# Álgebra I Práctica 5 Resuelta

Por alumnos de Álgebra I Facultad de Ciencias Exactas y Naturales UBA

# Choose your destiny:

(dobleclick en los ejercicio para saltar)

- Notas teóricas
- Ejercicios de la guía:

1.	<b>5.</b>	9.	13.	<b>17.</b>	<b>21.</b>	<b>25.</b>	<b>29.</b>
<b>2.</b>	<b>6.</b>	10.	14.	18.	<b>22.</b>	<b>26.</b>	30.
<b>3.</b>	<b>7.</b>	11.	<b>15.</b>	19.	<b>23.</b>	<b>27.</b>	
4.	8.	<b>12.</b>	<b>16.</b>	<b>20.</b>	<b>24.</b>	<b>28.</b>	

• Ejercicios Extras

<b>1</b> .	<b>3</b> .	<b>5</b> .	<b>७</b> 7.	<b>6</b> 9.
<b>2</b> .	<b>4</b> .	<b>♦</b> 6.	<b>\delta 8.</b>	

#### Notas teóricas:

Diofánticas:

• Sea aX + bY = c con  $a, b, c \in \mathbb{Z}, a \neq 0$  y  $b \neq 0$  y sea

$$S = \{(x, y) \in \mathbb{Z}^2 : aX + bY = c\} \Rightarrow S \neq \emptyset \iff (a : b) \mid c$$

¡Coprimizar siempre que se pueda!: Las soluciones de S son las mismas que las de S coprimizado.

$$aX + bY = c \stackrel{a' = \frac{a}{(a:b)} \text{ y } b' = \frac{b}{(a:b)}}{c' = \frac{c}{(a:b)}} a'X + b'Y = c'$$

• Las solución general del sistema S coprimizado :

$$S = \left\{ (x,y) \in \mathbb{Z}^2 : (x,y) = \underbrace{(x_0,y_0)}_{\text{Solución particular}} + k \cdot \underbrace{(-b',a')}_{\text{Solución particular}} \text{ con } , k \in \mathbb{Z} \right\}$$

Ecuaciones de congruencia:

•  $aX \equiv c(b) \operatorname{con} a, b \neq 0$ 

¡Coprimizar siempre que se pueda!: Las soluciones de la ecuación original son las mismas que las de la ecuación coprimizada.

$$aX \equiv c \ (b) \xleftarrow{a' = \frac{a}{(a:b)} \text{ y } b' = \frac{b}{(a:b)}} c' = \frac{c}{(a:b)} a'X \equiv c' \ (b')$$

• Ojo con el "  $\iff$  ": Si vas a multiplicar la ecuación por algún número d y se te ocurre poner un  $\iff$  conectando la operación justificá así:

$$\boxed{aX \equiv c\ (b) \iff \underset{\mathbf{d} \perp b}{\mathbf{d}aX} \equiv \mathbf{d}c\ (b)}$$

Porque si  $d \not\perp b$  no vale la vuelta ( $\Leftarrow$ ) en el " $\Longleftrightarrow$ ", y la cagás.

• Si te ponés a hacer cuentas en  $aX \equiv c$  (b)  $sin~que~a~\perp~b,~\underline{la~vas~a~cagar}$ . Yo te avisé  $\clubsuit$ .

Sistemas de ecuaciones de congruencia: Teorema chino del resto

• Sean  $m_1, \ldots m_n \in \mathbb{Z}$  coprimos dos a dos, es decir que  $\forall i \neq j$ , se tiene  $m_i \perp m_j$ , entonces, dados  $c_1, \ldots, c_n \in \mathbb{Z}$  cualesquiera, el sistema de ecuaciones de congruencia

$$\begin{cases}
X \equiv c_1 (m_1) \\
X \equiv c_2 (m_2) \\
\vdots \\
X \equiv c_n (m_n)
\end{cases} \iff X \equiv \mathbf{x_0} (m_1 \cdot m_2 \cdot \cdots \cdot m_n),$$

tiene solución y esa solución,  $x_0$  cumple  $0 \le x_0 < m_1 \cdot m_2 \cdots m_n$ .

Pequeño teorema de Fermat

• Sea p primo, y sea  $a \in \mathbb{Z}$ . Entonces:

1) 
$$a^p \equiv a \ (p)$$

2) 
$$p \nmid a \Rightarrow a^{p-1} \equiv 1 \ (p)$$

• Sea p primo, entonces  $\forall a \in \mathbb{Z}$  tal que  $p \not\mid a$  se tiene:

$$a^n \equiv a^{r_{p-1}(n)}(p), \quad \forall n \in \mathbb{N}$$

Amigate con ésta porque se usa mucho. Marco el p-1 en rojo, porque por alguna razón uno se olvida.

• Sea  $a \in \mathbb{Z}$  y p > 0 primo tal que (a : p) = 1, y sea  $d \in \mathbb{N}$  con  $d \leq p - 1$  el mínimo tal que:

$$\boxed{a^{\mathbf{d}} \equiv 1 \ (p) \Rightarrow \mathbf{d} \, | \, (p-1)}$$

Atento a esto que en algún que otro ejercicio uno encuentra un valor usando PTF, pero eso no quiere decir que no haya <u>otro valor menor!</u> Que habrá que encontrar con otro método.

