CONJUNTOS Y NÚMEROS. Curso 2011-2012.
HOJA DE REPASO

1. Calcular los últimos dos dígitos de 2012^{2012}.
   Indicación: Calcular primero el resto de dividir este número entre 25.

2. Demostrar que, dados $a, b, c \in \mathbb{Z}$, donde a y b son primos con n, la ecuación $ax+by = c$ tiene exactamente n soluciones $(x, y) \in \mathbb{Z}_n^2$.

3. Hallar el conjunto de soluciones de cada uno de los siguientes sistemas en $\mathbb{Z}_{10}$.

$$\left.\begin{aligned} x + y &= 5 \\ 2x + 9y &= 1 \end{aligned}\right\} \qquad \left.\begin{aligned} 2x + 4y &= 6 \\ x + y &= 4 \end{aligned}\right\} \qquad \left.\begin{aligned} x + 3y &= 1 \\ 3x - y &= 3 \end{aligned}\right\}$$

4. Calcular: a) $234^{432} \pmod{11}$; b) $145^{197} \pmod{13}$; c) $2025^{2025} \pmod{14}$.

5. Sea (a, b, c) una terna pitagórica, esto es, una solución en $\mathbb{Z}^3$ de la ecuación $X^2 + Y^2 = Z^2$.
   Demostrar lo siguiente:

   i) al menos uno de los valores a, b o c es múltiplo de 3;
   ii) abc es múltiplo de 4;
   iii) al menos uno de los valores a, b o c es múltiplo de 5;
   iv) $abc \equiv 0 \pmod{60}$.

   Indicación: Estudiar qué números son cuadrados en $\mathbb{Z}_3$, $\mathbb{Z}_4$ y $\mathbb{Z}_5$.

6. Demostrar que $n(n^5 - 1)(n^5 + 1)$ es divisible por 22 para todo $n \in \mathbb{Z}$.

7. Hallar todas las soluciones de los siguientes sistemas de congruencias:

$$\left.\begin{aligned} x &\equiv 13 \pmod{91} \\ x &\equiv -1 \pmod{119} \end{aligned}\right\} \qquad \left.\begin{aligned} x &\equiv -5 \pmod{77} \\ x &\equiv 17 \pmod{143} \end{aligned}\right\}$$

8. ¿Cuántas unidades hay en $\mathbb{Z}_{2310}$? ¿y en $\mathbb{Z}_{1764}$?

9. Verificar que si $z, w \in \mathbb{C}$ entonces $|z + w|^2 + |z - w|^2 = 2\big(|z|^2 + |w|^2\big)$. Explicar el significado geométrico de esa igualdad, dibujando un par de puntos z, w en el plano complejo.

10. Descomponer los siguientes polinomios en factores irreducibles en $\mathbb{Q}[X]$, $\mathbb{R}[X]$, $\mathbb{C}[X]$ y $\mathbb{Z}_2[X]$:
    $15X^2 - 19X - 8$, $X^2 + 6X + 25$, $X^3 + 6X^2 + 6X - 8$, $5X^3 + 9X^2 + 13X - 3$, $3X^3 + 2X^2 - 4X + 1$.
    Indicación: Son todos de grado menor o igual que 3.

11. Calcular el máximo común divisor $\Delta(X)$ de los polinomios
$$P(X) = 2X^3 - 7X^2 + 10X - 6,\ Q(X) = X^4 + 4.$$
    Encontrar dos polinomios $A(X)$ y $B(X)$ tales que $A(X)P(X) + B(X)Q(X) = \Delta(X)$.

12. Se consideran polinomios $P \in \mathbb{R}[X]$ de grado 5 tales que el máximo común divisor de $P(X)$ y $P(X + 1)$ es de grado 4.

    a) Dar un ejemplo de polinomio que cumpla esta condición.
    Indicación: Observar la relación que hay entre los ceros de $P(X)$ y los de $P(X + 1)$.
    b) Demostrar que si $P, Q \in \mathbb{R}[X]$ son ambos de este tipo, entonces existen constantes $a, b \in \mathbb{R}$ tales que $Q(X) = aP(X + b)$.

13. Para dos subconjuntos A, B de $\mathbb{Z}$ cualesquiera, se suelen definir su suma y su producto de la siguiente forma:
$$A + B = \{a + b : \quad a \in A,\ b \in B\}, \qquad A \cdot B = \{a \cdot b : \quad a \in A,\ b \in B\}.$$
Sea $n \in \mathbb{Z}_+$ y tomemos como A, B dos clases mod n :
$$A = \bar{a} = \{j : \quad j \equiv a \bmod n\}, \qquad B = \bar{b} = \{k : \quad k \equiv b \bmod n\}$$
Comprobar si la definición de arriba da el mismo resultado que la definición de la suma y el producto de clases módulo n. Es decir, si los $A+B$, $A \cdot B$ de arriba coinciden con las clases $\overline{a+b}$, $\overline{a \cdot b}$ respectivamente.

