Sea $G = \langle g \rangle = \{ e, g, g^2, \ldots, g^{n-1} \}$

$g^0 = g^n$

$o(g) = n$

Si $mcd(k, n) = 1 \Leftrightarrow g^k$ también es generador de G

Ejemplo: $n = 6$ $G = \{ e, g, g^2, g^3, g^4, g^5 \}$

$g^6 = e$ $k = 4$

$mcd(4, 6) = 2 \neq 1$, ¿g^4 genera G?

$\Leftrightarrow$ todos los elementos de G son potencias de g^4

En un grupo finito, haciendo potencias de un elemento fijo siempre llegamos al neutro en algún momento (el orden). Cuando llegamos, nos fijamos si recorrimos todo el grupo.

$\#G = 6$

$$(g^4)^1 = g^4$$

$$(g^4)^2 = g^8 = g^6 \cdot g^2 = g^2 \qquad (g^6 = e)$$

$$(g^4)^3 = g^{12} = g^6 g^6 = e \cdot e = e = g^0$$

$$\langle g^4 \rangle = \{e, g^4, g^2\}$$

ahora para $k=5$

$$(g^5)^1 = g^5$$

$$(g^5)^2 = g^{10} = g^6 g^4 = g^4$$

$$(g^5)^3 = g^{15} = g^{12} g^3 = g^3$$

$$(g^5)^4 = g^{20} = g^{18} g^2 = g^2$$

$$(g^5)^5 = g^{25} = g^{24} g^1 = g^1$$

$$(g^5)^6 = g^{30} = e$$

Haciendo potencias de 5 aparecieron todos los elementos de G

$\Rightarrow G = \langle g^5 \rangle$

g^5 genera a G

y por otro lado

$\text{mcd}(5,6) = 1$

$G = \{ g^i : i = 0, 1, \dots, n-1 \}$ son todos distintos si $o(g) = n$

los distintos restos mód n

$g^i = g^j \iff i \equiv j \pmod{n}$

Supongamos que $0 \leq i < j \leq n-1$

pero $g^i = g^j$ Entonces $g^j (g^i)^{-1} = e$

(si se hubiera repetido una potencia antes de llegar al neutro)

$(g^i)(g^{n-i}) = g^n = e$

$\Rightarrow (g^i)^{-1} = g^{n-i}$

Entonces $g^j \cdot g^{n-i} = e$

$g^{j+n-i} = e$

$g^{j-i} = e$, $j-i < n$ ↯

$o(g) = n$, es la mínima potencia de g que es igual a e

Si probamos que $g^0, g^k, g^{2k}, \dots, g^{(n-1)k}$ son todos elementos distintos, ya está.

Esto es lo mismo que $\theta(g^k) = n$

Esto es lo mismo que decir que los múltiplos de k abarcan todos los restos mód n

Supongamos que no: $\exists\ 0 \le i < j \le n$ tales que $(g^k)^i = (g^k)^j$

$$g^{ki} = g^{kj}$$

$$g^{ki}\left(g^{kj}\right)^{-1} = e$$

$$g^{ki}\, g^{-kj} = e$$

$$g^{k(i-j)} = e \Rightarrow n = o(g) \mid k(i-j)$$

$$\text{Si } mcd(k,n) = 1 \Rightarrow n \mid (i-j)$$

$$n \nmid k$$

$$\Rightarrow g^{i} = g^{j}, \text{ absurdo.}$$

La gracia es que $\langle g \rangle \cong (\mathbb{Z}_n, +)$

hay una función $f: \mathbb{Z}_n \longrightarrow \langle g \rangle \subseteq (G, \cdot)$

$$f(i) = g^i \in G$$

¿ f es morfismo de grupos?

$$f(a * b) = f(a) * f(b)$$

$$\downarrow \qquad\qquad \downarrow$$

$$+ \qquad\qquad \cdot$$

$$f(a+b) = f(a) \cdot f(b) \; ?$$

$f(a+b) = g^{a+b}$

$f(a) \cdot f(b) = g^a \cdot g^b$

¡ son iguales !

Por lo que vimos antes,

f es biyectiva

$\mathbb{Z}_n = \{\text{Todos los restos módn}\}$

Entonces f es un isomorfismo

$\langle g \rangle \cong \mathbb{Z}_n$