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

Matemática Discreta 2
Curso 2021

PRÁCTICO 9 : Grupos-Raíces primitivas.

Ejercicio 1.

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

b. Hallar todas las raices primitivas módulo 13.

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

Ejercicio 2. Asumiendo que 2 es raiz primitiva módulo 101, que $5 \equiv 2^{24} \pmod{101}$, que $6 \equiv 2^{70} \pmod{101}$ y que $n = 2^a 3^b$ con a, b enteros positivos, resuelva las siguientes partes.

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

b. Encontrar enteros positivos a, b tal que $\overline{n}$ tenga orden 50 en $U(101)$.

Ejercicio 3.

a. Probar que si G es un grupo y $x, y \in G$ entonces $\langle x \rangle \subseteq \langle y \rangle$ si y solo si $x \in \langle y \rangle$.

b. Sea g una raiz primitiva módulo p con p primo y sean x, y enteros positivos no múltiplos de p. Escribamos $x \equiv g^a \pmod{p}$ y $y \equiv g^b \pmod{p}$ con $a, b \in \mathbb{Z}$. Denotamos como es usual $\overline{x}$ la clase de x en $U(p)$ y por $o(\overline{x})$ su orden multiplicativo en este grupo.

   i. Probar que existe $t \in \mathbb{Z}$ tal que $x \equiv y^t \pmod{p}$ si y solo si $\mathrm{mcd}(b, p-1) | a$.

   ii. Probar que $o(\overline{x}) | o(\overline{y})$ si y solo si $\mathrm{mcd}(b, p-1) | \mathrm{mcd}(a, p-1)$.
   (Sug. utilize que en todo grupo G se cumple $o(g^n) = \frac{o(g)}{\mathrm{mcd}(o(g), n)}$.)

   iii. Concluya que si $o(\overline{x}) | o(\overline{y})$ entonces $\langle \overline{x} \rangle \subseteq \langle \overline{y} \rangle$.

Ejercicio 4.

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

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: pensar en raíces de $x^d - 1$ o utilice el ejercicio 3).

   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.

Ejercicio 5.

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 6. 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 $a^{\mathrm{mcm}(\varphi(r),\varphi(s))} \equiv 1 \pmod{rs}$.

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^α o $2p^\alpha$ con p primo impar y $\alpha \in \mathbb{N}$ (sugerencia: utilizar los ejercicios anteriores).

Ejercicio 7. 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 8. (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 $\log_r b = \beta \Leftrightarrow r^\beta \equiv b \pmod{p}$.

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 9. 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 10. (Directo del Teorema de Korselt) A un entero positivo compuesto n se le llama *pseudoprimo de Carmichael* si para todo a se cumple $a^n \equiv a \pmod{n}$. Sea n un pseudoprimo de Carmichael y sea p un divisor primo de n, pruebe que:

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 11. 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 12. Generalice la idea del ejercicio anterior para probar el siguiente resultado:

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

Ejercicio 13. Sea p un primo impar. Para cada $n \in \mathbb{Z}^+$ definimos $S_n = 1^n + 2^n + \ldots + (p-1)^n$. Probar que:

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