Nota: Cuando p es primo y a un entero cualquiera, será obvio o no, pero:  $p \not\mid a \Leftrightarrow p \perp a$ . Se usan indistintamente.

#### Ejercicios de la guía:

## **F**alta hacerlo!

Si querés mandarlo: Telegram  $\to \odot$ , o mejor aún si querés subirlo en  $\LaTeX \to \bigcirc$ .

Determinar todos los (a, b) que simultáneamente  $4 \mid a, 8 \mid b \land 33a + 9b = 120$ . **2**.

Si 
$$(33:9) | 120 \Rightarrow 33a + 9b = 120$$
 tiene solución.  $(33:9) = 3, 3 | 120 \checkmark$ 

$$\begin{cases}
4 | a \rightarrow a = 4k_1 \\
8 | b \rightarrow b = 8k_2
\end{cases} \xrightarrow{\text{meto en} \atop 33a + 9b = 120} 132k_1 + 72k_2 = 120 \xrightarrow{\text{(132:72)} = 12 | 120} \text{coprimizo} 11k_1 + 6k_2 = 10$$
Busco solución particular con Euclides:

Busco solución particular con Euclides:

$$\left\{ \begin{array}{l} 11 = 6 \cdot 1 + 5 \\ 6 = 5 \cdot 1 + 1 \end{array} \right\} \xrightarrow[\text{entera de 11 y 6}]{\text{1 como combinación}} 1 = 11 \cdot -1 + 6 \cdot -2 \xrightarrow[\text{particular}]{\text{solución}} 10 = 11 \cdot \left( \underbrace{-10}_{k_1} \right) + 6 \cdot \underbrace{20}_{k_2}$$

Para  $11k_1 + 6k_2 = 10$  tengo la solución general  $(k_1, k_2) = (-10 + (-6)k, 20 + 11k)$  con  $k \in \mathbb{Z}$ Pero quiero los valores de a y b:

La solución general será  $(a,b) = (4k_1, 8k_2) = (-40 + 24k, 160 + (-88)k)$ 

Otra respuesta con solución a ojo menos falopa, esta recta es la misma que la anterior:

$$(a,b) = (2+3k, 6-11k) \text{ con } k \equiv 2 (8)$$

Si se sabe que cada unidad de un cierto producto A cuesta 39 pesos y que cada unidad de un cierto producto B cuesta 48 pesos, ¿cuántas unidades de cada producto se pueden comprar gastando exactamente 135 pesos?

Armo diofántica con enunciado, tengo en cuenta que  $A \ge 0$  y  $B \ge 0$ , dado que son productos ...

$$\begin{cases} 39A + 28B = 135 \\ & \xrightarrow{\text{coprimizar}} \\ (A:B) = 3 \\ 13A + 16B = 45, \\ \text{tiene solución, ya que } \underbrace{(13:16)}_{=1} \mid 45 \\ & \xrightarrow{\text{sale a ojo}} \\ \hline (A,B) = (1,2) \end{cases}$$

Hallar, cuando existan, todas las soluciones de las siguientes ecuaciones de congruencia:

- i)  $17X \equiv 3$  (11)
- ii)  $56X \equiv 28 \ (35)$
- iii)  $56X \equiv 2 (884)$
- iv)  $78X \equiv 30 \ (12126)$

Página 4

i) 
$$17X \equiv 3 \ (11) \iff 6X \equiv 3 \ (11) \iff X \equiv 6 \ (11)$$

ii) 
$$56X \equiv 28 \ (35) \iff 21X \equiv 28 \ (35) \iff \overbrace{(21:35)=7}^{\text{coprimizo}} 3X \equiv 4 \ (5) \iff X \equiv 3 \ (5)$$

iii) 
$$56X \equiv 2 \ (884) \iff 28X \equiv 1 \ (442)$$
 tiene solución  $\iff X = \emptyset$   $X = \emptyset$ 

iv)

$$78X \equiv 30 \text{ (12126)} \xleftarrow{\text{coprimizar}}_{\text{(78:12126)} = 6} 13X \equiv 5 \text{ (2021)},$$

$$dado \ que \overbrace{\text{(13:2021)}}^{1} \mid 5 \ hay \ solución.$$

Busco solución particular con Euclides. Escribo al 5 como combinación entera de 13 y 2021:

$$\begin{cases} 2021 = 13 \cdot 155 + 6 \\ 13 = 6 \cdot 2 + 1 \end{cases} \xrightarrow{\text{1 como combinación}} 1 = 13 \cdot 311 + 2021 \cdot (-2) \\ 1 = 13 \cdot 311 + 2021 \cdot (-2) \Leftrightarrow \xrightarrow{\times 5} 5 = 13 \cdot 1555 + 2021 \cdot (-10) \\ 13 \cdot 1555 = 2021 \cdot 10 + 5 \xrightarrow{\text{Solución general}} X \equiv 1555 \cdot (2021) \end{cases} \checkmark$$
Solución particular

Si no ves el paso !!, hacé el procedimiento para resolver la diofántica, 13X + 2021Y = 5 que es equivalente a  $13X \equiv 5$  (2021).