Si alguna de estas igualdades no es cierta, estudiar si es cierta la inclusión en alguno de los dos sentidos.

14. Sean $m, n \in \mathbb{Z}_+$ dos números primos entre sí. Escribimos $r = \exp(2\pi i/m)$, $s = \exp(2\pi i/n)$.
   i) Recordemos que $1, r, r^2, \ldots, r^{(m-1)}$ son todas las raíces m-ésimas de 1. Demostrar que los números $1, r^n, r^{2n}, \ldots, r^{(m-1)n}$ también son *todas las raíces m-ésimas de* 1 (escritas en otro orden);
   ii) Demostrar que $\prod_{j=0}^{m-1} \prod_{k=0}^{n-1} \left(r^j + s^k\right)$ es igual a 2 o a 0, dependiendo de los valores de n y m. Decidir en qué casos vale 0 y en qué casos vale 2.
   Indicación: Comprobar primero la fórmula $\prod_{k=0}^{n-1}(z + s^k) = z^n - (-1)^n$. Utilizar esta igualdad y el apartado (i).

15. Sea $\mathcal{F}$ el conjunto de funciones de $\mathbb{N} \setminus \{0\}$ a $\mathbb{N} \setminus \{0\}$. Se define la siguiente relación en $\mathcal{F}$:
$$f\mathcal{R}g \iff \text{Para todo } n \in \mathbb{N} \setminus \{0\}, \text{ existe } N \in \mathbb{N},\ N \geq 1 \text{ tal que } g(n) = Nf(n).$$
   a) Demostrar que es una relación de orden.
   b) ¿Se trata de un orden total? ¿Con qué funciones está relacionada la función identidad $f(n) = n$? ¿Y la función constante $f(n) = 3$?
   c) ¿Existen elementos minimales? ¿Y elementos maximales?

16. Sea X el conjunto de listas formadas por reordenaciones de $1, 2, 3$. Por ejemplo, $[1, 2, 3] \in X$, $[3, 1, 2] \in X$, etc. Decimos que $[a, b, c]\ \mathcal{R}\ [d, e, f]$ si $F(x_a, x_b, x_c) = F(x_d, x_e, x_f)$ donde F es la función
$$F(x, y, z) = (x - y)(z - x)(y - z).$$
Demostrar que $\mathcal{R}$ define una relación de equivalencia en X y hallar el número de clases de equivalencia.

17. Se considera el subconjunto A del cuerpo $\mathbb{C}$, que consiste de todas las sumas finitas de la forma $\sum_k a_k\, e^{\pi i r_k}$ donde $a_k \in \mathbb{Z}$, $r_k \in \mathbb{Q}$.
   a) Demostrar que A es un anillo.
   b) Demostrar que $\sqrt{2}, \sqrt{3} \in A$.
   c) Calcular los cardinales de los siguientes conjuntos: A, $A[X]$, $\mathbb{C} \setminus A$. Decidir si son anillos (respecto de la operaciones usuales de la suma y el producto en $\mathbb{C}$).

18. Suponer dada en un conjunto A una relación $x\mathcal{R}y$ que tiene las propiedades *reflexiva* y *transitiva*, pero que *ni es simétrica, ni anti-simétrica.* Probar las siguientes afirmaciones:

(a) la relación $\mathcal{E}$ definida por: $x\mathcal{E}y \iff x\mathcal{R}y \wedge y\mathcal{R}x$, es de equivalencia;

(b) en el conjunto cociente $A/\mathcal{E}$, la relación $\mathcal{S}$ definida por: $\bar{x}\mathcal{S}\bar{y} \iff x\mathcal{R}y$, es de orden;

(c) en el anillo de polinomios $\mathbb{K}[X]$, la relación: $Q(X)$ ***divide a*** $P(x)$ tiene las propiedades postuladas para $\mathcal{R}$, y en cada clase $\bar{P} \in \mathbb{K}[X]/\mathcal{E}$, con $P \neq 0$, de la relación definida en (a), hay exactamente un *polinomio mónico*, si $\mathbb{K}$ es un cuerpo.

19. Llamemos $p_d(n)$ al número de puntos $(k_1, \ldots, k_d) \in \mathbb{N}^d$ cuyas coordenadas cumplen: $\sum_j k_j = n$.

(a) Probar que: $\quad p_{d+1}(n) = \sum_{k=0}^{n} p_d(k)$. *Sugerencia:* k_{d+1} *tomará algún valor* $\in [0, n]$.

(b) Por inducción sobre d, probar que $p_d(n)$ es un polinomio en n, con $p_d(0) = 1$ y grado $= d - 1$. Deducir fórmulas para cada $p_d(x)$, con $d \leq 4$.

Feliz Navidad