# Raices primitivas

→ nos preguntamos si $U(n)$ es cíclico y si lo es cuales son sus generadores

Dado $n \in \mathbb{Z}^+$, decimos que $g \in \{1, \ldots, n\}$ es una raiz primitiva módulo n si $\langle \bar{g} \rangle = U(n)$.

Propiedad: sea $n \in \mathbb{Z}^+$, $g \in \{1, \ldots, n\}$, son equivalentes

1. g es raiz primitiva módulo n
2. $mcd(g, n) = 1$ y $o(\bar{g}) = |U(n)| = \varphi(n)$
3. $mcd(g, n) = 1$ y $g^d \not\equiv 1 \pmod n$ para todo d divisor de $\varphi(n)$ y $d \neq \varphi(n)$
   $\bar{g}^d \neq \bar{1}$
4. → $mcd(g, n) = 1$ y $g^{\varphi(n)/p} \not\equiv 1 \pmod n$ para todo p primo divisor de $\varphi(n)$

**Ejercicio 1.**

**a**. Probar que 2 es raíz primitiva módulo 13.

**b**. Hallar todas las raíces primitivas módulo 13.

**c**. Probar que 2 es raíz primitiva módulo 27.

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

a) veamos que 2 es raiz primitiva modulo 13

* $mcd(2, 13) = 1 \Rightarrow \bar{2} \in U(13)$
* $\varphi(13) = 12 = 2^2 \cdot 3$

→ los primos que dividen a $\varphi(13)$ son 2 y 3

entonces 2 es raiz primitiva módulo 13 $\iff \begin{cases} 2^{12/2} \not\equiv 1 \pmod{13} \\ 2^{12/3} \not\equiv 1 \pmod{13} \end{cases}$

$\iff \begin{cases} 2^6 \not\equiv 1 \pmod{13} \\ 2^4 \not\equiv 1 \pmod{13} \end{cases}$

$2^4 \equiv 16 \equiv 3 \pmod{13}$ ✓

$2^6 \equiv 2^4 \cdot 2^2 \equiv 3 \cdot 4 \equiv 12 \pmod{13}$ ✓

entonces 2 es raíz primitiva modulo 13

b) Hallar todas las raíces primitivas modulo 13

$$U(13) = \{\bar{2}, \bar{2}^2, \bar{2}^3, \bar{2}^4, \bar{2}^5, \dots, \bar{2}^{12}\}$$

los generadores de $U(13)$ son $\{\bar{2}^k : k \in \{1, \dots, 12\}, \ mcd(k, \overset{o(\bar{2})}{12}) = 1\}$

$$= \{\bar{2}^k : 1, 5, 7, 11\}$$

$\Rightarrow$ los generadores de $U(13)$ son $\bar{2}, \bar{2}^5, \bar{2}^7$ y $\bar{2}^{11}$

$$2^5 \equiv 2^4 \cdot 2 \equiv 3 \cdot 2 \equiv 6 \pmod{13}$$
$$2^7 \equiv 2^5 \cdot 2^2 \equiv 6 \cdot 4 \equiv 24 \equiv 11 \pmod{13}$$
$$2^{11} \equiv 2^7 \cdot 2^4 \equiv 11 \cdot 3 \equiv 33 \equiv 7 \pmod{13}$$

las raíces primitivas modulo 13 son: 2, 6, 7 y 11.

c) 2 es raíz primitiva módulo 27

$$\varphi(27) = 27 \cdot \left(1 - \frac{1}{3}\right) = 27 \cdot \frac{2}{3} = 18 = 2 \cdot 3^2$$

$$27 = 3^3$$

$\rightarrow$ los primos que dividen a $\varphi(27)$ son 2 y 3

entonces 2 es raíz primitiva modulo 27 $\Leftrightarrow \begin{cases} 2^{18/2} \not\equiv 1 \pmod{27} \\ 2^{18/3} \not\equiv 1 \pmod{27} \end{cases}$

$$\Leftrightarrow \begin{cases} 2^9 \not\equiv 1 \pmod{27} \\ 2^6 \not\equiv 1 \pmod{27} \end{cases}$$

$$2^6 \equiv 2^5 \cdot 2 \equiv 32 \cdot 2 \equiv 5 \cdot 2 \equiv 10 \pmod{27} \checkmark$$
$$2^9 \equiv 2^6 \cdot 2^2 \cdot 2 \equiv 10 \cdot 4 \cdot 2 \equiv 13 \cdot 2 \equiv 26 \pmod{27} \checkmark$$

entonces 2 es raíz primitiva modulo 27.

d) d divisor de 18

buscamos un elemento en $U(27)$ con orden exactamente d.

divisores de 18 : 1, 2, 3, 6, 9, 18

$18 = 2 \cdot 3^2$

* elemento de orden 18

2 es raiz primitiva modulo 27

$\Rightarrow o(\bar{2}) = \varphi(27) = 18$

$\bar{2}$ es un elemento de orden 18 en $U(27)$

* elemento de orden 1

$\bar{1}$ es un elemento de orden 1 en $U(27)$

* elemento de orden 9

$\Rightarrow$ buscamos $g \in U(27)$ tal que $o(g) = 9$

como 2 es raiz primitiva modulo 27, tenemos $\langle \bar{2} \rangle = U(27)$

entonces $g = \bar{2}^k$ para algún k

$$9 = o(\bar{2}^k) = \frac{o(\bar{2})}{mcd(o(\bar{2}), k)} = \frac{18}{mcd(18,k)} \rightarrow k \text{ tiene que verificar } mcd(18,k) = 2$$

