31-05

Práctico 9: Raíces Primitivas

Repaso: $n \in \mathbb{Z}^+$, $g \in \{1, \dots, n\}$ es raíz primitiva módulo n si $\langle \bar{g} \rangle = U(n)$.

Ejemplo: $n=4$: $U(4) = \{1,3\}$

$\langle 1 \rangle = 1$, $\langle 3 \rangle = \langle 3, 3^2, \dots, 3^n \dots \rangle$

$= \langle 3, 1 \rangle \rightsquigarrow$ 3 es r.p. módulo 4.

$n=8$: $U(8) = \{1,3,5,7\}$

$\langle \bar{1} \rangle = \bar{1}$, $\langle \bar{3} \rangle = \langle \bar{3}, \bar{9}=\bar{1} \rangle$, $\langle 5 \rangle = \langle \bar{5}, \bar{1} \rangle$, $\langle 7 \rangle = \langle \bar{7}, \bar{1} \rangle$

No hay raíces primitivas módulo 8.

Teorema: Si existe una raíz primitiva módulo $n \Rightarrow$ hay exactamente $\varphi(\varphi(n))$ r.p.

Proposición (Equivalencias):

1. g raíz primitiva mód n
2. $\text{mcd}(g,n) = 1$ y $o(\bar{g}) = \varphi(n)$
3. $\text{mcd}(g,n) = 1$ y $g^d \not\equiv 1 \pmod{n}$ para $d \mid \varphi(n)$, $d \neq \varphi(n)$.
4. $\text{mcd}(g,n) = 1$ y $g^{\varphi(n)/p} \not\equiv 1 \pmod{n}$ $\forall p \mid \varphi(n)$ primo.

$$o(g^k) = \frac{o(g)}{\text{mcd}(k, o(g))}$$

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.

Módulo 13. "$\varphi(27)$"

(a) $\langle \bar{2} \rangle = \{\bar{2}, \bar{4}, \bar{8}, \bar{3}, \bar{6}, \bar{12}, \bar{11}, \bar{9}, \bar{5}, \bar{10}, \bar{7}, \bar{1}\}$ ✓ ✗ ✗ ✗ ✓ ✗ ✓ ✗ ✓ ✗ ✓ ✗

Basta verificar hasta acá.

→ genera $U(13)$ ⇒ es raíz primitiva

∉ no son r.p.

∈ son r.p.

Por Lagrange $|\langle \bar{2} \rangle| \mid |U(13)| = \varphi(13) = 12$

→ $o(2)$ puede ser 1, 2, 3, 4, 6, 12.

Módulo 27. Usemos (4) y veamos que $2^{\varphi(27)/p} \not\equiv 1 \ (27) \ \forall p \mid \varphi(27)$.

$\varphi(27) = 3^3 - 3^2 = 18$.

- $2^{18/3} \not\equiv 1 \ (27)$
  $2^6 \equiv 2^3 \cdot 2^2 \cdot 2 \ (27)$
  $\equiv 5 \cdot 2 \ (27)$
  $\equiv 10 \ (27)$
  $\not\equiv 1 \ (27)$

- $2^{18/2} \not\equiv 1 \ (27)$.
  $2^9 \not\equiv 1 \ (27)$
  $2^9 \equiv 2^3 \cdot 2^6 \ (27)$
  $\equiv 8 \cdot 10 \ (27)$
  $\equiv -1 \ (27)$

$\rightsquigarrow$ 2 es raíz primitiva módulo 27.

(b) Opción 1: A fuerza bruta, calcular $o(g) \ \forall g \in \{1, \dots, 12\}$

Opción 2: Todo $g \in U(13)$ va a ser de la forma 2^a con $a \in \{1, \dots, 13\}$

$\Rightarrow o(\bar{g}) = o(2^a) = \dfrac{\varphi(13)}{\text{mcd}(a, \varphi(13))}$

$\Rightarrow$ Basta chequear que $\text{mcd}(a, \varphi(13)) = 1$ para que g genere $U(13)$.

