APELLIDOS NOMBRE

Instrucciones. Escribir la respuesta a cada cuestión en hojas separadas. Entregar al final las hojas ordenadas por cuestiones. Durante la realización del examen exclusivamente se podrá disponer de material de escritura. Ningún otro objeto está permitido. El examen se puntuará sobre 30 puntos y cada uno de los ejercicios sobre 10 puntos.

Ejercicio 1 (10 puntos).

1) Definir subgrupo normal de un grupo G. Definir homomorfismo de grupos.
2) Sean $f\colon G \to H$ un homorfismo de grupos y $S \subset H$ un subgrupo normal. Probar que $f^{-1}(S)$ es un subgrupo normal de G.
3) Enunciar la factorización canónica de un homomorfismo de grupos.
4) Sea $f\colon G \to H$ un homorfismo de grupos finitos, probar que $|\operatorname{Im}(f)|$ divide a $|G|$.

Solución.

1) Dado un grupo $(G, \star)$ y un subgrupo $K \subset G$, decimos que K es **normal** en G si para todo $x \in G$ se tiene que
$$x^{-1}Kx \subset K.$$
Dados dos grupos $(G, \star)$ y $(H, *)$, un **homomorfismo de grupos**
$$f\colon (G, \star) \to (H, *)$$
es una aplicación $f\colon G \to H$ que satisface que para cada $x_1, x_2 \in G$,
$$f(x_1 \star x_2) = f(x_1) * f(x_2).$$

2) Sea S un subgrupo normal de H. Sabemos entonces que es subgrupo y que $y^{-1}Sy \subset S$ para todo $y \in H$.
Veamos primero que $f^{-1}(S)$ es subgrupo:
-) Es claro que $f^{-1}(S) \neq \emptyset$, pues el elemento neutro de H, e_H, está en S y $f(e_G) = e_H$. Luego $e_G \in f^{-1}(S)$.
-) Sean $a, b \in f^{-1}(S)$, ¿$ab^{-1} \in f^{-1}(S)$? En efecto $f(ab^{-1}) = f(a)f(b)^{-1} \in S$ porque $f(a), f(b) \in S$. Luego $ab^{-1} \in f^{-1}(S)$.
Ahora probemos que $f^{-1}(S)$ es normal. Es decir, que $x^{-1}f^{-1}(S)x \subset f^{-1}(S)$ para todo $x \in G$. Sea $a \in f^{-1}(S)$ (es decir, $f(a) \in S$. ¿Es $x^{-1}ax \in f^{-1}(S)$?
Tenemos que $f(x^{-1}ax) = f(x)^{-1}f(a)f(x)$. Además $f(x) \in H$ y $f(a) \in S$. Por ser $S \subset H$ normal, se tiene que $f(x)^{-1}f(a)f(x) \in S$. Es decir, $x^{-1}ax \in f^{-1}(S)$ como queríamos.

3) Factorización canónica: Todo homomorfismo $f\colon (G, \star) \to (H, *)$ factoriza como la composición $f = i \circ \bar{f} \circ p$ de un epimorfismo p, un isomorfismo $\bar{f}$ y un monomorfismo i del siguiente modo
$$\begin{array}{ccc} (G, \star) & \xrightarrow{\quad f \quad} & (H, *) \\ {\scriptstyle p}\downarrow & & \uparrow{\scriptstyle i} \\ (G/\ker(f), \bar{\star}) & \xrightarrow[\bar{f}]{\cong} & (\operatorname{Im}(f), *) \end{array}$$
Aquí p es la proyección natural sobre el cociente e i es la inclusión del subgrupo imagen.

4) Por la factorización canónica sabemos que

$$\frac{G}{\ker(f)} \cong \mathrm{Im}(f),$$

luego

$$\left|\frac{G}{\ker(f)}\right| = |\,\mathrm{Im}(f)|.$$

Además

$$\left|\frac{G}{\ker(f)}\right| = \frac{|G|}{|\ker(f)|},$$

de donde $|G| = |\ker(f)| \cdot |\,\mathrm{Im}(f)|$. Es decir, $|\,\mathrm{Im}(f)|$ divide a $|G|$.