**5.** Hallar todos los  $(a, b) \in \mathbb{Z}^2$  tales que  $b \equiv 2a$  (5) y 28a + 10b = 26.

Este es parecido al 2.

$$b \equiv 2a \ (5) \iff b = 5k + 2a \xrightarrow{\text{meto en}} 48a + 50k = 26 \xrightarrow{(48:59)=2} 24a + 25k = 13 \xrightarrow{\text{a}} \left\{ \begin{array}{c} a = -13 + (-25)q \\ k = 13 + 24q \end{array} \right\}$$

Let 's  $\ corroborate$ :

$$b = 5 \cdot \underbrace{(13 + 24q)}_{b} + 2 \cdot \underbrace{(-13 + (-25)q)}_{q} = 39 + 70q \begin{cases} b = 39 + 70q \equiv 4 \ (5) & \checkmark \\ 2a = -26 - 50q \equiv -1 \ (5) \equiv 4 \ (5) & \checkmark \end{cases}$$

#### 6. \*\* Falta hacerlo!

Si querés mandarlo: Telegram  $\to \bigcirc$ , o mejor aún si querés subirlo en LATEX  $\to \bigcirc$ .

#### 7. **\forall Falta hacerlo!**

Si querés mandarlo: Telegram  $\to \odot$ , o mejor aún si querés subirlo en LATEX  $\to \bigcirc$ .

## 8. \*\* Falta hacerlo!

Si querés mandarlo: Telegram  $\rightarrow \bigcirc$ , o mejor aún si querés subirlo en  $\LaTeX \rightarrow \bigcirc$ .

#### 9. 😭 Falta hacerlo!

Si querés mandarlo: Telegram  $\rightarrow \bigcirc$ , o mejor aún si querés subirlo en  $\LaTeX \rightarrow \bigcirc$ .

10. Hallar, cuando existan, todos los enteros a que satisfacen simultáneamente:

i) 
$$\begin{cases} \bigstar^{1} a \equiv 3 \ (10) \\ \bigstar^{2} a \equiv 2 \ (7) \\ \bigstar^{3} a \equiv 5 \ (9) \end{cases}$$
El sistema tiene s

El sistema tiene solución dado que 10, 7 y 9 son coprimos dos a dos. Resuelvo:

$$\xrightarrow[\text{en}^{\star^1}]{\text{Arranco}} a = 10k + 3 \stackrel{\text{(7)}}{\equiv} 3k + 3 \stackrel{\text{(*)}^{\star^2}}{\equiv} 2 \text{ (7)} \xrightarrow{\text{usando que}} k \equiv 2 \text{ (7)} \rightarrow k = 7q + 2.$$

$$\xrightarrow{\text{actualizo}\atop a} a = 10 \cdot \underbrace{(7q+2)}_{k} + 3 = 70q + 23 \stackrel{(9)}{\equiv} 7q \stackrel{(\stackrel{\bigstar}{\Rightarrow}^{3})}{\equiv} 5 (9) \xrightarrow{\text{usando que}\atop 7 \perp 9} q \equiv 0 (9) \rightarrow q = 9j$$

$$\xrightarrow{\text{actualizo}\atop a} a = 70 \underbrace{(9j)}_{a} + 23 = 680j + 23 \rightarrow \boxed{a \equiv 23 (630)} \quad \checkmark$$

La solución hallada es la que el Teorema chino del Resto me garantiza que tengo en el intervalo  $[0, 10 \cdot 7 \cdot 9)$ 

ii)

iii) 
$$\begin{cases} \bigstar^{1} a \equiv 1 \ (12) \\ \bigstar^{2} a \equiv 7 \ (10) \\ \bigstar^{3} a \equiv 4 \ (9) \end{cases}$$

#### 11. \* Falta hacerlo!

Si querés mandarlo: Telegram  $\rightarrow \bigcirc$ , o mejor aún si querés subirlo en  $\LaTeX \rightarrow \bigcirc$ .

#### 12. \*\* Falta hacerlo!

Si querés mandarlo: Telegram  $\rightarrow \bigcirc 3$ , o mejor aún si querés subirlo en  $\LaTeX \rightarrow \bigcirc 3$ .

#### 13. 🏖 Falta hacerlo!

Si querés mandarlo: Telegram  $\rightarrow \bigcirc 3$ , o mejor aún si querés subirlo en  $\LaTeX \rightarrow \bigcirc 3$ .

#### 14. Falta hacerlo!

Si querés mandarlo: Telegram  $\rightarrow \bigcirc$ , o mejor aún si querés subirlo en  $\LaTeX \rightarrow \bigcirc$ .

**15.** Hallar el resto de la división de a por p en los casos.

i) 
$$a = 71^{22283}$$
,  $p = 11$ 

$$a = 71^{22283} = 71^{10 \cdot 2228 + 2 + 1} = \underbrace{(71^{10})^{2228}}_{\stackrel{11 \neq p}{=} 1^{2228}} \cdot 71^2 \cdot 71^1 \equiv 71^3 \ (11) \rightarrow a \equiv 5^3 \ (11)$$

