) ¿Qué relación tiene esto con las sumas $\sum_{k=0}^{n} Q(k)$ de los valores del polinomio $Q(X)$? ¿Qué cambia si usamos cualquier $a \in \mathbb{Q}$ en la condición $P(X + a) - P(x)$, en lugar del 1?

7) Hallar todos los polinomios $P(X)$ de grado tres que cumplan: $P(0) = P(1) = P(2) = 1$.
Lo mismo si pedimos $P(0) = b_0$, $P(1) = b_1$, $P(2) = b_2$, para constantes dadas b_i.

8) Hallar el cociente y resto de dividir $P(X) = X^4 + 7X^3 + 9X^2 - 27X - 54$ por $(x + 3)^3$, y deducir cuáles son todos sus ceros, con sus multiplicidades. Razonar y comprobar lo que esos ceros implican para su derivada $P'(X)$ y para el máximo común divisor de $P(X)$ y $P'(X)$.

9) Demostrar que cada uno de los números $a = 2 + \sqrt[3]{3}$, $\sqrt{2} + \sqrt{3}$, $\sqrt[3]{2} + \sqrt{3}$ es un cero de algún polinomio de $\mathbb{Z}[X]$. Hallar esos polinomios.
Indicación: sus potencias a^k son combinaciones lineales con coeficientes en $\mathbb{Q}$ de unos pocos irracionales.

10) (a) Demostrar que para cualquier cuerpo $\mathbb{K}$, existen infinitos polinomios irreducibles en $\mathbb{K}[X]$.
Sugerencia: reconstruir la prueba de Euclides de que hay en $\mathbb{Z}$ infinitos números primos.

(b) Deducir que si $\mathbb{K}$ es un cuerpo con un número finito de elementos (por ejemplo $\mathbb{K} = \mathbb{Z}_p$ para p primo) habrá en $\mathbb{K}[X]$ polinomios irreducibles de grado arbitrariamente grande.

(c) Ejemplo: hallar los polinomios mónicos irreducibles en $\mathbb{Z}_2[X]$ de grados $1, 2, 3$ y 4.

11) (a) Para un producto de polinomios $(a_0 + \cdots + a_k X^k)(b_0 + \cdots + b_j X^j) = c_0 + \cdots + c_n X^n$, con coeficientes $\in \mathbb{Z}$ y grados $j, k < n$, probar por inducción que

si para un primo dado $p \in \mathbb{N}$, $p \nmid b_0$, pero $\forall i \leq k$, $p \mid c_i$, entonces $\forall i$ se tiene $p \mid a_i$.

(b) Deducir de (a) el ***criterio de irreducibilidad de Eisenstein:***
Si para algún primo p se tiene $p \mid c_i$ *para* $i < n$, $p \nmid c_n$, $p^2 \nmid c_0$,
entonces el polinomio $c_0 + \cdots + c_n X^n \in \mathbb{Z}[X]$ *es irreducible en* $\mathbb{Q}[X]$.

(c) Deducir que $\forall\, n > 1$ existen infinitos polinomios de grado n que son irreducibles en $\mathbb{Q}[X]$.

(d) Un ejemplo: descomponer $P(X) = X^5 - X^4 + 2X^3 - 2$ en factores irreducibles en $\mathbb{Q}[X]$.

12) ¿Es reducible en $\mathbb{Q}[X]$ el polinomio $p(X) = X^4 - 2X^3 + 2X - 3$? Justificar la respuesta. ¿Será reducible en $\mathbb{R}[X]$? Aquí puede ayudar el observar los ceros de su derivada $p'(X)$ y lo que eso implica sobre los ceros reales de $p(X)$. Ver por fin lo que ocurre con el polinomio $p(X)+2$.

13) Descomponer el polinomio $p(X) = X^4+3X^2+4$ en sus factores irreducibles en $\mathbb{Q}[X]$, $\mathbb{R}[X]$, $\mathbb{C}[X]$ y en $\mathbb{Z}_p[X]$, para $p = 2, 3, 5$ y 7.

14) (a) Probar que un polinomio $P(X) \in \mathbb{K}[X]$ es irreducible si y solamente si es irreducible el polinomio $Q(X) = P(X + a)$ para cualquier $a \in \mathbb{K}$.

(b) Probar que $P(X) = 1 + X + \cdots + X^{p-1}$ es irreducible sobre $\mathbb{Q}$ para cualquier primo p.

Indicación: aplicar el criterio de Eisenstein al $P(X + 1)$, recordando lo que es $P(X)(X - 1)$.

(c) Probar que si $n > 1$ no es primo, entonces $1 + X + X^2 + \cdots + X^{n-1}$ es reducible sobre $\mathbb{Q}$.

Indicación: Encontrar un factor de $X^n - 1$ de la forma $X^m - 1$ con $m > 1$.

15) Estudiar la reducibilidad sobre $\mathbb{Q}$ de los polinomios: $1 + X + X^4$ y $1 - X + X^4$.