

SEGUNDO PARCIAL - SOLUCIÓN.

Ejercicio 1.

- a. Dado que $\varphi(53) = 52 = 13 \cdot 2^2$, alcanza con comprobar que $2^4 \not\equiv 1 \pmod{53}$ y que $2^{26} \not\equiv 1 \pmod{53}$ (Ver teórico Proposición 4.1.4 pag 62). En primer lugar $2^4 \equiv 16 \not\equiv 1 \pmod{53}$. Para calcular $2^{26} \pmod{53}$ utilizamos exponenciación rápida.

Computamos la tabla:

t	$(2)^{2^t} \pmod{53}$
0	2
1	4
2	16
3	$256 \equiv 44 \pmod{53} \equiv (-9) \pmod{53}$
4	$(-9)^2 \equiv 28 \pmod{53}$

Dado que $26 = 2^4 + 2^3 + 2^1$, tenemos que $2^{26} \equiv 4 \times (-9) \times 28 \equiv 52 \not\equiv 1 \pmod{53}$.

- b. Como 2 es raíz primitiva módulo 53 y $\text{mcd}(19, 52) = 1$, tenemos que existe (un único) $m \in \{1, 2, \dots, 52\}$ tal que $x \equiv 2^m \pmod{53}$. Por lo tanto se debe cumplir que $(2^m)^{19} \equiv 32 \pmod{53}$; es decir que $(2^m)^{19} \equiv 2^5 \pmod{53}$. Por la parte 5 de la proposición 3.7.8 de los apuntes, como $o(2) = 52$, esto sucede si y sólo si $19m \equiv 5 \pmod{52}$. Utilizando el Algoritmo de Euclides Extendidos se deduce que $m \equiv 3 \pmod{52}$ y por lo tanto $x \equiv 2^3 \pmod{53} \equiv 8 \pmod{53}$. Es decir, los $x \in \mathbb{Z}$ que cumplen la ecuación original son entonces de la forma $x = 8 + 53n : n \in \mathbb{Z}$.
- c. La clave k se calcula como $g^{mn} \pmod{p}$. En este caso $p = 53$, $g = 2$ y $m = 28$; además tenemos que $g^m = 2^{28} \equiv 49 \pmod{53}$ (el número que Archivaldo envía). Por tanto $k \equiv g^{mn} \equiv (g^m)^n \equiv (49)^5 \equiv (-4)^5 \pmod{53} \equiv 36 \pmod{53}$. Por lo tanto la clave es $k = 36$.

Ejercicio 2. Ver Teórico

Ejercicio 3.

- a. Ver teórico

- b. i) Observar que \mathbb{Z}_6 es cíclico; por ejemplo tenemos que $\mathbb{Z}_6 = \langle \bar{1} \rangle$. Por lo tanto fijando la imagen de un generador (por ejemplo $f(\bar{1})$) con la condición de que $o(f(\bar{1})) \mid o(\bar{1})$, f queda bien definida y es homomorfismo (definiendo $f(\bar{n}) = f(\bar{1})^n$). (Ver Proposición 3.3.9 de las notas). Entonces, para dar un homomorfismo hay que elegir $f(\bar{1})$ un elemento en S_3 tal que su orden divida a 6. Además, si queremos que f no sea trivial, debemos elegir $f(\bar{1}) \neq e_{S_3} = Id$.

Ahora

$$S_3 = \left\{ Id, \tau_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \tau_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \tau_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \sigma_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \right. \\ \left. \sigma_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \right\}.$$

y tenemos que $o(\tau_i) = 2$ y $o(\sigma_j) = 3$; por lo tanto $f(\bar{1})$ puede ser cualquiera de estos 5 elementos (τ_i o σ_j). Existen entonces 5 homomorfismos no triviales, uno por cada posible asignación de $f(\bar{1})$.

- ii) Como $\text{mcd}(6!, 7) = 1$, los órdenes de los grupos son coprimos en este caso, por lo tanto solo existe el homomorfismo trivial (corolario 3.9.11 en las notas). Se puede probar directamente sin usar el corolario: como $\text{Im}(f) < \mathbb{Z}_7$, tenemos por el Teo. de Lagrange que $|\text{Im}(f)| \mid |\mathbb{Z}_7| = 7$, y si f no es trivial, entonces $|\text{Im}(f)| \neq 1$ y por lo tanto debería ser $|\text{Im}(f)| = 7$. Pero como $7 \nmid 6!$, no se puede cumplir el teo. de órdenes, es decir no se cumple que $6! = |\ker(f)| \cdot 7$. Por lo tanto el único homomorfismo es el trivial.

- c. Si bien $|D_{12}| = 24 = 6 \times 4 = |S_3 \times U(8)|$, los grupos no son isomorfos ya que si existiera un isomorfismo f , se debería cumplir que $o(f(g)) = o(g)$ para todo elemento g . Observar que en D_{12} hay un elemento de orden 12 (por ejemplo rotación de ángulo $\frac{360}{12}$) pero en $S_3 \times U(8)$ no existen elementos de orden 12. Esto es porque los elementos de $S_3 \times U(8)$ son de la forma (σ, x) con $\sigma \in S_3$ y $x \in U(8)$, y $(\sigma, x)^6 = (\sigma^6, x^6) = (Id, \bar{1})$; entonces el orden de cada elemento de $S_3 \times U(8)$ es a lo sumo 6.