$\Rightarrow k = 2$

entonces $\bar{2}^2 = \bar{4}$ tiene orden 9 en $U(27)$

* elemento de orden 6

$\hookrightarrow$ buscamos $g \in U(27)$ tal que $o(g) = 6$

$g = \bar{2}^k$ para algún k

$$6 = o(\bar{2}^k) = \frac{o(\bar{2})}{mcd(o(\bar{2}), k)} = \frac{18}{mcd(18,k)} \rightarrow k \text{ tiene que verificar}$$

$mcd(18,k) = 3$

$\Rightarrow k = 3$

entonces $\bar{2}^3 = \bar{8}$ es un elemento de orden 6 en $U(27)$

**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 $k \geq 3$.

a) $b$ impar, $k \geq 3$ un entero

$$b^{2^{k-2}} \equiv 1 \pmod{2^k}$$

Vamos a probarlo por inducción en $k$

* <u>caso base</u>: $k = 3$

queremos ver que $b^{2^{3-2}} \equiv 1 \pmod{2^3}$

$$\boxed{b^2 \equiv 1 \pmod 8}$$

$b$ es impar $\Rightarrow b = 2n+1$ para algún $n \in \mathbb{Z}$

$\Rightarrow b^2 = (2n+1)^2 = 4n^2 + 4n + 1 = 8(\text{----}) + 1$

(1) $n$ es par: $n = 2q$ para algún $q \in \mathbb{Z}$

$$\begin{aligned} b^2 &= 4(2q)^2 + 4(2q) + 1 \\ &= 4 \cdot 4q^2 + 8q + 1 \\ &= 8 \cdot 2q^2 + 8q + 1 \\ &= 8(2q^2 + q) + 1 \end{aligned}$$

$\Rightarrow b^2 \equiv 1 \pmod 8$

(2) $n$ es impar $\Rightarrow n = 2q+1$ para algún $q \in \mathbb{Z}$

$$\begin{aligned} b^2 &= 4(2q+1)^2 + 4(2q+1) + 1 \\ &= 4(4q^2 + 4q + 1) + 8q + 4 + 1 \\ &= 8 \cdot 2q^2 + 8 \cdot 2q + 4 + 8q + 4 + 1 \\ &= \underbrace{8 \cdot 2q^2 + 8 \cdot 2q + 8q + 8} + 1 \\ &= 8(2q^2 + 2q + q + 1) + 1 \end{aligned}$$

$\Rightarrow b^2 \equiv 1 \pmod 8$

* <u>paso inductivo</u>

Supongamos que se cumple: $b^{2^{k-2}} \equiv 1 \pmod{2^k}$

Queremos ver que: $b^{2^{(k+1)-2}} \equiv 1 \pmod{2^{k+1}}$

$$b^{2^{k-1}} \equiv 1 \pmod{2^{k+1}}$$

$b^{2^{k-2}} \equiv 1 \pmod{2^k} \Rightarrow \underbrace{b^{2^{k-2}} - 1}_{} = 2^k \alpha$ para algún $\alpha \in \mathbb{Z}$

$\Downarrow$

$b^{2^{k-2}} = 2^k \alpha + 1$

$$\begin{aligned}
b^{2^{k-1}} - 1 &= b^{2^{k-2+1}} - 1 \\
&= b^{2^{k-2} \cdot 2^1} - 1 \\
&= b^{2^{k-2} \cdot 2} - 1 \\
&= \left(b^{2^{k-2}}\right)^2 - 1 \\
&= (2^k \alpha + 1)^2 - 1 \\
&= (2^k \alpha)^2 + 2 \cdot 2^k \alpha + 1 - 1 \\
&= 2^{2k} \alpha^2 + 2^{k+1} \alpha \qquad\qquad 2k = (k+1) + (k-1) \\
&= \underbrace{2^{k+1}}_{} 2^{k-1} \alpha^2 + \underbrace{2^{k+1}}_{} \alpha \\
&= 2^{k+1} (\underbrace{2^{k-1} \alpha^2 + \alpha}_{\in \mathbb{Z}})
\end{aligned}$$

$$\Rightarrow b^{2^{k-1}} - 1 = 2^{k+1} (2^{k-1} \alpha^2 + \alpha)$$

$$\Rightarrow b^{2^{k-1}} \equiv 1 \pmod{2^{k+1}}$$

b) Veamos que no existen raices primitivas modulo $2^k$ para $k \geq 3$

sea $b \in \mathbb{Z}$

$\overline{b} \in U(2^k)$ sii $b$ es impar

$\varphi(2^k) = 2^k(1-\frac{1}{2}) = 2^k \frac{1}{2} = 2^{k-1}$

$\Rightarrow$ el único primo que divide a $\varphi(2^k)$ es 2

entonces $\underset{\text{impar}}{b}$ es raíz primitiva modulo $2^k$ $\Leftrightarrow$ $b^{\varphi(2^k)/2} \not\equiv 1 \pmod{2^k}$

$\Leftrightarrow b^{2^{k-1}/2} \not\equiv 1 \pmod{2^k}$

$\Leftrightarrow \underbrace{b^{2^{k-2}} \not\equiv 1 \pmod{2^k}}$

pero probamos en a) que esto no es cierto

---

Otra forma: sea $\bar{b} \in U(2^k)$

$\Rightarrow b$ impar

$b^{2^{k-2}} \equiv 1 \pmod{2^k}$

$\Rightarrow o(\bar{b}) \leq 2^{k-2} < 2^{k-1} = |U(2^k)|$

$\Rightarrow o(\bar{b}) < |U(2^k)|$

$\Rightarrow \bar{b}$ no es generador de $U(2^k)$

$\Rightarrow b$ no es raíz primitiva modulo $2^k$

No existen raíces primitivas módulo $2^k$