Ejemplo: $\bar{6} = \bar{2}^5 \ (13) \Rightarrow \bar{6}$ es raíz primitiva sii $\text{mcd}(5, 12) = 1$ ✓

(c) En $U(27)$.

$d=1$	$d=2$	$d=3$	$d=6$	$d=9$	$d=18$
$1 \to$ def de $o(g)$	$-1 \equiv 26 \ (27)$	$\bar{12}$	$\bar{2}^3 = \bar{8}$	$\bar{2}^{18/9} = \bar{2}^2 = \bar{4}$	$2 \to$ parte (a)

$$d = o(g^k) = \frac{o(g)}{\text{mcd}(k, o(g))}$$

$$o(2^k) = \frac{o(2)}{\text{mcd}(k, o(2))} = \frac{18}{\text{mcd}(k, 18)} = 3$$

Para tener g de orden 3 tomamos k t.q. $\text{mcd}(k, 18) = 6$ y $g = 2^k$.

$k = 6 \quad g = 2^6 = \bar{12}$

Otra forma de verlo: $o(2)=18$ y $d \mid 18 \Rightarrow o\left(2^{18/d}\right)=d$

$2^{18} \equiv 1 \ (27)$ y 18 es el mínimo que cumple eso $\rightsquigarrow$ $\left(2^{18/d}\right)^{d} \equiv 2^{18} \equiv 1$ y d es el mínimo que cumple esto.

Ejercicio 2. Asumiendo que 2 es raiz primitiva módulo 101, que $5 \equiv 2^{24}$ (mód 101), que $6 \equiv 2^{70}$ (mód 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 $U(101)$.

(a) $o(g^k) = \dfrac{o(g)}{\mathrm{mcd}(k, o(g))}$ $g=2$ es r.p. $\Rightarrow$ el orden de g es $\varphi(101)$.

$\varphi(101) = 100$

$$o(5) = \frac{o(2)}{\mathrm{mcd}(24, o(2))} = \frac{100}{\mathrm{mcd}(24, 100)} = \frac{100}{4} = 25.$$

($24 = 3 \cdot 2^3$, $100 = 2^2 \cdot 5^2$)

$$o(6) = o(2^{70}) = \frac{o(2)}{\mathrm{mcd}(70, o(2))} = \frac{100}{\mathrm{mcd}(70, 100)} = \frac{100}{10} = 10.$$

(b) $n = 2^a 3^b$ con $a, b > 0$.

Queremos a y b para que $\overline{n}$ tenga orden 50.

Obs: $o(2) = \varphi(101) = 100 \Rightarrow 2^2$ tiene orden 50, pero no cumple $b > 0$.

Obs2: 2 es r.p. $\Rightarrow 3 \in \langle 2 \rangle \Rightarrow 3 = 2^t$ para algún $t \in \{1, \dots, 100\}$.

$\{2^t : t \in \mathbb{Z}\}$

$\Rightarrow n = 2^a \cdot (2^t)^b$ con $a, b > 0$ y t que podemos calcular.

$\Rightarrow n = 2^{a+tb}$ y usamos la fórmula.

$$50 = o(n) = o\left(2^{a+tb}\right) = \frac{o(2)}{\mathrm{mcd}(a+tb, o(2))}.$$

Tenemos que: 1. hallar t tal que $3 \equiv 2^t \ (101)$
2. usar la fórmula para encontrar algún par (a,b)

1. Sabemos que $6 \equiv 2^{70} \ (101)$

$2^{-1} \cdot 2 \cdot 3 \equiv 2^{70-1} \ (101)$

$3 \equiv 2^{69} \ (101)$

$\boxed{t = 69}$

2. $50 = o(n) = o\left(2^{a+69b}\right) = \frac{100}{mcd(a+69b, 100)}$

Queremos $a, b > 0$ tales que $mcd(a+69b, 100) = 2$.

Podemos pensar $1 \leq a+69b \leq 100 \Rightarrow b = 1$ y a cualquiera tq $mcd(a+69, 100) = 2$

$a = 13 \quad mcd(82, 100) = 2$ ✓

$a = 5$ ✓