APELLIDOS NOMBRE

Observaciones:

-) Escribir el nombre y los apellidos en esta hoja, que deberá entregarse con el examen.
-) Escribir la respuesta a cada ejercicio en hojas separadas. Entregar al final las hojas ordenadas por ejercicios.
-) Durante la realización del examen exclusivamente se podrá disponer de material de escritura. Ningún otro objeto está permitido.
-) El examen se puntuará sobre 20 puntos y cada uno de los ejercicios sobre 10 puntos. Para superar este examen, habrá que alcanzar un mínimo de 3 puntos sobre 10 en cada uno de los ejercicios realizados.

Ejercicio 1. (10 puntos)

(a) (2,5 puntos) Sea $N > 1$ un número natural cualquiera, que consideraremos fijo. Resolver el siguiente sistema de congruencias, justificando primero por qué ha de tener solución:

$$\begin{aligned} x &\equiv 1 \pmod{N} \\ x &\equiv 2 \pmod{N^2-1}. \end{aligned}$$

(b) (2,5 puntos)
(i) Calcular los últimos dos dígitos de 49^{19}.
(ii) Calcular: $1 \times 10 + 2 \times 10^2 + 3 \times 10^3 + ... + 2018 \times 10^{2018} \pmod{11}$.

(c) (2,5 puntos) Sean $m \neq 0, 1$ y a unos enteros. Probar que las dos propiedades siguientes son equivalentes:
(i) $a + \mathbb{Z}m$ es una unidad en $\mathbb{Z}/\mathbb{Z}m$.
(ii) $\text{mcd}(a, m) = 1$.

(d) (2,5 puntos) Sea $p > 2$ un primo. Demostrar que cada divisor primo de $2^p - 1$ es $\equiv 1$ módulo p (y por tanto $> p$). Indicación: se puede seguir el siguiente esquema. Sea q un primo que divide a $2^p - 1$.
-) Observa y justifica que: $2^p \equiv 1 \pmod{q}$. ¿Cuál sería el orden de la clase de 2 en el grupo de las unidades de $\mathbb{Z}/\mathbb{Z}q$?
-) Prueba que: $2^{q-1} \equiv 1 \pmod{q}$. ¿Qué relación puedes deducir entre p y $q - 1$?

Ejercicio 2. (10 puntos)

A. (5 puntos) Sean $f(x) = x^6 - 4x^4 - 3x^3 + 2x^2 + 6x + 4$ y $g(x) = x^4 - x^2 - 2$ dos polinomios con coeficientes enteros. Se pide:
(1) Calcular $\text{mcd}(f(x), g(x))$ y una identidad de Bézout (en $\mathbb{Q}[x]$) para estos polinomios.
(2) Descomponer $f(x)$ en factores irreducibles en $\mathbb{Q}[x]$, $\mathbb{R}[x]$ y $\mathbb{C}[x]$.

B. (5 puntos)
(1) Sean en este caso $f(x) = x^3 + 1 \in \mathbb{F}_2[x]$ e $I = \langle f(x) \rangle$. ¿Es $A = \mathbb{F}_2[x]/I$ un cuerpo? Dar la lista de las unidades de A. Calcular, si existe, el inverso de la clase del polinomio x en A.
(2) Sean k un cuerpo, $f(x) \in k[x]$ un polinomio e $I = \langle f(x) \rangle$ el ideal generado por $f(x)$. Probar que $g(x) + I$ es una unidad en $A = k[x]/I$ si y sólo si $\text{mcd}(g(x), f(x)) = 1$. (Indicación: La prueba es análoga al caso de $\mathbb{Z}$).