Ejercicio 2 (10 puntos).

1) Probar que un número entero es divisible por 3 si y sólo si la suma de sus cifras es múltiplo de 3. (Indicación: $10 \equiv 1(\text{mód}\,3)$).
2) Un niño quiere recordar cuánto dinero tiene en una hucha. Lo contó ayer y solo recuerda que la cantidad es múltiplo de 13 y que si lo hubiera cambiado por monedas de 2€ o por billetes de 5€ le habría sobrado un euro. También recuerda que tiene más de 300€ y menos de 400€. ¿Cuánto dinero tiene en la hucha?
3) Probar que un entero a tiene inverso multiplicativo módulo un entero b si y sólo si $\mathrm{mcd}(a,b) = 1$.
4) Calcular, si es posible, el inverso multiplicativo de 121^{301} módulo 250.

Solución.

1) La clave está en probar que si $m = a_r 10^r + \cdots a_1 10 + a_0$ es un número de $r+1$ cifras $a_r, \ldots, a_1, a_0$ entonces $m \equiv a_r + \cdots a_1 + a_0(\text{mód}\,3)$.
Y esto es evidente, pues $10 \equiv 1(\text{mód}\,3)$):

$$m = a_r 10^r + \cdots a_1 10 + a_0 \equiv a_r + \cdots a_1 + a_0(\text{mód}\,3).$$

Luego

$$3|m \Leftrightarrow m = a_r 10^r + \cdots a_1 10 + a_0 \equiv 0(\text{mód}\,3) \Leftrightarrow$$
$$\Leftrightarrow a_r + \cdots a_1 + a_0 \equiv 0(\text{mód}\,3) \Leftrightarrow 3|a_r + \cdots a_1 + a_0.$$

2) Siguiendo el enunciado, si x es la cantidad de dinero de la hucha, obtenemos el siguiente sistema de ecuaciones en congruencias:

$$\begin{cases} x \equiv 0(\mod 13) \\ x \equiv 1(\text{mód}\,2) \\ x \equiv 1(\text{mód}\,5) \end{cases}$$

Se trata de un sistema que verifica las condiciones del Teorema Chino del Resto, luego tiene solución.
La solución general del sistema es $x = 91 + 130k$ con $k \in \mathbb{Z}$. Como x está entre 300 y 400, ha de ser

$$x = 351e.$$

3) Supongamos primero que un entero a tiene inverso multiplicativo módulo un entero b. Esto quiere decir que existe $x \in \mathbb{Z}$ tal que $xa \equiv 1(\text{mód}\,b)$, es decir, que $b|xa - 1$. Luego existe un entero y tal que $yb = xa - 1$. O lo que es lo mismo, $xa - yb = 1$. Por tanto, $\mathrm{mcd}(a,b)$ debe dividir a 1. Lo que ocurre solo si $\mathrm{mcd}(a,b) = 1$.
Reciprocamente, supongamos que $\mathrm{mcd}(a,b) = 1$. Por la identidad de Bézout sabemos que existen $\alpha, \beta \in \mathbb{Z}$ tales que $\alpha a + \beta y = 1$. De aquí se deduce que $b|1 - \alpha a$. Es decir, que $\alpha a \equiv 1(\text{mód}\,b)$. Luego α es un inverso multiplicativo de a módulo b.

4) Como $\mathrm{mcd}(121, 250) = 1$, sabemos por el Teorema de Euler que $121^{\phi(250)} \equiv 1 (\mathrm{mód}\, 250)$.
Calculando $phi(250) = \phi(2 \cdot 5^5) = 100$ se tiene entonces que

$$121^{301} \equiv 121 (\mathrm{mód}\, 250).$$

Luego el inverso de 121^{301} módulo 250 es el de 121.
Usando el algoritmo de Euclides para el cálculo de $\mathrm{mcd}(250, 121) = 1$ obtenemos una identidad de Bézout

$$31 \cdot 121 - 15 \cdot 250 = 1.$$

De donde el inverso multiplicativo de 121 módulo 250 es 31.

