

Resolución del 1er parcial de Matemática Discreta II Lunes 13 de mayo de 2002

Problema 1

- a) **(4 Puntos)** Hallar x entre 0 y 21 inclusive tal que $x \equiv 5^{2002} \pmod{22}$.

Resolución: Por el teorema chino de los restos $x \equiv 5^{2002} \pmod{22}$ si y solo si

$$\begin{cases} x \equiv 5^{2002} \pmod{2} \\ x \equiv 5^{2002} \pmod{11} \end{cases}.$$

La primer ecuación es trivial ya que al ser $5 \equiv 1 \pmod{2}$ nos queda que $x \equiv 5^{2002} \pmod{2}$ si y solo si $x \equiv 1^{2002} \pmod{2}$ si y solo si $x \equiv 1 \pmod{2}$ si y solo si x es impar. Para resolver la segunda ecuación podemos usar el teorema (pequeño) de Fermat que en la versión que dice que $a^{p-1} \equiv 1 \pmod{p}$ si $a \not\equiv 0 \pmod{p}$. En este caso tenemos que $5^{10} \equiv 1 \pmod{11}$ por lo tanto $5^{2000} \equiv (5^{10})^{200} \equiv 1 \pmod{11}$ y entonces la segunda ecuación será equivalente a la ecuación $x \equiv 5^2 \pmod{11}$. Como $5^2 \equiv 25 \equiv 3 \pmod{11}$ y 3 es impar y está entre 0 y 21 inclusive, la solución al sistema es $x = 3$.

- b) **(4 Puntos)** Hallar y entre 0 y 22 inclusive tal que $y \equiv 13^{5^{2002}} \pmod{23}$.

Resolución: Por la parte anterior sabemos que $5^{2002} = 22k + 3$ para algún k . Además por el teorema (pequeño) de Fermat sabemos, por ser 23 primo, que $13^{22} \equiv 1 \pmod{23}$ por lo tanto $13^{5^{2002}} \equiv 13^{22k+3} \equiv (13^{22})^k 13^3 \equiv 13^3 \equiv (-10)^3 \equiv -1000 \equiv -(1000 - 4 \cdot 230) \equiv -(1000 - 920) \equiv -80 \equiv -80 + 4 \cdot 23 \equiv 12 \pmod{23}$. Por lo tanto $x = 12$ es la solución.

Problema 2

- a) **(3 Puntos)** Hallar $MCD(a, b)$ sabiendo que $MCD(a, b) \cdot mcm(a, b) = 48$ y que $a^2 = b^2 + 28$.

Resolución: Una forma es resolver el sistema

$$\begin{cases} a \cdot b = 48 \\ a^2 = b^2 + 28 \end{cases}.$$

ya que $MCD(a, b) \cdot mcm(a, b) = ab$. Otra forma podría ser expresar la segunda ecuación en la forma $(a + b)(a - b) = 28 = 4 \cdot 7$ por lo tanto tenemos las siguientes posibilidades

- 1) $a + b = 28$ y $a - b = 1$, pero sumando daría $2a = 29$, lo cual es imposible para un entero a .
- 2) $a + b = 14$ y $a - b = 2$.
- 3) $a + b = 7$ y $a - b = 4$, pero sumando daría $2a = 11$.

Por lo tanto la única posibilidad es la segunda que nos da $a = 8$ y $b = 6$, la cual es la solución del problema ya que $8 \cdot 6 = 48$.

- b) **(5 Puntos)** ¿Existe algún múltiplo de 28 cuyas dos últimas cifras sean 16?. En caso afirmativo, hallar una fórmula para ellos.

Resolución: El problema tiene solución si y solo si la ecuación diofántica $28x = 16 + 100y$ tiene solución o equivalentemente si la ecuación en congruencias $28x \equiv 16 \pmod{100}$ tiene solución. Como $\text{mcd}(28, 100) = 4 \mid 16$ las ecuaciones tiene solución. Además al ser $25 \cdot 2 - 7 \cdot 7 = 1$ tenemos que $100 \cdot 2 - 28 \cdot 7 = 4$ y las soluciones serán $y = 2 \cdot 4 - 7k$ y $x = 7 \cdot 4 + 25k$ para todo k entero, es decir, los múltiplos positivos de 28 serán los de la forma $28(-28 + 25k)$ para cada entero $k \geq 2$ mientras que los múltiplos negativos serán los de la forma $-28(-28 + 25k)$ para cada entero $k \geq 2$.

Problema 3 (8 Puntos) Sean H y K subgrupos de un grupo G . Demostrar que HK es un subgrupo de G si y solo si $HK = KH$.

Resolución:

• $HK \leq G \Rightarrow HK = KH$

– $HK \subset KH$: Sea $hk \in HK$, debemos probar que $hk \in KH$.

$$hk \in HK \xRightarrow{HK \leq G} (hk)^{-1} \in HK \Rightarrow$$

$$k^{-1}h^{-1} \in HK \Rightarrow$$

$$\exists h', k' : k^{-1}h^{-1} = h'k'.$$

Ahora bien, como tanto H como K son subgrupos de G , contendrán a los inversos de h' y k' respectivamente, por lo tanto $k'^{-1}h'^{-1} \in KH$, pero $k'^{-1}h'^{-1} = (h'k')^{-1} = (k^{-1}h^{-1})^{-1}$

– $KH \subset HK$: Sea $kh \in KH$, como H y K son subgrupos de G , contendrán a h^{-1} y k^{-1} respectivamente, por lo tanto $h^{-1}k^{-1} \in HK$. Pero como $HK \leq G$, entonces $(h^{-1}k^{-1})^{-1} \in HK$, pero $(h^{-1}k^{-1})^{-1} = kh$, por lo tanto $kh \in HK$.

