

# Solución del Primer Parcial - Matemática Discreta II

Jueves 10 de diciembre de 2020

## Ejercicio 1

- (a) El Teorema de Lagrange asegura que si  $G$  es un grupo de orden finito y  $H$  es un subgrupo de  $G$ , entonces  $|H|$  divide a  $|G|$ .
- (b) El Teorema de Euler afirma que si  $\text{mcd}(a, n) = 1$ , entonces  $a^{\varphi(n)} \equiv 1 \pmod{n}$ .

A continuación, vamos a probar este resultado asumiendo el Teorema de Lagrange. Consideremos el grupo  $U(n)$  de los invertibles módulo  $n$ , y  $a$  tal que  $\text{mcd}(a, n) = 1$ . Como  $a$  es coprimo con  $n$ , entonces  $a \in U(n)$ . Consideremos el subgrupo generado por  $a$  dentro de  $U(n)$ , es decir,  $\langle a \rangle \subseteq U(n)$ . Por el Teorema de Lagrange, si  $r = |\langle a \rangle|$  es el orden de  $\langle a \rangle$ , entonces  $r$  divide a  $|U(n)| = \varphi(n)$ . Entonces, existe un entero  $k$  tal que  $kr = \varphi(n)$ . Como  $r$  es el orden de  $\langle a \rangle$ , sabemos que  $a^r \equiv 1 \pmod{n}$ . Pero entonces:  $a^{\varphi(n)} = (a^r)^k \equiv 1^k \equiv 1 \pmod{n}$ , como queríamos demostrar.

## Ejercicio 2

- (a) Como 19 es primo impar,  $U(19)$  tiene en total  $\varphi(\varphi(19)) = \varphi(18) = \varphi(3^2)\varphi(2) = 6$  raíces primitivas. Veremos que 3 es raíz primitiva. Sea  $r$  el orden del subgrupo  $\langle 3 \rangle$ . Por el Teorema de Lagrange,  $r$  divide a  $|U(19)| = \varphi(19) = 18$ . Luego  $r \in \{1, 2, 3, 6, 9, 18\}$ . Tomando las primeras potencias en base 3, sabemos que  $\langle 3 \rangle$  contiene al menos a  $\{3, 9, 8, 5\}$ , por lo que  $r$  vale 6, 9 o 18. Pero  $3^6 \equiv 7$ , y  $3^9 \equiv 18 \pmod{19}$ , por lo que la única posibilidad es que el primer exponente positivo que iguala al neutro es  $3^{18} \equiv 1 \pmod{19}$ , y  $\langle 3 \rangle = U(19)$ . Concluimos entonces que 3 es raíz primitiva módulo 19.
- (b) Ver detalles sobre Diffie-Hellman en las Notas del Curso.
- (c) Como  $3^{11 \times 7} = 3^{77} = 3^{18 \times 4 + 5} \equiv 3^5 \equiv 15 \pmod{19}$ , la clave compartida es  $k = 15$ .

## Ejercicio 3

- (a) Sea  $(G, *)$  un grupo con neutro  $e_G$ . Luego  $(H, *)$  es subgrupo de  $G$  si cumple con las siguientes propiedades:
- $e_G \in H$  (existencia de neutro).
  - $\forall a, b \in H, a * b \in H$  (cerradura con la operación).
  - $\forall a \in H, \exists b : b * a = a * b = e_G$  (existencia de inverso).

Observar que la propiedad asociativa se hereda de  $G$ . Se puede omitir que el inverso por izquierda lo es por derecha, pues también se hereda de  $G$ .

- (b) Sea  $G$  un grupo y  $H$  un subconjunto de  $G$  que satisface las dos condiciones siguientes:
- (i)  $H$  es no vacío.
- (ii) Si  $h_1, h_2 \in H$  entonces  $h_1 h_2^{-1} \in H$ .

Probemos que  $H$  es un subgrupo de  $G$ . Como  $H$  es no vacío, existe  $h \in H$ . Por la Propiedad (ii):  $h, h \in H$  entonces  $h h^{-1} = e_G \in H$ , por lo que contiene al neutro de  $G$ . Sea  $h \in H$  arbitrario. Por (ii):  $e_G, h \in H$  entonces  $e_G h^{-1} = h^{-1} \in H$ , por lo que contiene a los inversos. Finalmente, veremos que  $H$  es cerrado con su operación: si  $a, b \in H$ , sabemos que  $b^{-1} \in H$ . Por (ii):  $a, b^{-1} \in H$  entonces  $a(b^{-1})^{-1} = ab \in H$ . Concluimos así que  $H$  es subgrupo de  $G$ , como queríamos demostrar.

#### Ejercicio 4

- (a) Como  $G = Z_p$  tiene una cantidad  $p$  prima de elementos, por Lagrange sabemos que si  $\varphi$  es morfismo entonces  $\text{Ker}(\varphi)$  tiene 1 o  $p$  elementos. Si tuviese 1 elemento, el morfismo sería inyectivo, e  $\text{Im}(\varphi)$  tendría  $p$  elementos. Pero esto no es posible porque contradice el Teorema de Lagrange, dado que el subgrupo  $\text{Im}(\varphi)$  de  $K$  tendría orden  $p$ , que no divide a  $(p-1)! = |S_{p-1}|$ . Luego, todo morfismo de  $G = Z_p$  en  $K = S_{p-1}$  debe ser trivial.
- (b) Por el teorema de la raíz primitiva sabemos que  $G = \mathbb{Z}_p$  es cíclico, con orden  $\varphi(p) = p-1$ . Además, como  $p$  es impar entonces  $p-1$  es par. Sea una  $g$  raíz primitiva de  $p$ . Por lo tanto, para definir un morfismo  $f : G \rightarrow K$ , alcanza con encontrar un elemento  $\sigma \in K = S_{p-2}$  de orden  $a$  que divida a  $p-1$ . El morfismo queda definido por  $f(g^n) = \sigma^n$ . Podemos tomar  $\sigma$  tal que  $\sigma(1) = 2$ ,  $\sigma(2) = 1$  y  $\sigma(i) = i$  si  $i \neq 1, 2$ . Es claro que  $\sigma^1 \neq \text{id}$ , y que  $\sigma^2 = \text{id}$ , por lo que  $\sigma$  tiene orden 2.
- (c) Veamos como es  $G$ ,  $U(12) = \{\bar{1}, \bar{5}, \bar{7}, \bar{11}\}$ . Los elementos  $\bar{5}, \bar{7}, \bar{11}$  tienen orden 2 y  $\bar{5} \cdot \bar{7} = \bar{11}$ , sabemos que  $\text{o}(f(g)) \mid \text{o}(g)$  para  $g \in G$  y  $K$  tiene un solo elemento de orden 2 que es  $\bar{2}$ , puedo definir el morfismo  $f(\bar{1}) = \bar{0}, f(\bar{5}) = \bar{2}, f(\bar{7}) = \bar{0}, f(\bar{11}) = \bar{2}$ .