Raíces primitivas

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

fijamos $n \in \mathbb{Z}^+$

decimos que $g \in \{1, .., n\}$ es raíz primitiva modulo n

si es generador de $U(n)$ $\left(\langle \bar{g} \rangle = U(n) \right)$

* g es raíz primitiva modulo $n \iff o(\bar{g}) = \varphi(n)$
* g es raíz primitiva modulo $n \iff$

$$\begin{cases} mcd(g, n) = 1 \\ g^{\varphi(n)/p} \not\equiv 1 \pmod{n} \text{ para todo } p \text{ divisor primo de } \varphi(n) \end{cases}$$

Ejercicio 1.

a. Probar que 2 es raíz primitiva módulo 13.

b. Hallar todas las raíces primitivas módulo 13.

a) 2 raíz primitiva módulo 13

$\varphi(13) = 12 = 2^2 \cdot 3$

→ los divisores primos de $\varphi(13)$ son 2 y 3

$$2 \text{ es raíz primitiva modulo } 13 \iff \begin{cases} 2^{\varphi(13)/2} \not\equiv 1 \pmod{13} \\ 2^{\varphi(13)/3} \not\equiv 1 \pmod{13} \end{cases}$$

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

$2^4 \equiv 16 \equiv 3 \pmod{13}$

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

entonces 2 es raiz primitiva modulo 13

b) todas las raices primitivas modulo 13

2 es raiz primitiva modulo 13

$\Rightarrow \langle \bar{2} \rangle = U(13)$

$\Rightarrow U(13) = \{ \bar{2}, \bar{2}^2, \bar{2}^3, \bar{2}^4, \bar{2}^5, \dots, \underset{\overset{\shortparallel}{\bar{1}}}{\bar{2}^{12}} \}$

si $\bar{2}^k$ es otro generador de $U(13)$

$$\underbrace{o(\bar{2}^k)}_{\overset{\shortparallel}{12}} = \frac{o(\bar{2})}{mcd(o(\bar{2}), k)} = \frac{12}{mcd(12, k)}$$

$\bar{2}^k$ es generador de $U(13)$ sii $mcd(12, k) = 1$

el conjunto de generadores de $U(13)$ es:

$$\{ \bar{2}^k : k \in \{1, \dots, 12\} \text{ y } mcd(k, 12) = 1 \} = \{ \bar{2}^k : k = 1, 5, 7, 11 \}$$
$$= \{ \bar{2}^1, \bar{2}^5, \bar{2}^7, \bar{2}^{11} \}$$

#generadores de $U(13)$ es $\varphi(12) = \varphi(\varphi(13))$

2 raiz primitiva

6 raiz primitiva

$2^5 \equiv 2^4 \cdot 2 \equiv 3 \cdot 2 \equiv 6 \pmod{13}$

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

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

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

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.

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

$27 = 3^3$

$\rightarrow$ los divisores primos de $\varphi(27)$ son 2 y 3

2 es raiz primitiva modulo 27 $\iff \begin{cases} 2^{\varphi(27)/2} \not\equiv 1 \pmod{27} \\ 2^{\varphi(27)/3} \not\equiv 1 \pmod{27} \end{cases}$

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

$2^6 = 2^5 \cdot 2 \equiv 32 \cdot 2 \equiv 5 \cdot 2 \equiv 10 \pmod{27}$

$2^9 = 2^6 \cdot 2^2 \cdot 2 \equiv 10 \cdot 4 \cdot 2 \equiv 40 \cdot 2 \equiv 13 \cdot 2 \equiv 26 \pmod{27}$

$\Rightarrow$ 2 es raiz primitiva modulo 27

d) para cada d divisor de 18 buscamos un elemento de $U(27)$ cuyo orden sea d

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

$\Rightarrow U(27) = \{\bar{2}, \bar{2}^2, \bar{2}^3, \dots, \bar{2}^{18}\}$

$= \{\bar{2}^k : k \in \{1, \dots, 18\}\}$

d divisor de 18 $\rightarrow$ $d = 1, 2, 3, 6, 9, 18$

* elemento de orden 18:

$\langle \bar{2} \rangle = U(27)$

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

* elemento de orden 1:

$\bar{1}$ (el neutro)

* elemento de orden 9:

buscamos k tal que $o(\bar{2}^k) = 9$

$$9 = o(\bar{2}^k) = \frac{o(\bar{2})}{mcd(o(\bar{2}), k)} = \frac{18}{mcd(18, k)}$$

$\Rightarrow mcd(18, k) = 2$

tomamos $k = 2$

$\Rightarrow o(\bar{2}^2) = 9$

$\Rightarrow \bar{4}$ es un elemento de orden 9

* elemento de orden 6:

buscamos k tal que $o(\bar{2}^k) = 6$

$$6 = o(\bar{2}^k) = \frac{o(\bar{2})}{mcd(o(\bar{2}), k)} = \frac{18}{mcd(18, k)}$$

$\Rightarrow mcd(18, k) = 3$

$k \in \{1, \ldots, 18\}$

tomamos $k = 3$

$\bar{2}^3 = \bar{8}$ tiene orden 6

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 $\log_3 38 \in \mathbb{Z}_{42}$.

$\bar{a} \in U(p) \rightsquigarrow \bar{a} = \bar{r}^{?}$

$\log_r(a)$

a) * $\underbrace{r \text{ raíz primitiva}}_{\bar{r} \in U(p) \Rightarrow r \text{ es invertible módulo } p}$ módulo p $\Rightarrow U(p) = \langle \bar{r} \rangle$

$\Rightarrow o(\bar{r}) = |U(p)| = \varphi(p) = p-1$

* $\bar{r}^n = \bar{1} \Leftrightarrow o(\bar{r}) \mid n$

$\bar{r}^{a-b} = \bar{1} \Leftrightarrow o(\bar{r}) \mid a-b \Leftrightarrow p-1 \mid a-b$

queremos probar que

$$r^a \equiv r^b \pmod{p} \Leftrightarrow \overbrace{a \equiv b \pmod{p-1}}^{p-1 \mid a-b}$$

$$r^a \equiv r^b \pmod{p} \Leftrightarrow r^a r^{-b} \equiv r^b r^{-b} \pmod{p}$$

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

$$\Leftrightarrow \bar{r}^{a-b} = \bar{1} \text{ en } U(p)$$

$\iff o(\bar{r}) \mid a-b$

$\iff p-1 \mid a-b$

$\iff a \equiv b \pmod{p-1}$

b) Vamos a definir $e: \mathbb{Z}_{p-1} \longrightarrow \mathbb{Z}_p^*$

$\mathbb{Z}_{p-1} = \{$