Usando corolario con p primo y  $p \perp 71$ ,  $\rightarrow 71^{22283} \equiv 71^{r_{10}(22283)}$  (11)  $\equiv 71^3$  (11)  $\rightarrow a \equiv 5^3$  (11)  $\checkmark$ 

ii) 
$$a = 5 \cdot 7^{2451} + 3 \cdot 65^{2345} - 23 \cdot 8^{138}, \, p = 13$$

$$a \equiv 5 \cdot 7^{204 \cdot 12 + 3} + 3 \cdot 8^{11 \cdot 12 + 6} (13) \rightarrow a \equiv 5 \cdot (7^{12})^{204} \cdot 7^3 + 3 \cdot (8^{12})^{11} \cdot 8^6 (13)$$

$$\xrightarrow{p \not \uparrow 7} a \equiv 5 \cdot 7^3 + 3 \cdot 8^6 (13) \rightarrow a \equiv 5 \cdot (-6^3 + 3 \cdot 5^5) (13) \text{ consultar}$$

16. Resolver en  $\mathbb{Z}$  las siguientes eecuaciones de congruencia:

i) 
$$2^{194}X \equiv 7 (97)$$

$$\xrightarrow{2 \perp 97} 2^{194} = (2^{96})^2 \cdot 2^2 \equiv 4 \ (97) \to 4X \equiv 7 \ (97) \xrightarrow{\times 24} -X \equiv \underbrace{168}_{\stackrel{(97)}{\equiv} 71} (97) \xrightarrow{-71 \stackrel{(97)}{\equiv} 26} X \equiv 26 \ (97) \quad \checkmark$$

ii)  $5^{86}X \equiv 3 (89)$ 

## Y Falta hacerlo!

Si querés mandarlo: Telegram  $\to \bigcirc$ , o mejor aún si querés subirlo en  $\LaTeX \to \bigcirc$ .

- Probar que para todo  $a \in \mathbb{Z}$  vale
  - i)  $728 \mid a^{27} a^3$
  - ii)  $\frac{2a^7}{25} + \frac{a}{7} \frac{a^3}{5} \in \mathbb{Z}$
  - i)  $728 = 2^3 \cdot 7 \cdot 13$

Pruebo congruencia con  $2^3$ , 7 y 13.

$$728 \mid a^{27} - a^3 \Rightarrow$$

$$\begin{cases}
2 \mid a^{27} - a^{3} \Rightarrow \\
2 \mid a^{27} - a^{3} \xrightarrow{2 \not | a} (\underline{a})^{27} - (\underline{a})^{3} \equiv 0 \ (2) \Rightarrow 2 \mid a^{27} - a^{3}
\end{cases}$$

$$\begin{cases}
2 \mid a^{27} - a^{3} \xrightarrow{2 \not | a} (\underline{a})^{27} - (2k)^{3} \equiv 0 \ (8) \Leftrightarrow 2^{3} \cdot (\underline{2^{3}})^{8} \cdot k^{27} - \underline{2^{3}} \cdot k^{3} \equiv 0 \ (8) \end{cases}$$

$$\begin{cases}
3 \mid a^{27} - a^{3} \Leftrightarrow 3^{27} - 3^{3} \equiv 0 \ (8) \Leftrightarrow (\underline{3^{2}})^{13} \cdot 3 - \underline{3^{2}} \cdot 3 \equiv 0 \ (8) \end{cases}$$

$$\begin{cases}
5 \mid a^{27} - a^{3} \Leftrightarrow 5^{27} - 5^{3} \equiv 0 \ (8) \Leftrightarrow (\underline{5^{2}})^{13} \cdot 5 - \underline{5^{2}} \cdot 5 \equiv 0 \ (8)
\end{cases}$$

$$\begin{cases}
7 \mid a^{27} - a^{3} \Leftrightarrow a^{27} - a^{3} \Leftrightarrow a^{27} - a^{3} \equiv 0 \ (7) \xrightarrow{\text{Caso } 7 \not | a} a^{27} - a^{3} \equiv 0 \ (7) \Leftrightarrow a^{3} - a^{3} \equiv 0 \ (7)
\end{cases}$$

$$\begin{cases}
8 \mid a^{27} - a^{3} \Leftrightarrow a^{27} - a^{3} \equiv 0 \ (7) \xrightarrow{\text{Caso } 7 \not | a} a^{27} - a^{3} \equiv 0 \ (7) \Leftrightarrow a^{3} - a^{3} \equiv 0 \ (7)
\end{cases}$$

$$\begin{cases}
8 \mid a^{27} - a^{3} \Leftrightarrow a^{27} - a^{3} \equiv 0 \ (13) \xrightarrow{\text{Caso } 13 \not | a} a^{27} - a^{3} \equiv 0 \ (13) \Leftrightarrow a^{3} - a^{3} \equiv 0 \ (13) \end{cases}$$

#### 🚰 Falta hacerlo!

Si querés mandarlo: Telegram  $\to \bigcirc 3$ , o mejor aún si querés subirlo en  $\LaTeX \to \bigcirc 3$ .

#### 😭 Falta hacerlo!

Si querés mandarlo: Telegram  $\to \odot$ , o mejor aún si querés subirlo en  $\LaTeX \to \bigcirc$ .

