# RAICES PRIMITIVAS:

**Definición:** Si $U(n) = \langle \bar{g} \rangle$ decimos que $g$ es Raíz primitiva modulo $n$

**Proposición:** Si existe una raíz primitiva modulo $n \Rightarrow$ Hay $\varphi(\varphi(n))$ Raíces

**Proposición:** Dado $n \in \mathbb{Z}^+$ y $g \in \{1, \dots, n\}$ Entonces las siguientes afirmaciones son equivalentes

1) $g$ es raíz primitiva mod $n$
2) $mcd(g,n) = 1$ y $o(\bar{g}) = \varphi(n)$
3) $mcd(g,n) = 1$ y $g^d \not\equiv 1 \mod n$ $\forall d \neq \varphi(n)$, $d \mid \varphi(n)$
4) $mcd(g,n) = 1$ y $g^{\frac{\varphi(n)}{p}} \not\equiv 1 \mod n$ $\forall p$ primo, $p \mid \varphi(n)$

## Teorema de la Raíz Primitiva

Si $p$ es primo $\Rightarrow$ Existen raíces primitivas modulo $p$

**Recíproco:** Para $n = 1, 2, 4$ existen raíces primitivas

**Lema:** Sea $p$ impar

1) Si $g$ es una raíz primitiva mod $p$ $\Rightarrow g$ o $g+p$ es raíz primitiva mod $p^2$

2) si $g$ es raíz primitiva mod $p^2$ $\Rightarrow g$ es raíz primitiva mod $p^k$ $\forall k \geq 2$

3) Si $g$ es raíz primitiva mod $p^k$

si $g$ es impar $\Rightarrow g$ es raíz primitiva mod $2p^k$

si $g$ es par $\Rightarrow g + p^k$ es raíz primitiva mod $2p^k$

**Teorema:** Sea $n \in \mathbb{Z}^+$ Si existe una raíz primitiva mod $n$. Entonces
- $n = 1, 2, 4$
- $n = p$ con $p$ primo impar
- $n = p^k$ con $p$ primo impar $k \in \mathbb{Z}^+$
- $n = 2p^k$ con $p$ primo impar $k \in \mathbb{Z}^+$

**Lema:** Sea $G$ un grupo, $x, y \in G$ tales que $xy = y \cdot x$ y $mcd(|x|, |y|) = 1$ $\Rightarrow o(xy) = o(x) \cdot o(y)$

**Lema:** Si $f(x)$ es un polinomio con coef. enteros de grado $d$ y $p$ primo $f(x) = x^d + a_{d-1}x^{d-1} + \dots + a_1 x + a_0$ $\Rightarrow f(x) \equiv 0 \mod p$ tiene a lo sumo $d$ soluciones en $\mathbb{Z}_p$

OBS: ¡No es cierto si $p$ no es primo!

OBS 2: $f(x) \equiv 0 \mod p$ puede tener menos soluciones que el grado

**Lema:** Si $p$ es primo y $d$ divide a $p-1 \Rightarrow x^d \equiv 1 \mod p$ tiene exactamente $d$ soluciones distintas en $U(p)$ o $\mathbb{Z}_p$.

**Propiedad 1:** Sean $r, s \in \mathbb{N}$ $\exists a$ y $b \in \mathbb{N}$ coprimos: $a \mid s$ y $b \mid r$ y $mcd(r,s) = a.b$

**Propiedad 2:** Sea $G$ un grupo finito y $x, y \in G$: $xy = yx$ $\Rightarrow \exists z \in G : o(z) = mcm(o(x), o(y))$