Ejercicio 3 (10 puntos).

1) Sean $f(x) = x^2 + 1 \in \mathbb{F}_7[x]$ e $I = (f(x))$ el ideal generado por $f(x)$. ¿Es el anillo $\mathbb{F}_7[x]/I$ un cuerpo? ¿Cuántos elementos tiene?
2) Dar razonadamente un ejemplo de un cuerpo con 25 elementos.
3) Sean $f_1(x) = x^5 + x^4 + 6x + 6$ y $f_2(x) = x^3 + 2x^2 + x + 2$ polinomios en $\mathbb{F}_7[x]$. Calcular $\mathrm{mcd}(f_1(x), f_2(x))$, expresarlo como un polinomio mónico. Calcular una identidad de Bézout para estos polinomios.
4) Descomponer el polinomio anterior $f_1(x) \in \mathbb{F}_7[x]$ en factores irreducibles.

Solución.

1) Sabemos que $\mathbb{F}_7[x]/I$ es un cuerpo si y solo si I es maximal, lo que ocurre si y solo si $f(x)$ es irreducible.
Al ser $f(x)$ un polinomio de grado 2, es irreducible si y solo si no tiene raíces en $\mathbb{F}_7$. Como ninguno de los elementos de $\mathbb{F}_7$ anula al polinomio, $f(x)$ no tiene raíces. De aquí que el anillo $\mathbb{F}_7[x]/I$ sea un cuerpo.
Cada clase $g(x) + I \in \mathbb{F}_7[x]/I$ está representada por el resto de dividir $g(x)$ entre $f(x)$. Al ser $f(x)$ de grado 2, los restos son de grado menor o igual que 1. Luego se trata de contar los polinomios de grado menor o igual que 1, $ax + b$, en $\mathbb{F}_7[x]$. Como hay 7 posibles valores para a y b, obtenemos $7^2 = 49$ elementos en el cuerpo $\mathbb{F}_7[x]/I$.
2) Siguiendo el apartado anterior, como $25 = 5^2$, se trata de encontrar un poinomio irreducible de grado 2 en $\mathbb{F}_5[x]$. Se comprueba fácilmente que $f(x) = x^2 + 2$ es irreducible y el cuerpo $\mathbb{F}_5[x]/I$, siendo $I = (f(x))$, tiene 25 elementos.
3) Aplicando el algoritmo de Euclides obtenemos

$$f_1(x) = (x^2 + 6x + 1) f_2(x) + 4x^2 + 4.$$

$$f_2(x) = (2x + 4)(4x^2 + 4) + 0.$$

Luego el máximo común divisor es $4x^2 + 4$. Como nos lo piden mónico, multiplicando por 2 (el inverso de 4 módulo 7) se tiene

$$\mathrm{mcd}(f_1(x), f_2(x)) = x^2 + 1.$$

Deshaciendo los cálculos realizados para el cálculo del máximo común divisor obtenemos la identidad

$$4x^2 + 4 = f_1(x) + (6x^2 + x + 6) f_2(x).$$

Multiplicando por 2 para obtener el polinomio mónico tenemos la Identidad de Bézout buscada:

$$x^2 + 1 = 2 f_1(x) + (5x^2 + 2x + 5) f_2(x).$$

4) Desde luego, uno de los factores de $f_1(x)$ es x^2+1, que además es irreducible como hemos visto en el apartado 1). Dividiendo

$$f_1(x) = (x^2+1)(x^3+x^2+6x+6).$$

Se comprueba que x^3+x^2+6x+6 tiene a 1 y a 6 como raíces, a 6 con multiplicidad 2. Es decir, $x^3+x^2+6x+6 = (x+1)^2(x+6)$. Luego

$$f_1(x) = (x^2+1)(x+1)^2(x+6).$$