- 20. Hallar el resto de la división de:
  - i)  $43 \cdot 7^{135} + 24^{78} + 11^{222}$  por 70
  - ii)  $\sum_{i=1}^{1759} i^{42}$  por 56

## i) **\*** Falta hacerlo!

Si querés mandarlo: Telegram  $\rightarrow \bigcirc 0$ , o mejor aún si querés subirlo en LATEX $\rightarrow \bigcirc 0$ .

ii) Calcular el resto pedido equivale a resolver la ecuaición de equivalencia:

$$X \equiv \sum_{i=1}^{1759} i^{42} (56) \text{ que será aún más simple en la forma: } \begin{cases} X \equiv \sum_{i=1}^{1759} i^{42} (7) \\ X \equiv \sum_{i=1}^{1759} i^{42} (8) \end{cases}$$

Primerlo estudio la ecuación de módulo 7: 
$$\begin{cases} \sum_{i=1}^{1759} i^{42} \equiv X \ (7) \\ \stackrel{1}{\bigstar}^{1} \xrightarrow{\text{7 es primo, uso Fermat}} \\ \sum_{i=1}^{1759} i^{42} \equiv X \ (7) \\ \stackrel{1}{\bigstar}^{1} \xrightarrow{\text{7 es primo, uso Fermat}} \\ \sum_{i=1}^{1759} i^{42} = \sum_{i=1}^{1759} (i^{6})^{7} \xrightarrow{251 \cdot 7 + 2 = 1759} \\ \sum_{i=1}^{1759} (i^{6})^{7} \stackrel{(7)}{\equiv} 251 \cdot ((1^{6})^{7} + (2^{6})^{7} + (3^{6})^{7} + (4^{6})^{7} + (5^{6})^{7} + (6^{6})^{7} + (7^{6})^{7}) + ((1^{6})^{7} + (2^{6})^{7} + (3^{6})^{7} + (4^{6})^{7}) \\ \sum_{i=1}^{1759} (i^{6})^{7} \stackrel{(7)}{\equiv} 251 \cdot (1 + 1 + 1 + 1 + 1 + 1 + 1) + (1 + 1 + 1 + 1) = 251 \cdot 6 + 4 \\ \stackrel{(7)}{\equiv} 1 \\ \stackrel{(7)}{\Longrightarrow} 1 \\ \stackrel{(7)}{\Longrightarrow}$$

$$\begin{cases} \sum_{i=1}^{1759} i^{42} \equiv X \ (8) \xrightarrow{\text{8 no es primo}} \text{Analizo a mano} \xrightarrow{219 \cdot 8 + 7 = 1759} X \equiv \sum_{i=1}^{1759} i^{42} \ (8) \stackrel{\text{(8)}}{\equiv} \\ 219 \cdot \underbrace{(1^{42} + 2^{42} + 3^{42} + 4^{42} + 5^{42} + 6^{42} + 7^{42} + 0^{42})}_{\text{8 terminos: } r_8(i^{42}) = (r_8(i))^{42}} + \underbrace{(1^{42} + 2^{42} + 3^{42} + 4^{42} + 5^{42} + 6^{42} + 7^{42})}_{\text{8 terminos: } r_8(i^{42}) = (r_8(i))^{42}} \\ \begin{cases} 2^{42} = (2^3)^{14} \stackrel{\text{(8)}}{\equiv} 0 \\ 4^{42} = (2^3)^{14} \cdot (2^3)^{14} \stackrel{\text{(8)}}{\equiv} 0 \\ 6^{42} = (2^3)^{14} \cdot 3^{42} \stackrel{\text{(8)}}{\equiv} 0 \\ 1^{42} = 1 \\ 3^{42} = (3^2)^{21} \stackrel{\text{(8)}}{\equiv} 1^{21} = 1 \\ 5^{42} = (5^2)^{21} \stackrel{\text{(8)}}{\equiv} 1^{21} = 1 \\ 7^{42} = (7^2)^{21} \stackrel{\text{(8)}}{\equiv} 1^{21} = 1 \end{cases}$$

$$\xrightarrow{\text{reemplazo} \atop \text{esa en}} \sum_{i=1}^{1759} i^{42} \stackrel{\text{(8)}}{\equiv} 219 \cdot 4 + 4 = 880 \stackrel{\text{(8)}}{\equiv} 0 \rightarrow X \equiv 0 \text{ (8)}$$

El sistema  $\begin{cases} X \equiv 3 \ (7) \\ X \equiv 0 \ (8) \end{cases}$  tiene solución  $X \equiv 24 \ (56)$ , por lo tanto el resto pedido:  $r_{56}$ 

$$o: \left[ r_{56} \left( \sum_{i=1}^{1759} i^{42} \right) = 24 \right]$$

#### **F**alta hacerlo!

Si querés mandarlo: Telegram  $\to \odot$ , o mejor aún si querés subirlo en  $\LaTeX \to \bigcirc$ .

Resolver en  $\mathbb{Z}$  la ecuación de congruencia  $7X^{45} \equiv 1$  (46).

$$7X^{45} \equiv 1 \text{ (46)} \xrightarrow{\text{multiplico por} \atop 13} 91X^{45} \equiv 13 \text{ (46)} \rightarrow X^{45} \equiv -13 \text{ (46)} \rightarrow X^{45} \equiv 33 \text{ (46)}$$

$$\rightarrow \begin{cases} X^{45} \equiv 33 \text{ (23)} \rightarrow X^{45} \equiv 10 \text{ (23)} \xrightarrow{23 \text{ primo y } 23 \text{ / } X} X^{22}X^{22}X^{1} \stackrel{(23)}{\equiv} X \equiv 10 \text{ (23)} \end{cases}$$

$$X^{45} \equiv 10 \text{ (2)} \rightarrow X^{45} \equiv 0 \text{ (2)} \xrightarrow{\text{si mismo impar veces}} X \equiv 0 \text{ (2)}$$

La ecuación de congruencia  $|X \equiv 10 (46)|$  cumple las condiciones encontradas.

