4e) i) Hallar el resto de dividir 2^{20} entre 253

Ideas: $\mapsto 2^8 = 256 = 253 + 3$ (depende de que es 2)

$$2^8 \equiv 3 \pmod{253}$$

$$2^{20} = 2^{8 \cdot 2 + 4} = (2^8)^2 \cdot 2^4$$

$$\equiv 3^2 \cdot 2^4 \equiv 9 \cdot 16 \equiv 144 \pmod{253}$$

llegamos

En rojo lo interpretamos según la teoría de grupos:

Otra idea: usar lo que aprendimos en la primera parte del curso

Teo. Euler + T.Ch.R.

$253 = 11 \cdot 23$

Queremos saber $\bar{2}^{20} \in U(253)$

2 es coprimo con 253 $\Rightarrow \bar{2} \in U(253)$

$2^{20} \equiv x \pmod{253} \Leftrightarrow \begin{cases} 2^{20} \equiv x \pmod{11} \\ 2^{20} \equiv x \pmod{23} \end{cases}$

$f(a) = (b, c)$

$a \equiv b \pmod{11}$

$a \equiv c \pmod{23}$

$Cop(253) \xrightarrow{f} Cop(11) \times Cop(23)$

$U(253) \xrightarrow{f} U(11) \times U(23)$

f biyectiva

f es homomorfismo de grupos

2 coprimo con 11 $\Rightarrow 2^{\varphi(11)} \equiv 1 \pmod{11}$

$2^{10} \equiv 1 \pmod{11} \Rightarrow 2^{20} = (2^{10})^2 \equiv 1^2 \equiv 1 \pmod{11}$

2 coprimo con 23 $\Rightarrow 2^{\varphi(23)} \equiv 1 \pmod{23}$

$2^{22} \equiv 1 \pmod{23} \Rightarrow 2^{20} = 2^{22-2} = 2^{22} (2^{-1})^2$

inverso mód 23

¿Qué cumple $2^{-1} \pmod{23}$ $\overline{12}$ es el inverso de $\overline{2}$ en $U(23)$

$2^{-1} \cdot 2 \equiv 1 \pmod{23}$

$\overline{2}^{-1} = \overline{12}$

Hay que encontrar un a tal que

$$2a \equiv 1 \pmod{23}$$

$2 \cdot 12 = 24 \equiv 1 \pmod{23}$

$\Rightarrow 2^{-1} \pmod{23} = 12$

Volviendo a la cuenta:

$$2^{20} = 2^{22} \cdot (2^{-1})^2 \equiv 1 \cdot 12^2 \equiv 144 \pmod{23}$$

$$\begin{cases} x \equiv 1 \pmod{11} \\ x \equiv 144 \pmod{23} \end{cases}$$

$\equiv 6 \pmod{23}$

$144 \equiv 144 \pmod{23}$

Si no lo reducíamos y después lo resolvíamos,

$f(\overline{144}) = (\bar{1}, \bar{6})$

pero también $144 = 143 + 1 \equiv 1 \pmod{11}$ $= f(\bar{2}^{23}) = (\bar{2}^{23}, \bar{2}^{20})$

$\Rightarrow x \equiv 144 \pmod{253}$

$\in U(11)$ $\in U(23)$

$2^{20} \equiv 144 \pmod{253}$

$\Rightarrow$ El resto de dividir 2^{20} entre 253 es 144

4e) ii) Hallar el orden de $\bar{2}$ en $U(253)$

$$\theta(\bar{2}) = \min\{n : \bar{2}^n = \bar{1} \in U(253)\}$$

$$= \min\{n : 2^n \equiv 1 \pmod{253}\}$$

Ideas: Teorema de Euler

2 coprimo con 253 $\Rightarrow 2^{\varphi(253)} \equiv 1 \pmod{253}$

$\varphi(253) = \varphi(11)\varphi(23) = 10 \cdot 22 = 220$ $\qquad \bar{2}^{\varphi(253)} = \bar{1} \in U(253)$

$2^{220} \equiv 1 \pmod{253}$

$\bar{2}^{220} = \bar{1} \pmod{253} \Rightarrow \theta(\bar{2}) \mid 220$

$o(\bar{2})$ es un divisor de 220

¿cuáles son los divisores de 220?

