1b) 2 es raiz primitiva de 27.

$$|U(27)| = \varphi(27) = 18$$

$\mathbb{Z}_{18}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\cdots \bar{i} \cdots$	$\overline{16}$	$\overline{17}$	$\overline{18} = \bar{0}$	
$\updownarrow$									
$U(27)$	$\bar{1}$	$\bar{2}$	$\bar{4}$	$\bar{8}$	$\cdots \overline{2^i} \cdots$			$\bar{1}$	por ej.

Si quiero un elemento de orden 6 en $U(27)$

Es lo mismo que encontrar un elemento de orden 6 en $\mathbb{Z}_{18}$ (con la suma)

o sea, un x tal que $\underbrace{x+x+x+x+x+x}_{6 \text{ veces}} = 18$, pero menos no

El $\bar{3}$ me sirve

$6 \cdot 3 = 18$ pero ningún múltiplo más chico de 3 es múltiplo de 18

6 es el mínimo ("elevar" en multiplicativo es "multiplicar" en aditivo)

$\Rightarrow \theta(\bar{3}) = 6$ en $\mathbb{Z}_{18}$

¿Qué elemento de $U(27)$ corresponde al $\bar{3}$ de $\mathbb{Z}_{18}$?

Le corresponde $\bar{2}^3 = \bar{8}$, $\theta(\bar{8}) = 6$ en $U(27)$

La correspondencia (el isomorfismo) llamale f

entre $\mathbb{Z}_{18}$ y $U(27)$ no es única

Para cada raíz primitiva hay una

$\overline{2}$ es raíz primitiva, $f(\overline{i}) = \overline{2}^{i}$

por ejemplo,

$\overline{14} = \overline{2}^{5}$ es raíz primitiva.

entonces $f(i) = \overline{14}^{i}$ también es

un isomorfismo entre $\mathbb{Z}_{18}$ y $U(27)$

$$\begin{tikzcd}
\text{Problema en } U(27) \arrow[r, "f^{-1}"] & \text{Problema en } \mathbb{Z}_{18} \arrow[d, "\text{congruencias}"'] \\
\text{Solución en } U(27) & \text{Solución en } \mathbb{Z}_{18} \arrow[l, "f"']
\end{tikzcd}$$

Si G es cíclico de orden m

$$G \longleftrightarrow \mathbb{Z}_m$$

2) Datos: 2 es raiz primitiva mód 101

$$5 \equiv 2^{24} \pmod{101}, \quad 6 \equiv 2^{70} \pmod{101}$$

$n = 2^a 3^b$, a, b enteros positivos

Hallar $\theta(\bar{5})$ y $\theta(\bar{6})$ en $U(101)$

$$U(101) \longleftrightarrow \mathbb{Z}_{100} \qquad \varphi(101) = 100$$

$$\bar{2}^i \longleftrightarrow \bar{i}$$

$$\bar{5} = \bar{2}^{24} \longleftrightarrow \overline{24}$$

$$\bar{6} = \bar{2}^{70} \longleftrightarrow 70$$

Entonces $\theta(\bar{5})$ en $U(101)$ es el mismo que $\theta(\overline{24})$ en $\mathbb{Z}_{100}$

$mcd(24, 100) = 4$

$0 \quad 24 \quad 48 \quad - \quad 99$

todos los que recorro son los múltiplos de 4

son todos los los

$i \equiv k \cdot 4 \mod 100$

$i = k \cdot 4 + l \cdot 100$

Bézout

todos los i van a ser los múltiplos de 4, son 25. $|\langle \overline{24} \rangle| = 25 \Rightarrow \theta(\overline{24}) \boxed{= 25}$

De la misma manera el orden de $\bar{6}$ en $U(101)$ es igual al orden de $\overline{70}$ en $\mathbb{Z}_{100}$

$$\theta(\overline{70}) = \frac{100}{\text{mcd}(70,100)} = 10$$

$$= 10$$

$\bar{n} = \bar{2}^a \, \bar{3}^b$ tal que $\theta(\bar{n}) = 50$ en $U(101)$

$\boxed{a=2, b=0 \text{ es solución}}$

$U(101) \longleftrightarrow \mathbb{Z}_{100}$

$\bar{4} = \bar{2}^2 \longleftrightarrow \bar{2}$ tiene orden 50

$\bar{n} = \bar{2}^k \longleftrightarrow \bar{k}$ tiene orden 50 sii $\text{mcd}(k,100) = 2$

¿qué pasa si queremos una solución con $a, b > 0$?

Podríamos escribir $\bar{2}^a \bar{3}^b$ como $\bar{2}^k$, para eso alcanza despejar $\bar{3}$ como potencia de $\bar{2}$

$$\bar{6} = \bar{2}^{70} \Rightarrow \bar{3} = \bar{6} \cdot \bar{2}^{-1} = \bar{2}^{69}$$

$$\Rightarrow \bar{n} = \bar{2}^a \bar{3}^b = \bar{2}^a \cdot \bar{2}^{69b} = \bar{2}^{a+69b}.$$

queremos que $mcd(a+69b, 100) = 2$

Si $a=1$, $b=1$, $a+69b = 70$ (no sirve) (por ejemplo)

Si $a=5$, $b=1$, $a+69b = 74 = 2 \cdot 37 \Rightarrow mcd(74, 100) = 2$