Hallar todos los divisores positivos de  $5^{140} = 25^{70}$  que sean congruentes a 2 módulo 9 y 3 módulo 11.

Quiero que ocurra algo así:  $\begin{cases} 25^{70} \equiv 0 \ (d) \to 5^{140} \equiv 0 \ (d) \\ d \equiv 2 \ (9) \\ d \equiv 3 \ (11) \end{cases}$ . De la primera ecuación queda que el divisor  $d = 5^{\alpha} \text{ con } \alpha \text{ compatible con las otras ecuaciones.} \to \begin{cases} 5^{\alpha} \equiv 2 \ (9) \\ 5^{\alpha} \equiv 3 \ (11) \end{cases}$ 

 $\rightarrow$  Busco periodicidad en los restos de las exponenciales  $5^{i\alpha?} \equiv 1$ :

$$5^{\alpha} \equiv 2 \ (9)$$

$$5^{3} \equiv -1 \ (9) \Leftrightarrow 5^{6} \equiv 1 \ (9) \Leftrightarrow 5^{6k+r_{6}(\alpha)} = (5^{6})^{k} 5^{r_{6}(\alpha)}.$$
Busco, posibles valores para  $r_{6}(\alpha)$ : 
$$\frac{r_{6}(\alpha)}{r_{9}(5^{\alpha})} = (5^{6})^{k} 5^{r_{6}(\alpha)}.$$
Busco, posibles valores para  $r_{6}(\alpha)$ : 
$$\frac{r_{6}(\alpha)}{r_{9}(5^{\alpha})} = (5^{6})^{k} 5^{r_{6}(\alpha)}.$$

$$\frac{1}{r_{9}(5^{\alpha})} = (5^{6})^{k} 5^{r_{6}(\alpha)}.$$
El PTF no me asegura que no haya un  $\alpha = (5^{6})$  of  $\alpha = 3 \ (11)$  of termateo en búsqueda de periodicidad 11 es primo,  $\alpha = (5^{6})^{k} 5^{r_{6}(\alpha)}.$ 
El PTF no me asegura que no haya un  $\alpha = (5^{6})^{k} 5^{r_{6}(\alpha)}.$ 

$$\frac{r_{10}(\alpha)}{r_{10}(\alpha)} = (5^{6})^{k} 5^{r_{6}(\alpha)}.$$
El PTF no me asegura que no haya un  $\alpha = (5^{6})^{k} 5^{r_{6}(\alpha)}.$ 

$$\frac{r_{10}(\alpha)}{r_{10}(\alpha)} = (5^{6})^{k} 5^{r_{6}(\alpha)}.$$
El sistema 
$$\frac{r_{10}(\alpha)}{r_{10}(\alpha)} = (5^{6})^{k} 5^{r_{10}(\alpha)}.$$
El sistema 
$$\frac{r_{10}(\alpha)}{r_{10}(\alpha)} = (5^{6})^{k} 5^{r_{10}(\alpha)$$

$r_{10}(\alpha)$	0	1	2	3	4	5
$r_{11}(5^{\alpha})$	1	5	3	4	9	1
non la tanta harr						

periodicidad de 5
$$5^{\alpha} \equiv 3 \ (11) \Leftrightarrow \boxed{\alpha \equiv 2 \ (5)} \quad \mathbf{v}$$

cumple para 
$$\alpha = 30k + 17 = \begin{cases} 17 & \text{si} \quad k = 0 \\ 47 & \text{si} \quad k = 1 \\ 77 & \text{si} \quad k = 2 \\ 107 & \text{si} \quad k = 3 \\ 137 & \text{si} \quad k = 4 \end{cases}$$
  $\rightarrow \boxed{\mathcal{D}_{+}(25^{70}) = \{5^{17}, 5^{47}, 5^{77}, 5^{107}, 5^{137}\}}$ 

## Falta hacerlo!

Si querés mandarlo: Telegram  $\to \bigcirc 3$ , o mejor aún si querés subirlo en  $\LaTeX \to \bigcirc 3$ .

#### Falta hacerlo!

Si querés mandarlo: Telegram  $\rightarrow \bigcirc \bigcirc$ , o mejor aún si querés subirlo en  $\LaTeX \rightarrow \bigcirc$ .

#### **\*** Falta hacerlo!

Si querés mandarlo: Telegram  $\rightarrow \bigcirc 3$ , o mejor aún si querés subirlo en  $\LaTeX \rightarrow \bigcirc 3$ .

#### Falta hacerlo!

Si querés mandarlo: Telegram  $\to \odot$ , o mejor aún si querés subirlo en  $\LaTeX \to \bigcirc$ .

## **\*** Falta hacerlo!

Si querés mandarlo: Telegram  $\to \odot$ , o mejor aún si querés subirlo en  $\LaTeX \to \bigcirc$ .

# 29. 🚼 Falta hacerlo!

Si querés mandarlo: Telegram  $\to \odot$ , o mejor aún si querés subirlo en LATEX  $\to \odot$ .

