1a) Probar que 2 es raíz primitiva mód 13

Criterio para saber si r es raíz primitiva mód n:

① $\mathrm{mcd}(r, n) = 1$

② $r^{\frac{\varphi(n)}{p}} \not\equiv 1 \pmod{n}$ para ningún p primo que divide a $\varphi(n)$

Se hace este criterio con $r = 2$ y $n = 13, 27$.

(en principio es hacer cuentas directamente)

Lo bueno de este criterio
es que son muchas menos cuentas
en vez de calcular $2^2, 2^3, \dots, 2^{12}$ ya sabemos que es 1
($\underline{10}$ cuentas)

Factorizar 12: $12 = 2 \cdot 2 \cdot 3$ ($\underline{2}$ cuentas)

$2^{\frac{12}{2}}, \quad 2^{\frac{12}{3}}$ ($\underline{2}$ cuentas) $4 < 10$

Fíjense cuánto es la diferencia
con números grandes.

Esto es así porque

r es raíz primitiva mód n

$$\Updownarrow$$

$$o(\bar{r}) = \varphi(n) \text{ en } U(n)$$

$$\parallel$$

$$|U(n)|$$

ojo no confundir las operaciones

Es lo mismo que decir que

$$f : \mathbb{Z}_{\varphi(n)}^{\text{suma}} \longrightarrow U(n)^{\text{multiplicación}}$$

$$f(\bar{i}) = \overline{r^{i}}$$ es un isomorfismo

Esta f siempre es morfismo

$f(\bar a + \bar b) = \bar r^{\,a+b}$, $f(a)\cdot f(b) = \bar r^{\,a} \cdot \bar r^{\,b}$

$$f(\bar a + \bar b) = f(\bar a)\cdot f(\bar b)$$

La pregunta es si f es bijectiva

en este caso es que

$\theta(\bar r) = \varphi(n)$ = cantidad de elementos distintos

Ejemplo $r=2$, $n=13$, $\varphi(13)=|U(13)|=12$ en $U(n)$

3 y 12 no son coprimos

$\theta(8)=4$ $\Rightarrow$ 8 no es raíz prim

f													Verificación
$\mathbb{Z}_{12}$:	0	1	2	3	4	5	6	7	8	9	10	11	12 $(=0)$
$U(13)$:	2^0	2^1	2^2	2^3	2^4	2^5	2^6	2^7	2^8	2^9	2^{10}	2^{11}	2^{12}
mód 13	1	2	4	8	3	6	12	11	9	5	10	7	1
	8^4			8^1			8^2			8^3			8^4

¿9 es raíz primitiva?

$9 \equiv 2^{8} \pmod{13}$ $\quad$ $2^{12} \equiv 1 \pmod{13}$

$9^{2} = 2^{8 \cdot 2} \equiv 2^{16} \equiv 2^{4} \pmod{13}$

$9^{3} \equiv 2^{8 \cdot 3} \equiv 2^{24} \equiv 2^{0} \pmod{13}$

$o(9) = 3$

Ya sabíamos que no iba a funcionar: $8 = \dot{4}$, $12 = \dot{4}$ $\Big\}$ → nunca voy a llegar a todos

entonces todos los restos del exponente de 8^{i} mód 12 son $\dot{4}$

8 y 12 no son coprimos

$$6 \equiv 2^5 \pmod{13}$$

Sí es raíz primitiva, porque 5 y 12 son coprimos.

$$6^1 \equiv 2^5$$

$$6^2 \equiv 2^{10}$$

$$6^3 \equiv 2^{15} \equiv 2^3$$

+5

2^5	6	2^{11}	7
2^{10}	10	2^4	3
2^3	8	2^9	5
2^8	9	2^2	4
2^1	2	2^7	11
2^6	12	$2^{12} \equiv 1 \equiv 2^0$	

El exponente recorrió todos los restos del 1 al 12

5 es coprimo con 12

$\Updownarrow$

$\bar{5}$ genera $\mathbb{Z}_{12}$ $\Leftrightarrow$ $o(\bar{5}) = 12$ en $\mathbb{Z}_{12}$

$\Updownarrow$ por la f $\qquad\qquad\qquad\qquad$ $\Updownarrow$

$\bar{2}^5$ genera $U(13)$ $\Leftrightarrow$ $o(\bar{2}^5) = 12$ en $U(13)$

$\bar{2}^5 = \bar{6}$

$\Updownarrow$

6 es raíz primitiva mód 13

Si r es una raíz primitiva mód n todas las raíces primitivas mód n son:

$$\{ r^i : i \text{ es coprimo con } \varphi(n) \}$$

por eso la cantidad es $\varphi(\varphi(n))$

En el ejercicio:

$r = 2$, $n = 13$, $\varphi(n) = 12$

Los coprimos con 12 son 1, 5, 7 y 11

$\Rightarrow$ las raíces primitivas son $2^1, 2^5, 2^7, 2^{11}$

$2, 6, 11, 7$