Universidad de la República
Facultad de Ingeniería
Instituto de Matemática y Estadística

Matemática Discreta 2
Segundo semestre 2023

PRÁCTICO 9: Grupos - Raíces primitivas.

Ejercicio 1.

a. Probar que 2 es raíz primitiva módulo 13 y también módulo 27.

b. Hallar todas las raíces primitivas módulo 13.

c. Para cada d divisor de 18, hallar un elemento de $U(27)$ con orden exactamente d.

Ejercicio 2. Se sabe que 2 es raíz primitiva módulo 101, $5 \equiv 2^{24} \pmod{101}$, y $6 \equiv 2^{70} \pmod{101}$.

a. Hallar los órdenes de $\bar{5}$ y $\bar{6}$ en $U(101)$.

b. Sea $n = 2^a 3^b$. Hallar a y b enteros positivos para que $\bar{n}$ tenga orden 50 en $U(101)$.

Ejercicio 3.

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

a. Probar que si $a \in U(rs)$ entonces $a^{\mathrm{mcm}(\varphi(r),\varphi(s))} \equiv 1 \pmod{rs}$. Sugerencia: usar Teorema Chino.

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

c. Probar que sólo pueden existir raíces primitivas módulo m para $m = 2, 4, p^\alpha$ o $2p^\alpha$, siendo p primo impar y $\alpha \in \mathbb{N}$. Sugerencia: utilizar las partes anteriores.

Ejercicio 5. 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 6. (Logaritmo discreto) Sea p un primo impar y r una raíz primitiva módulo p.

a. Probar que $r^a \equiv r^b \pmod{p} \Leftrightarrow a \equiv b \pmod{p-1}$.

b. Esto permite definir la función $e : \mathbb{Z}_{p-1} \to \mathbb{Z}_p^*$, tal que: $e\,(a \pmod{p-1}) = r^a \pmod{p}$. 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: $\log_r b = \beta \Leftrightarrow r^\beta \equiv b \pmod{p}$.

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

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

Ejercicio 7. 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: 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 8.

a. Sean $r, s \in \mathbb{N}$. Probar que existen a y b enteros coprimos tales que $a|r$, $b|s$ y $\mathrm{mcm}(r, s) = ab$. Sugerencia: expresar r y s usando sus factorizaciones de primos.

b. Sea G un grupo finito y $x, y \in G$ tales que $xy = yx$. Probar que existe $z \in G$ tal que $o(z) = \mathrm{mcm}(o(x), o(y))$ (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: utilizar que si p es primo, el polinomio $x^d - 1$ tiene a lo sumo d raíces distintas módulo p.

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.

Ejercicios adicionales

Ejercicio 9. (Directo del Teorema de Korselt) Decimos que un entero positivo n es pseudoprimo de Carmichael, si n es compuesto, y se cumple: $a^n \equiv a \pmod{n}$, para todo a. Sea n un pseudoprimo de Carmichael, y sea p un primo que divide a n. Probar:

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 10. 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 11. Generalice la idea del ejercicio anterior para probar el siguiente resultado: si p es un primo impar, y $m = p^\alpha$, entonces: $\prod_{\mathrm{mcd}(a,m)=1}^{m-1} a \equiv -1 \pmod{p}$.

Ejercicio 12. Sea p un primo impar. Para cada $n \in \mathbb{Z}^+$ definimos $S_n = 1^n + 2^n + \ldots + (p-1)^n$. Probar:

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