

PÁG. 110 | EX. 2

SIGUE P UN NOMBRE PRIMER NOSTRAR:

$$a) a^2 \equiv b^2 \pmod{p} \Rightarrow a \equiv b \pmod{p} \text{ ó } a \equiv -b \pmod{p}$$

DEM/  $a^2 \equiv b^2 \pmod{p} \Rightarrow p \mid (a^2 - b^2) \Rightarrow p \mid (a+b)(a-b) \Rightarrow$

$\uparrow_{\text{DEF.}} \quad \uparrow_{a^2 - b^2 = (a+b) \cdot (a-b)}$

$\text{COMPROVACIA}$

$$\Rightarrow p \mid (a+b) \text{ ó } p \mid (a-b) \Rightarrow p \mid (a - (-b)) \text{ ó } p \mid (a-b) \Rightarrow$$

$\uparrow \quad \uparrow$

$$a+b = a - (-b)$$

LEMA EUCLIDES  
P PRIMER.

$$\Rightarrow a \equiv -b \pmod{p} \text{ ó } a \equiv b \pmod{p} \quad \checkmark$$

$\uparrow \text{ DEF. COMPR.}$

$$b) x^2 \equiv 1 \pmod{p} \Rightarrow x \equiv 1 \pmod{p} \text{ ó } x \equiv -1 \pmod{p}$$

$\uparrow_{\text{AP. a})}$

$$1 = 1^2$$

c) ÉS CERT b) SI P NO ÉS PRIMER? NO!!

CONTRAEIX:

$$3^2 \equiv 1^2 \pmod{8}$$

PERO

$$3 \not\equiv 1 \pmod{8} \text{ i } 3 \not\equiv -1 \pmod{8}$$

PÁG. 113 |  $m$  ES MÚLTIPLO DE 5  $\Leftrightarrow m$  ACABA EN 0 ó 5.  
Ex: 4b

DENO| SIGUE  $m = \underbrace{a_k a_{k-1} \dots a_2 a_1 a_0}_{\text{DIGITS DEM}}$  ( $m$  ACABA EN  $a_0$ )

ALESHORES  $m = \sum_{i=0}^k a_i \cdot 10^i = a_0 + a_1 \cdot 10 + \dots + a_k \cdot 10^k$ .

[ RECORDATONE:  $a = b \Rightarrow a \equiv b \pmod{\text{QUALSEVO}}$ . ]

\* PER TANT PODER PEDIR MODUL 5 ( $\mathbb{Z}_5$ )

$$m \equiv a_0 + a_1 \cdot 10 + \dots + a_k \cdot 10^k \pmod{5} \Leftrightarrow$$

$$\overline{m} = \overline{a_0} + \overline{a_1} \overline{10} + \dots + \overline{a_k} \overline{10}^k \stackrel{\substack{\uparrow \\ \text{RECORDATONE}}}{=} \overline{a_0} + \overline{0} + \dots + \overline{0} = \overline{a_0}$$

$$\overline{10} = \overline{0} \pmod{5}$$

PER TANT,  $\overline{m} = \overline{a_0}$ .

\* ARA VESEM (A  $\mathbb{Z}_5$ )

$$\overline{m} = \overline{a_0}$$

$$m \text{ MÚLTIPLE DE } 5 \Leftrightarrow \overline{m} = \overline{0} \Leftrightarrow \overline{a_0} = \overline{0} \Leftrightarrow a_0 \in \{0, 5\}$$

(\*)  $a_0$  PERTENECE A  $\mathbb{Z}_5$

(\*) OBS.  $\overline{0} = \{-\dots, -10, -5, 0, 5, 10, 15, \dots\}$  (A  $\mathbb{Z}_5$ )

PER TANT:  $a_0 = 0$  ó  $a_0 = 5$ .  $\Leftrightarrow m$  MÚLTIPLE DE 5

$$\overline{a} + \overline{b} = \overline{a+b}$$

$$\overline{a} \cdot \overline{b} = \overline{a \cdot b}$$

$$\frac{\overline{a^m}}{\overline{a^m}} = \overline{a^m}$$

$$a_0 + a_1 \cdot 10 + \dots + a_k \cdot 10^k$$

$$\overline{a_0} + \overline{a_1} \overline{10} + \dots + \overline{a_k} \overline{10}^k$$

PÀG. 113 |  $m$  MÚLTIPLE DE 9  $\Leftrightarrow$  SUMA DE DIGITS DE  $m$  ÉS MÚLTIPLE DE 9.  
EX. 4c

DENO SIGUE  $m = a_k a_{k-1} \dots a_0$  SÉGUENT EL MATEIX

RAONAMENT QUE A L'APARTAT 4a, PERO MÒDUL 9 ( $\mathbb{Z}_9$ ), TENIM:

$$m = \sum_{i=0}^k a_i 10^i \Rightarrow \bar{m} = \sum_{i=0}^k \bar{a}_i \bar{10}^i = \sum_{i=0}^k \bar{a}_i \bar{10}^i = \sum_{i=0}^k \bar{a}_i$$

$$\text{ÉS A DIR, A } \mathbb{Z}_9, \bar{m} = \sum_{i=0}^k \bar{a}_i \quad \bar{10} = \bar{1} (\mathbb{Z}_9)$$

- PER UNA ALTRA BANDA:

$$m \text{ MÚLTIPLE DE 9} \Leftrightarrow \bar{m} = \bar{0} \text{ (A } \mathbb{Z}_9) \Leftrightarrow \sum_{i=0}^k \bar{a}_i = 0 \text{ (A } \mathbb{Z}_9)$$

$$\bar{m} = \sum_{i=0}^k \bar{a}_i$$

$$\Leftrightarrow 9 \mid \sum_{i=0}^k a_i \Leftrightarrow \sum_{i=0}^k a_i \text{ ÉS MÚLTIPLE DE 9.}$$

DEF.  $\bar{0} (\mathbb{Z}_9)$       DEF. MÚLTIPLE.