220	2
110	2
55	5
11	11
0	

$220 = 2^2 \cdot 5 \cdot 11$

Los divisores de 220 son

1	$\bar{2}^0$	5	$\bar{2}^{32}$ ×	11	55	$\bar{2}^{45}$	×
2	$\bar{2}^4$ ×	10		22	110		
4	$\bar{2}^{16}$ ×	20	$\bar{2}^{144}$ ×	44	220	$\bar{2}^{1}$	

En verde al lado de k anotamos $\bar{2}^k$

× se pueden descartar porque $2^8 = 256$

si $n < 8 \Rightarrow n \leq 7$ $2^n \leq 2^7 \leq 128 < 254$

$\bar{2}^{110} = (\bar{2}^{55})^2$

$= \overline{-45}^2 = \overline{45}^2$

$45 \cdot 45$

225

180

2025

$\theta(\bar{2}) \mid 220 = 2^2 \cdot 5 \cdot 11$

entonces $\theta(\bar{2}) = 2^{\alpha} 5^{\beta} 11^{\gamma}$

$\alpha = 0, 1 \text{ ó } 2$, $\beta = 0 \text{ ó } 1$, $\gamma = 0 \text{ ó } 1$

$220 \quad 1$

$110 \quad 1 \quad 20 \quad 1 \quad 44$?

Si $\theta(\bar{2}) \neq 220$,

entonces

$\theta(\bar{2}) \mid 110$, $(\alpha < 2)$ $\bar{2}^{110} = \bar{1}$

$\theta(\bar{2})$ $\theta(\bar{2}) \mid 20$, $(\gamma < 1)$ $\bar{2}^{20} = \bar{1}$

ó $\theta(\bar{2}) \mid 44$ $(\beta < 1)$ $\bar{2}^{44} = \bar{1}$

Si $\bar{2}^{110} \neq 1$, $\bar{2}^{20} \neq 1$ y $\bar{2}^{44} \neq 1$,

entonces $o(\bar{2}) = 220$

$\bar{2}^{20} = \overline{144} \neq 1$, $\bar{2}^{44} \cdots$

$\bar{2}^{110} = \overline{2025} = \bar{1}$

conclusión: $o(\bar{2}) \mid 110$

$22 = 20 + 2$

$\bar{2}^{22} = \bar{2}^{20}\,\bar{2}^{2}$

$= \overline{144} \cdot \bar{4}$

$= \bar{70}$

576 = 253 · 2 + 70

2025 | 253

2024 8

1

$2 \cdot 5 \cdot 11$

Repetimos el procedimiento

$\bar{2}^{10} = \bar{1}\bar{2} \neq \bar{1}$, $\bar{2}^{55} = \overline{-45} \neq 1$, $\bar{2}^{22} = \overline{70} \neq 1$

110 → 55, 22, 10 → 1

$\neq 1$ $\neq 1$ $\neq 1$

entonces $o(\bar{2}) = 110$

$o(g) \mid |G|$: ¿todos los divisores de $|G|$ son el orden de algún elemento de G?

NO NECESARIAMENTE

$G = U(3) \times U(3)$

$= \{\bar{1}, \bar{2}\} \times \{\bar{1}, \bar{2}\}$ tiene 4 elementos

y todos tienen orden 1 ó 2

(no hay elementos de orden 4)

Si $G = U(3) \times U(3) \times U(3)$

tiene 8 elementos, y todos tienen orden 1 ó 2

(no hay elementos de orden 4 ni de orden 8)