02/06

Práctico 9: Raíces primitivas

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

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

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

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

$\varphi(\varphi(4)) = \varphi(2) = 1$

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

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

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.

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 $x \in \langle y \rangle$.

$= \{x^n : n \in \mathbb{Z}\}$

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 $\text{mcd}(b, p-1) | a$.

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

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

(a) $\Rightarrow$ $\langle x \rangle \subseteq \langle y \rangle$ $\quad x = x^1 \in \langle x \rangle \subseteq \langle y \rangle \Rightarrow x \in \langle y \rangle$

$\Leftarrow$ $x \in \langle y \rangle \rightsquigarrow x = y^t \Rightarrow \langle x \rangle = \{y^{tn} : n \in \mathbb{Z}\} \subseteq \langle y \rangle$

(b) $\quad \bar{g}^a = \bar{g}^{bt}$

Si $o(g)$ es finito, entonces $g^m = g^k$ si y sólo si $m \equiv k \pmod{o(g)}$.

$g^a \equiv g^{bt} \ (p) \iff a \equiv bt \pmod{\underset{p-1}{o(g)}} \overset{2.4.2}{\iff} a \equiv bt \pmod{p-1}$

$\iff \text{mcd}(b, p-1) | a$

Teorema 2.4.2. *Dados $a, b, n \in \mathbb{Z}$ y sea $d = \operatorname{mcd}(a, n)$. Entonces la ecuación*

$bt \equiv a \ (p-1)$

$$ax \equiv b \quad (\text{mód } n)$$

tiene solución si y sólo si $d \mid b$. Además, si $d \mid b$ existen exactamente d soluciones distintas módulo n.

b) ii $o(\bar{x}) \mid o(\bar{y}) \iff o(\bar{g}^a) \mid o(\bar{g}^b)$

$\iff \dfrac{o(\bar{g})}{\operatorname{mcd}(a, o(\bar{g}))} \Big| \dfrac{o(\bar{g})}{\operatorname{mcd}(b, o(\bar{g}))}$

$o(g) = p-1$ porque g raíz primitiva módulo p

$\iff \dfrac{p-1}{\operatorname{mcd}(a, p-1)} \Big| \dfrac{p-1}{\operatorname{mcd}(b, p-1)}$

$\iff \exists q$ tal que $\dfrac{p-1}{\operatorname{mcd}(b,p-1)} = q \cdot \dfrac{p-1}{\operatorname{mcd}(a,p-1)}$

$\iff \operatorname{mcd}(a, p-1) = q \operatorname{mcd}(b, p-1)$

$\iff \operatorname{mcd}(b, p-1) \mid \operatorname{mcd}(a, p-1)$

iii $\Leftarrow$ $\langle \bar{x} \rangle \subseteq \langle \bar{y} \rangle \Rightarrow$ Lagrange $o(\bar{x}) \mid o(\bar{y})$.

$\Rightarrow$ $o(\bar{x}) \mid o(\bar{y}) \Rightarrow \operatorname{mcd}(b, p-1) \mid \operatorname{mcd}(a, p-1) \mid a$

$\Rightarrow x \equiv y^t \ (\text{mod } p)$

$\Rightarrow \bar{x} \in \langle \bar{y} \rangle$

$\Rightarrow \langle \bar{x} \rangle \in \langle \bar{y} \rangle$.

Ejercicio 5.

a. Sea b impar y $k \geq 3$ un entero, probar que $b^{2^{k-2}} \equiv 1 \ (\text{mód } 2^k)$ (sugerencia: inducción en k).

b. Concluir que no existen raíces primitivas módulo 2^k para $k \geq 3$.

a) · Caso base ($k=3$) $b^2 \equiv 1 \ (\text{mod } 8)$

$b = 1$	$b = 3$	$b = 5$	$b = 7$
$b^2 \equiv 1 \ (8)$	$b^2 = 9 \equiv 1 \ (8)$	$b^2 = 25 \equiv 1 (8)$	$b^2 = 49 \equiv 1 (8)$

· Supongamos $b^{2^{k-2}} \equiv 1 \ (\text{mod } 2^k)$ (HI)

· Queremos ver si $b^{2^{(k-1)}} \equiv 1 \ (\text{mod } 2^{k+1})$ ☆

$b^{2^{(k-1)}} - 1 \equiv 0 \quad (\text{mod } 2^{k+1})$

$$\boxed{\left(b^{2^{k-2}}\right) \cdot \left(b^{2^{k-2}}\right) = b^{2 \cdot 2^{k-2}} = b^{2^{k-1}}}$$

$$\left(b^{2^{(k-1)}}-1\right) = \overbrace{\left(b^{2^{k-2}}-1\right)}^{2^k}\ \overbrace{\left(\underbrace{b}_{\text{impar}}^{2^{k-2}}+\underbrace{1}_{\text{impar}}\right)}^{2}$$

HI

$$\left.\begin{array}{l} \cdot\ 2^k \mid b^{2^{k-2}}-1 \\ \cdot\ 2 \mid b^{2^{k-2}}+1 \end{array}\right\} \Rightarrow 2^{k+1} \mid b^{2^{k-1}}-1$$

(b) Una raíz primitiva módulo 2^k es b impar tal que $o(b)=\varphi(2^k)=2^k-2^{k-1}=2^{k-1}$

Por la parte (a) $\min\{n\in\mathbb{Z}^+ : b^n\equiv 1\ (2^n)\} \leq 2^{k-2} \underset{\text{estricto.}}{\underset{\uparrow}{<}} 2^{k-1}$