• $HK = KH \Rightarrow HK \leq G$

– $a, b \in HK \Rightarrow ab \in HK$: Sean $h, h' \in H$ y $k, k' \in K$ tales que $a = hk$ y $b = h'k'$, entonces $ab = hkh'k'$. Como $HK = KH$, entonces $kh' \in HK$, por lo que existirán $h'' \in H$ y $k'' \in K$ tales que $kh' = h''k''$ y por lo tanto $hkh'k' = hh''k''k'$, pero al ser H y K son subgrupos de G , $hh'' \in H$ y $k''k' \in K$ lo cual implica que $ab = hh''k''k' \in HK$.

– $a \in HK \Rightarrow a^{-1} \in HK$: Sean $h \in H$ y $k \in K$ tales que $a = hk$, entonces $a^{-1} = k^{-1}h^{-1} \in KH = HK$.

Aclaración: Le recordamos que HK se define como el conjunto de todos los productos posibles de la forma hk con $h \in H$ y $k \in K$.

Problema 4 Sean H y K dos subgrupos normales y finitos de un grupo G , tales que

$$MCD(|H|, |K|) = 1.$$

a) **(3 Puntos)** Demostrar que $hk = kh \forall h \in H, k \in K$. **Resolución:** Primero observamos que como H y K son subgrupos, $H \cap K$ también lo será. Por lo tanto, por el teorema de Lagrange: $|H \cap K| \mid |H|, |K|$ por lo tanto $|H \cap K| \mid MCD(|H|, |K|) = 1$, así que $|H \cap K| = 1$, es decir $H \cap K = \{e\}$. Ahora sabemos que $hk = kh$ sii $hkh^{-1}k^{-1} = e$, es decir, bastaría entonces probar que $hkh^{-1}k^{-1} \in H \cap K$. Esto último es así porque al ser K normal $x = hkh^{-1} \in K$ y por ser subgrupo $k^{-1} \in K$ por lo que el producto estará en K . De forma similar, por ser H normal, tenemos que $kh^{-1}k^{-1} \in H$ y por ser subgrupo que el producto con h también estará en H . Al estar $hkh^{-1}k^{-1}$ tanto en H como en K estará en su intersección, como queríamos demostrar.

b) **(5 Puntos)** Demostrar que la función $f : H \times K \rightarrow HK$ definida por $f((h, k)) = hk$ es un isomorfismo de grupos. **Resolución:**

$$\begin{aligned} \text{Homomorfismo: } f((h, k)(h', k')) &= f((hh', kk')) \\ &= hh'kk' =_{\text{parte anterior}} hkh'k' \\ &= f((h, k))f((h', k')) \end{aligned}$$

$$\begin{aligned} \text{Inyectiva: } f((h, k)) = e &\Rightarrow hk = e \\ e &\Rightarrow h = k^{-1} \Rightarrow h \in K \Rightarrow h \in H \cap K \\ &\Rightarrow h = e \Rightarrow k = e. \end{aligned}$$

$$\begin{aligned} \text{Sobreyectiva: si } z \in HK &\Rightarrow \exists h, k : \\ z = hk &= f((h, k)). \end{aligned}$$

Aclaración: $H \times K$ es el grupo cuyos elementos son las parejas ordenadas (h, k) del producto cartesiano de H por K con la operación $(h, k)(h', k') = (hh', kk')$.

Problema 5 Sea $a > 0$ y Γ el conjunto formado por las siguientes biyecciones de $\mathbb{R} \setminus \{0, 1\}$ en sí mismo:

$$\varphi_1(z) = z, \quad \varphi_2(z) = \frac{1}{1-z}, \quad \varphi_3(z) = \frac{z-1}{z},$$

$$\varphi_4(z) = \frac{a}{z}, \quad \varphi_5(z) = 1-z, \quad \varphi_6(z) = \frac{z}{z-1}.$$

Se sabe que (Γ, \circ) es un grupo.

a) **(2 Puntos)** Hallar a . **Resolución:**

Sabemos que al ser Γ un grupo, tiene que ser cerrado bajo la composición, por lo que $\varphi_4 \circ \varphi_5 \in \Gamma$, pero $\varphi_4 \circ \varphi_5(z) = a/(1-z)$ y la única función de Γ que tiende a infinito cuando z tiende a 1 y no vale 0 en 0 es φ_2 por lo tanto $a = 1$.

b) **(2 Puntos)** Escribir la tabla de composición de estas funciones.

	φ_1	φ_2	φ_3	φ_4	φ_5	φ_6
φ_1	φ_1	φ_2	φ_3	φ_4	φ_5	φ_6
φ_2	φ_2	φ_3	φ_1	φ_6	φ_4	φ_5
φ_3	φ_3	φ_1	φ_2	φ_5	φ_6	φ_4
φ_4	φ_4	φ_5	φ_6	φ_1	φ_2	φ_3
φ_5	φ_5	φ_6	φ_4	φ_3	φ_1	φ_2
φ_6	φ_6	φ_4	φ_5	φ_2	φ_3	φ_1

c) **(2 Puntos)** Hallar el orden de cada elemento de Γ .

i	$o(\varphi_i)$
1	1
2	3
3	3
4	2
5	2
6	2

d) **(2 Puntos)** ¿Es $\{\varphi_1, \varphi_4\}$ un subgrupo normal de Γ ? Justificar. **Resolución:** No es normal ya que $\varphi_5\varphi_4\varphi_5^{-1} = \varphi_2\varphi_4\varphi_5 = \varphi_6\varphi_5 = \varphi_3 \notin \{\varphi_1, \varphi_4\}$.