PÀG. 113

Ex. 7

NO EXISTEIX CAP  $m \in \mathbb{Z}$  TQ  $5m+3 \in$   
UN QUADRAT.

DEMO, RED. ABS.

SUPOSEM  $\exists m \in \mathbb{Z} \quad \exists t \in \mathbb{Z} \quad \text{tq} \quad 5m+3 = t^2$

PER TANT  $5m+3 \equiv t^2 \pmod{\text{QUALSEvol.}}$

\* PRENEM MÒDUL 5 I TENIM:

$$5m+3 \equiv t^2 \pmod{5} \Leftrightarrow \overline{5m+3} = \overline{t^2} \quad (\text{A } \mathbb{Z}_5)$$

$$\Leftrightarrow \overline{5m} + \overline{3} = \overline{t}^2 \quad (\text{A } \mathbb{Z}_5) \Leftrightarrow \overline{0} + \overline{3} = \overline{t}^2 \Leftrightarrow \overline{3} = \overline{t} \quad (\mathbb{Z}_5)$$

$$\Leftrightarrow \overline{3} = \overline{t}^2 \quad (\mathbb{Z}_5)$$

COM ESTEN A  $\mathbb{Z}_5 \quad t \in \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}\}$

PERÒ

$$*\overline{0}^2 = \overline{0^2} = \overline{0} \neq \overline{3}$$

$$*\overline{1}^2 = \overline{1^2} = \overline{1} \neq \overline{3}$$

$$*\overline{2}^2 = \overline{2^2} = \overline{4} \neq \overline{3}$$

$$*\overline{3}^2 = \overline{3^2} = \overline{9} = \overline{4} \neq \overline{3}$$

$$*\overline{4}^2 = \overline{4^2} = \overline{16} = \overline{1} \neq \overline{3}$$

RECORDATORI

$$\left[ \overline{\alpha}^n = \overline{\alpha^n} \right]$$

CONTRADICCIÓ !!

PÀG 114]  $U_n \geq 0$   $3^{2m+2} - 8m - 9$  ÉS MÚLTIPLO DE 64.  
Ex. 9 (USANT CLASSES i INDУCCIÓ)

DEMO INDУCCIÓ SIMPLE SOBRE M

\* PAS BASE:  $m=0 \Rightarrow 3^{2m+2} - 8m - 9 = 3^2 - 9 - 0 = 64 - 0 = 64$ . O

(RECORDEM QUE 0 ÉS MÚLTIPLO DE QUALSEVOL ENTER TA QUE  
 $U_n \in \mathbb{Z}$  m/0, ÉS A DFN,  $0 = 0 \cdot m$ )

$\xrightarrow{m \geq 0}$  \* PAS. IND: SUPOSEM QUE L'AFIRMACIÓ ÉS CERTA PER  
 $m$  (i.e.  $\underbrace{3^{2m+2} - 8m - 9 = 64k}$ ) i PROVEN PER  $m+1$ :

\* PER  $m+1$  TENGIM

$$3^{2(m+1)+2} - 8(m+1) - 9 = \underbrace{3^{2m+4}}_{\substack{\downarrow \\ 3^2 \cdot 3^{2m+2}}} - 8m - 8 - 9 =$$

$$= 9 \cdot 3^{2m+2} - 8m - 8 - 9 = \underbrace{3^{2m+2} - 8m - 9}_{\substack{\uparrow \\ \text{H.I. } 3^{2m+2} - 8m - 9 = 64k}} + 8 \cdot 3^{2m+2} - 8 =$$

$$\text{H.I. } 3^{2m+2} - 8m - 9 = 64k$$

H.I.

$$\Downarrow 64k + 8(3^{2m+2} - 1)$$

\* ARA, SOCS BASTA VEURE QUE  $3^{2m+2} - 1$  ÉS MÚLTIPLO DE 8 !!

PRENEM MÒDUL 8 i TENGIM:

$$\begin{aligned} \overline{3^{2m+2} - 1} &= \overline{3^{2m} \cdot 3^2 - 1} = \overline{q^m \cdot q^2 - 1} = \overline{q^m} \cdot \overline{q^2} - \overline{1} \\ &= \overline{1}^m \cdot \overline{1}^2 - \overline{1} = \overline{0} \Rightarrow 3^{2m+2} - 1 \text{ ÉS MÚLTIPLO DE 8.} \quad \checkmark \\ \overline{q} &= \overline{1} \pmod{8} \end{aligned}$$