

Soluciones.

Ejercicio 1.

- a. Dar la definición de subgrupo de un grupo G .

Solución. En las notas de teórico es la Definición 3.7.1.

- b. Enunciar y demostrar el Teorema de Lagrange para grupos finitos.

Solución. En las notas de teórico es el Teorema 3.8.1.

- c. Para los siguientes grupos G y K determinar si existen homomorfismos no triviales $f : G \rightarrow K$. En caso afirmativo dar un ejemplo, justificando que es un homomorfismo.

i) $G = D_5$, $K = \mathbb{Z}_{13}$.

ii) $G = U(11)$, $K = \mathbb{Z}_5$.

Solución. En el primer caso, $|D_5| = 10$ y $|\mathbb{Z}_{13}| = 13$ son coprimos, entonces el único homomorfismo $f : D_5 \rightarrow \mathbb{Z}_{13}$ es el trivial (ver Corolario 3.9.11, ítem 2)

En el segundo caso, $U(11)$ es un grupo cíclico de orden 10. Para ver si existen homomorfismos $f : U(11) \rightarrow \mathbb{Z}_5$ usamos la Proposición 3.9.9. Un generador de $U(11)$ es 2, de orden 10; el orden de $1 \in \mathbb{Z}_5$ es 5 que divide a 10. Entonces la función $f : U(11) \rightarrow \mathbb{Z}_5$ dada por $f(2^n) = n$ está bien definida y es un homomorfismo no trivial. Explícitamente:

g	2	4	8	5	10	9	7	3	6	1
$f(g)$	1	2	3	4	0	1	2	3	4	0

Ejercicio 2.

- a. Probar que 14 es raíz primitiva módulo 97. Puede asumir que 97 es primo.

Solución. Hay que probar que $o(14) = \varphi(97) = 96$. Para esto utilizamos el criterio de la Proposición 4.1.4 (ítem 4). Como los divisores primos de 96 son 2 y 3, alcanza ver que $14^{32} \not\equiv 1$ (mód 97) y que $14^{48} \not\equiv 1$ (mód 97).

Calculamos módulo 97:

$$14^2 \equiv 2,$$

$$14^4 \equiv (14^2)^2 \equiv 2^2 \equiv 4$$

$$14^8 \equiv (14^4)^2 \equiv 4^2 \equiv 16$$

$$14^{16} \equiv (14^8)^2 \equiv 16^2 \equiv 62$$

$$14^{32} \equiv (14^{16})^2 \equiv 62^2 \equiv 61$$

$$14^{48} \equiv 14^{32} \cdot 14^{16} \equiv 61 \cdot 62 \equiv 96$$

- b. Encontrar un elemento en $U(97)$ de orden 24.

Solución. Usando la fórmula para el orden de una potencia (Proposición 3.7.8, ítem 7), sabemos que $o(14^k) = 96/\text{mcd}(k, 96)$. Si tomamos por ejemplo $k = 4$ tenemos $\text{mcd}(k, 96) = 4$ y entonces $o(14^4) = 24$. Concluimos que $14^4 \equiv 4$ tiene orden 24 en $U(97)$.

- c. Ana y Bernardo quieren acordar una clave común utilizando el método de intercambio de claves Diffie-Hellman. Para ello eligen públicamente el primo $p = 97$ y la raíz primitiva $g = 14$. Ana elige un número secreto n y le envía a Bernardo $g^n \equiv 94$ (mód 97). Bernardo elige en secreto $m = 6$ y le envía a Ana $g^m \equiv 8$ (mód 97). ¿Cuál es la clave común k acordada?

Solución. Bernardo puede calcular $k \equiv (g^n)^m \equiv 94^6 \equiv 50$ (mód 97). Ana también puede calcular $k \equiv (g^m)^n \equiv 8^n$, pero el ejercicio no nos dice cuál es n .

Por si quieren verificarlo, $n = 86$ y efectivamente $8^{86} \equiv 50$ (mód 97). *NOTA: el ejercicio no pide averiguar n .*