

Universidad de la República - Facultad de Ingeniería - IMERL
Matemática Discreta 2

SEGUNDO PARCIAL - 29 DE JUNIO DE 2017. DURACIÓN: 3 HORAS

El parcial es *sin* material y *sin* calculadora.

Ejercicio 1. Sea $g \in G$ tal que $o(g) = n$

- a. Probar que para todo $m \in \mathbb{Z}$ se cumple $g^m = e \iff n \mid m$.
- b. Probar que $g^a = g^b \iff a \equiv b \pmod{n}$.
- c. Probar que $|\langle g \rangle| = n$.
- d. Usar el Teorema de Lagrange para probar que si G es finito, entonces $n \mid |G|$.

Solución.

- a. (\Rightarrow) Si $g^m = e$, dividiendo m entre n tenemos que $m = nq + r$ con $0 \leq r < n$. Por lo tanto $e = g^m = g^{nq+r} = (g^n)^q g^r = e^q g^r = g^r$. En otras palabras $g^r = e$, pero n es el menor entero positivo que cumple $g^n = e$, y como $0 \leq r < n$ debe ser $r = 0$. Luego, $m = nq$ y $n \mid m$.
(\Leftarrow) Si $m = nq$, entonces $g^m = g^{nq} = (g^n)^q = e^q = e$.
- b. $g^a = g^b \iff g^{a-b} = e \xLeftrightarrow{\text{(a)}} n \mid a - b \iff a \equiv b \pmod{n}$.
- c. Por la parte anterior $\langle g \rangle = \{g^k : k \in \mathbb{Z}\} = \{g^0, g^1, \dots, g^{n-1}\}$, donde los elementos g^0, g^1, \dots, g^{n-1} son todos distintos. Concluimos que $|\langle g \rangle| = n$.
- d. Como $\langle g \rangle$ es un subgrupo de G , el Teorema de Lagrange implica que $n = |\langle g \rangle| \mid |G|$.

Ejercicio 2.

- a. Probar que 11 es una raíz primitiva módulo 71.
- b. Aldo y Beatriz eligen $p = 71$ y $g = 11$ para intercambiar claves utilizando el método de Diffie y Hellman. Beatriz elige $m = 7$ y Aldo le envía el número $g^n \equiv 61 \pmod{71}$. ¿Cuál es la clave que acuerdan?

Solución.

- a. Como 71 es primo $\varphi(71) = 70 = 2 \cdot 5 \cdot 7$. Entonces alcanza probar que $11^{10} \not\equiv 1 \pmod{71}$, que $11^{14} \not\equiv 1 \pmod{71}$, y que $11^{35} \not\equiv 1 \pmod{71}$. En efecto calculamos $11^2 \equiv 50$, $11^4 \equiv 50^2 \equiv 15$, $11^8 \equiv 15^2 \equiv 12$, $11^{16} \equiv 12^2 \equiv 2$, $11^{32} \equiv 2^2 \equiv 4$. Ahora $11^{10} \equiv 11^8 \cdot 11^2 \equiv 32 \not\equiv 1$, $11^{14} \equiv 11^{10} \cdot 11^4 \equiv 54 \not\equiv 1$, y $11^{35} \equiv 11^{32} \cdot 11^2 \cdot 11 \equiv 70 \not\equiv 1$.
- b. La clave que acuerdan es $g^{nm} = (g^n)^m \equiv 61^7 \pmod{71}$. Calculamos $61^2 \equiv 29$, $61^4 \equiv 29^2 \equiv 60$, y tenemos $61^7 \equiv 61 \cdot 61^2 \cdot 61^4 \equiv 60 \cdot 10 \cdot 29 \equiv 66 \pmod{71}$.

Ejercicio 3. Alicia y Beto quieren comunicarse con el método ElGamal. A tales efectos eligen un primo p y una raíz primitiva g módulo p . Alicia elige un entero a como su clave privada y calcula $h \equiv g^a \pmod{p}$ como su clave pública. Beto quiere enviar un mensaje $m \in \mathbb{Z}_p$ a Alicia.

- a. Describir el algoritmo de cifrado E que debe usar Beto.
- b. Describir la función de descifrado D que debe usar Alicia.
- c. Demostrar que $D(E(m)) = m$ para todo $m \in \mathbb{Z}_p$.

Solución.

- Beto elige un entero b secreto (utilizable una única vez) y calcula $r \equiv g^b \pmod{p}$ y $c \equiv h^b \cdot m \pmod{p}$, obteniendo $E(m) = (r, c)$.
- Ana calcula $D(r, c) = c \cdot r^{-a} \pmod{p}$
- $D(E(m)) \equiv D(g^b, h^b \cdot m) \equiv (h^b \cdot m) \cdot (g^b)^{-a} \equiv (g^a)^b \cdot m \cdot g^{-ab} \equiv m \cdot (g^{ab} \cdot g^{-ab}) \equiv m \pmod{p}$

Ejercicio 4. Consideramos el grupo dihedral D_3 .

- Describir todos los elementos de D_3 indicando su orden.
- Sean $u, v \in D_3$ dos elementos distintos de orden 2. Probar que uv tiene orden 3.
- Consideramos la función $f : D_3 \rightarrow D_3$ dada por $f(x) = x^2$. ¿Es f un homomorfismo?
- Describir todos los homomorfismos $h : \mathbb{Z}_6 \rightarrow D_3$.

Solución.

- $D_3 = \{e, r, r^2, s, sr, sr^2\}$ donde r y r^2 son rotaciones y tienen orden 3, mientras que s, sr y sr^2 son simetrías axiales y tienen orden 2.
- Como u y v tienen orden 2 son simetrías axiales. Entonces uv es un movimiento directo, debiendo ser $1, r$, o r^2 . Pero $u \neq v$ implica que $uv \neq e$. Entonces uv es una rotación, luego tiene orden 3.
- No es un homomorfismo, por ejemplo si u y v son como en la parte anterior $f(u) = e$ y $f(v) = e$, pero $f(uv) = (uv)^2 \neq e$.
- Como \mathbb{Z}_6 es cíclico generado por $\bar{1}$ de orden 6, cualquier homomorfismo es de la forma $h(\bar{n}) = g^n$ para algún $g \in D_3$ con $o(g) \mid 6$. Pero esto último vale para cualquier $g \in D_3$, entonces hay 6 homomorfismos $h : \mathbb{Z}_6 \rightarrow D_3$, uno para cada posible g .

Bonus. Determinar geoméricamente el punto $P + Q$ en la siguiente curva elíptica:

