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) Calcular: $1 \times 10 + 2 \times 10^2 + 3 \times 10^3 + ... + 2018 \times 10^{2018} \pmod{11}$.

(b) 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 $q - 1$?

(c) Determinar si la siguiente matriz es singular o no singular:

$$\begin{bmatrix} 54401 & 65432 & 45530 & 45678 \\ 34567 & 12121 & 11111 & 12345 \\ 12345 & 76543 & 98760 & 65456 \\ 43211 & 45678 & 88888 & 98765 \end{bmatrix}.$$

(Indicación: trabajar en algún $\mathbb{Z}/\mathbb{Z}m$)

(d) Demostrar que la sucesión $11, 111, 1111, ...$ no contiene ningún cuadrado (de un entero, claro está). (Indicación: considerar los restos módulo 100 y después pensar un poco más...)

(e) Probar que el único entero n para el que existen enteros a y b con $n = a^3(3a+1)$ y $n = b^2(b+1)^3$ y $\mathrm{mcd}(a, b) = 1$ es 2000.

Ejercicio 2. (a) Dar un ejemplo de un polinomio mónico $f(x) \in \mathbb{Z}[x]$ de grado 3 que sea irreducible en $\mathbb{Q}[x]$ (y por tanto en $\mathbb{Z}[x]$) y cuyas reducciones módulo 3 y módulo 5, respectivamente en $\mathbb{F}_3[x]$ y en $\mathbb{F}_5[x]$, no sean irreducibles. ¿Podrías contestar a esta misma pregunta si el grado fuera distinto de 3? ¿Y si en lugar de 3 y 5 considerásemos otros primos p y q arbitrarios? ¿Y si en lugar de considerar sólo las reducciones módulo dos primos las considerásemos módulo un número finito de primos $p_1, \ldots, p_r$?

(b) Sea $n \geq 1$ un entero y $P_n(x) = 1 + x + x^2 + ... + x^n$. Determinar para qué valores de n se tiene que $P_n(x)$ divide $P_n(x^2)$. [Indicación: analizar cuándo $1 + x$ divide a $1 + x^n$]

(c) Dar justificadamente un ejemplo de un cuerpo con 16 elementos.