Universidad de la República **Matemática Discreta 2**
Facultad de Ingeniería **Curso 2021**
Instituto de Matemática y Estadística

PRÁCTICO 9 : Grupos-Raíces primitivas.

Recordamos: g es una raíz primitiva módulo n si $U(n) = \langle g \rangle$ (es decir, si $o(g) = \varphi(n)$).

Ejercicio 1. Sea $n \in \mathbb{N}$ y $g \in U(n)$,

a. Probar que g es una raíz primitiva módulo n si y sólo si, para todo $d \neq \varphi(n)$ tal que $d|\varphi(n)$, se tiene que $g^d \not\equiv 1 \pmod{n}$ (esta propiedad es útil para saber si un elemento es raíz primitiva módulo n).

b. Sabiendo que $2^{16} \equiv 3 \pmod{71}$ hallar el resto de dividir 2^{35} entre 71. ¿Es 2 raíz primitiva módulo 71?

c. Probar que g es una raíz primitiva módulo n si y sólo si, para cada primo p divisor de $\varphi(n)$, se cumple que $g^{\varphi(n)/p} \not\equiv 1 \pmod{n}$ (esta propiedad facilita aún más saber si un elemento es raíz primitiva módulo n).

d. Probar que 2 es raíz primitiva módulo 81. Hallar todas las raíces primitivas módulo 81.

Ejercicio 2.

a. Probar que 2 es raíz primitiva módulo 13.

b. Hallar todas las raíces primitivas módulo 13.

Ejercicio 3.

a. Sean G un grupo finito, $g \in G$ y $n \in \mathbb{N}$, probar que $o(g^n) = \frac{o(g)}{\text{mcd}(o(g),n)}$.

b. Sabiendo que 2 es raíz primitiva módulo 101, hallar un elemento de $U(101)$ con orden 10.

Ejercicio 4.

a. Sean $r, s \in \mathbb{N}$. Probar que existen a y b enteros coprimos tales que $a|r$, $b|s$ y $\text{mcm}(r, s) = ab$.

b. Sea G un grupo finito y $x, y \in G$ tales que $xy = yx$. Probar que existe $z \in G$ tal que $o(z) = \text{mcm}(o(x), o(y))$ (recordar que si g y h conmutan y tienen órdenes coprimos, entonces $o(gh) = o(g)o(h)$).

c. Sea p primo y $g \in U(p)$ tal que $o(g) = d < p - 1$.

- **i)** Probar que si $h \notin \langle g \rangle$ entonces $o(h)$ no divide a d (sugerencia: pensar en raíces de $x^d - 1$).
- **ii)** Probar que existe $z \in U(p)$ con $o(z) > o(g)$.

d. Si p es primo, utilizar lo anterior para obtener un algoritmo para hallar una raíz primitiva módulo p.

e. Hallar $\langle 2 \rangle \subset U(23)$ y utilizar el algoritmo anterior para hallar una raíz primitiva módulo 23. Hacer lo análogo para hallar una raíz primitiva módulo 41.

Ejercicio 5. Hallar todas las raíces primitivas módulo 17.

Ejercicio 6.

a. Sea b impar y $k \geq 3$ un entero, probar que $b^{2^{k-2}} \equiv 1 \pmod{2^k}$ (sugerencia: inducción en k).

b. Concluir que no existen raíces primitivas módulo 2^k para $k \geq 3$.

Ejercicio 7. Sean $r, s \in \mathbb{N}$ con $1 < r < s$ y $\operatorname{mcd}(r, s) = 1$.

a. Probar que si $a \in U(rs)$ entonces $a^{\operatorname{mcm}(\varphi(r),\varphi(s))} \equiv 1 \pmod{rs}$.

b. Probar que si $r > 2$ entonces $\operatorname{mcd}(\varphi(r), \varphi(s)) > 1$ (sugerencia: probar que ambos son pares).

c. Probar que sólo pueden existir raíces primitivas módulo m para $m = 2, 4, p^\alpha$ o $2p^\alpha$ con p primo impar y $\alpha \in \mathbb{N}$ (sugerencia: utilizar los ejercicios anteriores).

Ejercicio 8. Sea p un número primo impar y a una raíz primitiva módulo p^α.

a. Probar que si a es impar entonces la clase de a en $U(2p^\alpha)$ es un generador de dicho grupo.

b. Probar que si a es par entonces la clase de $a + p^\alpha$ en $U(2p^\alpha)$ es un generador de dicho grupo.

c. Concluir que existen raíces primitivas módulo $2p^\alpha$ para p primo impar.

d. Hallar una raíz primitiva módulo 162.

Ejercicio 9. (Logaritmo discreto) Sea p un primo impar y r una raíz primitiva módulo p.

a. Probar que $r^a \equiv r^b \mod p \Leftrightarrow a \equiv b \mod (p-1)$.

b. Por lo tanto podemos definir la función $e : \mathbb{Z}_{p-1} \to \mathbb{Z}_p^*$ definida por $e(a \mod (p-1)) = r^a \mod p$. Probar que esta función es biyectiva (*sugerencia: probar que es inyectiva*). A la función inversa de e la llamamos *logaritmo discreto en base* r y se caracteriza por la propiedad $\log_r b = \beta \Leftrightarrow r^\beta \equiv b \mod p$.

c. Probar que si $a \not\equiv 0 \mod p$ y $n \in \mathbb{Z}^+$ entonces $\log_r(a^n) \equiv n \log_r a \mod (p-1)$.

d. Probar que 3 es raíz primitiva módulo 43 y hallar $\log_3 38 \in \mathbb{Z}_{42}$.

Ejercicio 10. Resolver las siguientes congruencias:

a. $x^{27} \equiv 38 \pmod{43}$.

b. $x^{11} \equiv 38 \pmod{43}$.

c. $x^{20} \equiv 38 \pmod{43}$.

d. $28^z \equiv 38 \pmod{43}$

(sugerencia: utilizar que si g es raíz primitiva módulo 43, entonces si $x \in U(43)$, se tiene que $x = g^\alpha$ para algún $\alpha \in \{0, 1, \cdots 41\}$)

Ejercicio 11. (Directo del Teorema de Korselt) Si n es un pseudoprimo de Carmichael (es decir, n es un número compuesto y para todo a se cumple $a^n \equiv a \pmod{n}$; ver ejercicio 10 del Práctico 5) y p es un primo que divide a n entonces:

a. p^2 no divide a n (sugerencia: tomar $a = p$ en la definición de pseudoprimo de Carmichael).

b. $p - 1 | n - 1$ (sugerencia: considerar una raíz primitiva módulo p).

Ejercicio 12. Sea p primo.

a. Probar que si p es impar y r es una raíz primitiva módulo p entonces $r^{p-1/2} \equiv -1 \pmod{p}$.

b. Probar el Teorema de Wilson utilizando raíces primitivas: Si p es primo, entonces $(p-1)! \equiv -1 \pmod{p}$.

Ejercicio 13. Generalice la idea del ejercicio anterior para probar el siguiente resultado:

Si p es un primo impar y $m = p^\alpha$ entonces $\displaystyle\prod_{\text{mcd}(a,m)=1}^{m-1} a \equiv -1 \mod p$

Ejercicio 14. Sea p un primo impar. Para cada $n \in \mathbb{Z}^+$ definimos $S_n = 1^n + 2^n + \ldots + (p-1)^n$. Probar que:

$$S_n \equiv \begin{cases} 0 \pmod{p} & \text{si } n \text{ no es múltiplo de } p-1 \\ -1 \pmod{p} & \text{si } n \text{ es múltiplo de } p-1 \end{cases}$$