# 30. 😭 Falta hacerlo!

Si querés mandarlo: Telegram  $\to \odot$ , o mejor aún si querés subirlo en LATEX  $\to \odot$ .

#### Ejercicios extras:

Hallar los posibles restos de dividir a a por 70, sabiendo que  $(a^{1081} + 3a + 17:105) = 35$ 

$$\underbrace{(a^{1081} + 3a + 17)}_{m} : \underbrace{105}_{3 \cdot 5 \cdot 7} = \underbrace{35}_{5 \cdot 7} \xrightarrow{\text{debe ocurrix}} \begin{cases} 5 \mid m \\ y \\ 7 \mid m \\ y \\ 3 \nmid m \end{cases}$$

$$5 \mid m \to a^{1081} + 3a + \underbrace{17}_{\binom{5}{2}} \equiv 0 \ (5) \to \begin{cases} \text{si} \quad 5 \mid a \to 2 \equiv 0 \ (5) \Rightarrow a \not \equiv 0 \ (5) \end{cases}$$

$$\circ \text{si} \quad 5 \mid a \xrightarrow{a^{1081} = a(a^4)^{270}} \Rightarrow a + 3a + 2 \equiv 0 \ (5) \Rightarrow a \equiv 2 \ (5) \end{cases}$$

$$7 \mid m \to a^{1081} + 3a + \underbrace{17}_{\binom{5}{2}} \equiv 0 \ (7) \to \begin{cases} \text{si} \quad 7 \mid a \to 3 \equiv 0 \ (7) \Rightarrow a \not \equiv 0 \ (7) \end{cases} \Rightarrow a + 3a + 2 \equiv 0 \ (5) \Rightarrow a \equiv 2 \ (5) \end{cases}$$

$$3 \mid m \to a^{1081} + \underbrace{3a + 17}_{\binom{5}{2}} \equiv 0 \ (3) \to \begin{cases} \text{si} \quad 7 \mid a \xrightarrow{a^{1081} = a(a^6)^{180}} \Rightarrow a + 3a + 3 \equiv 0 \ (7) \to 4a \equiv -3 \ (7) \Rightarrow a \equiv 1 \ (7) \end{cases}$$

$$\circ \text{si} \quad 3 \mid a \to 2 \not \equiv 0 \ (3) \Rightarrow a \equiv 0 \ ($$

Sea  $a \in \mathbb{Z}$  tal que  $(a^{197} - 26:15) = 1$ . Hallar los posibles valores de  $(a^{97} - 36:135)$ 

Nota: No perder foco en que no hay que encontrar "para que a el mcd vale tanto", sino se pone más complicado en el final.

$$(a^{97} - 36: \overbrace{135}^{3^{3} \cdot 5}) = 3^{\alpha} \cdot 5^{\beta} \text{ con } \bigstar^{1} \left\{ \begin{array}{l} 0 \leq \alpha \leq 3 \\ 0 \leq \beta \leq 1 \end{array} \right\}.$$
  
Luego  $(a^{197} - 26: \underbrace{15}_{3 \cdot 5}) = 1$  se debe cumplir que:  $\left\{ \begin{array}{l} 5 \not \mid a^{197} - 26 \\ 3 \not \mid a^{197} - 26 \end{array} \right\}$ 

Análisis de  $(a^{197} - 26:15) = 1$ : Estudio la divisibilidad 5:

$$5 \not | a^{197} - 26 \iff a^{197} - 26 \not\equiv 0 (5) \iff a^{197} - 1 \not\equiv 0 (5) \xrightarrow{\text{analizo casos} \atop 5 \mid a \circ 5 \mid a}$$

**2** Errores? Mandá tu solución, entendible y coqueta, así corregimos.

$$a^{197} \not\equiv 1 \ (5) \Leftrightarrow \begin{cases} (\operatorname{rama} 5 \not\mid a) \xrightarrow{5 \text{ es primo}} a \cdot (\overbrace{a^4})^{49} \not\equiv 1 \ (5) \Leftrightarrow a \not\equiv 1 \ (5) \end{cases} \checkmark$$
$$(\operatorname{rama} 5 \mid a) \xrightarrow{5 \text{ es primo}} 0 \not\equiv 1 \ (5) \to a \equiv 0 \ (5)$$

Conclusión divisilidad 5:

Para que 
$$5 \text{ // } a^{197} - 26 \iff a \not\equiv 1 (5) \bigstar^2$$

Estudio la divisibilidad 3:

$$3 \not\mid a^{197} - 26 \iff a^{197} - 2 \not\equiv 0 \ (3) \iff a^{197} - 2 \not\equiv 0 \ (3) \xrightarrow{\text{analizo casos} \atop 3 \mid a \circ 3 \mid a}$$

$$a^{197} \not\equiv 2 \ (3) \Leftrightarrow \left\{ \begin{array}{l} (\operatorname{rama} \ 3 \not\mid a) \xrightarrow{3 \text{ es primo}} a \cdot (\overbrace{a^2})^{98} \not\equiv 2 \ (3) \Leftrightarrow a \not\equiv 2 \ (3) \\ (\operatorname{rama} \ 3 \mid a) \xrightarrow{3 \text{ es primo}} 0 \not\equiv 2 \ (3) \to a \equiv 0 \ (3) \end{array} \right.$$

Conclusión divisilidad 3:

Para que 
$$3 \nmid a^{197} - 26 \iff a \not\equiv 2 (3) \not\nearrow^3$$

Necesito que 
$$\left\{ \begin{array}{l} 3 \mid a^{97} - 36 : 135 \right)$$
:
$$\left\{ \begin{array}{l} 3 \mid a^{97} - 36 \\ \text{o bien,} \\ 5 \mid a^{97} - 36 \end{array} \right\}, \text{ para obtener valores distintos de 1 para el MCD.}$$

$$\left\{ \begin{array}{l} \text{Fatudio la divicibilidad 5. (avieta a \sqrt{2}^2 a \sqrt{3}^3)}, \end{array} \right\}$$

Estudio la divisibilidad 5 (sujeto a  $\star^2$  y  $\star^3$ ):

Si 
$$5 \mid a^{97} - 36 \iff a^{97} - 1 \equiv 0 \ (5) \iff a^{97} \equiv 1 \ (5) \xrightarrow{\text{analizo casos} \atop 5 \mid a \circ 5 \mid a}$$

$$a^{97} \equiv 1 \ (5) \Leftrightarrow \begin{cases} (\operatorname{rama} 5 \not | a) \xrightarrow{5 \text{ es primo}} a \cdot (a^4)^{24} \equiv 1 \ (5) \Leftrightarrow a \equiv 1 \ (5), \text{ absurdo con } \bigstar^2 \\ (\operatorname{rama} 5 | a) \xrightarrow{5 \text{ es primo}} 0 \equiv 1 \ (3) \to \text{ si } a \equiv 0 \ (5) \Rightarrow a^{97} \not\equiv 1 \ (5) \end{cases}$$

Conclusión divisilidad 5: 
$$5 \not\mid a^{97} - 36 \quad \forall a \in \mathbb{Z} \rightarrow \text{el MCD no puede tener un 5 en su factorización.}$$

Estudio la divisibilidad 3 (sujeto a  $\bigstar^2$  y  $\bigstar^3$ ):

$$3 \mid a^{97} - 36 \iff a^{97} \equiv 0 \ (3) \iff a^{97} \equiv 0 \ (3) \xrightarrow[3]{\text{analizo casos}}$$

$$a^{97} \equiv 0 \ (3) \Leftrightarrow \begin{cases} (\operatorname{rama} 3 \not | a) \xrightarrow{3 \text{ es primo}} a \cdot (a^2)^{48} \equiv 0 \ (3) \Leftrightarrow a \equiv 0 \ (3) \end{cases} \checkmark$$

$$(\operatorname{rama} 3 \mid a) \xrightarrow{3 \text{ es primo}} a \equiv 0 \ (3) \Leftrightarrow 0 \equiv 0 \ (3) \to \text{ si } a \equiv 0 \ (3) \Rightarrow a^{97} \equiv 0 \ (3)$$

Conclusión divisilidad 3:

$$3 \mid a^{97} - 36 \iff a \equiv 0 \ (3)^{*}$$

De  $\bigstar^1$  3 es un posible MCD, tengo que ver si  $3^2$  o  $3^3$  también dividen.

Estudio la divisibilidad 9 en a = 3k por  $\bigstar^4$ :

$$9 \mid (3k)^{97} - 36 \iff 3k^{97} \equiv 0 \ (9) \iff 3 \cdot (3^2)^{48} \cdot k^{97} \equiv 0 \ (9) \iff 0 \equiv 0 \ (9) \quad \checkmark \quad \forall k \in \mathbb{Z}$$

Conclusión divisilidad 9:

Conclusión divisilidad 9:
$$9 \mid a^{97} - 36 \text{ puede ser que } (a^{97} - 26:135) = 9$$

Estudio la divisibilidad 27 en 
$$a = 3k \text{ por } \star^4$$
:  
 $27 \mid (3k)^{97} - 36 \iff (3k)^{97} \equiv 9 \ (27) \iff 3 \cdot (3^3)^{32} \cdot k^{97} \equiv 9 \ (27) \iff 0 \equiv 9 \ (27)$ 

Conclusión divisilidad 27:

Si 
$$a \equiv 0 \ (3) \Rightarrow 27 \ / a^{97} - 36$$

Finalmente: el mcd es 9

#### Determinar todos los $n \in \mathbb{Z}$ tales que

$$(n^{433} + 7n + 91:931) = 133.$$

Expresar las soluciones mediante una única ecuación.

Para que se cumpla que  $(n^{433} + 7n + 91)$ : deben ocurrir las siguientes condiciones:

1: 
$$\underbrace{931}_{7^2 \cdot 19}$$
 =  $\underbrace{133}_{7 \cdot 19}$  deben ocurs
$$\begin{cases}
7 & | n^{433} + 7n + 91 \\
19 & | n^{433} + 7n + 91 \\
7^2 & | n^{433} + 7n + 91
\end{cases}$$

Si 
$$7 \mid n^{433} + 7n + 91 \iff n^{433} + 7n + 91 \equiv 0 \ (7) \iff n^{433} \equiv 0 \ (7) \xrightarrow[7]{\text{analizo casos}} 0$$

Estudio la divisibilidad 7:  
Si 
$$7 \mid n^{433} + 7n + 91 \iff n^{433} + 7n + 91 \equiv 0 \ (7) \iff n^{433} \equiv 0 \ (7) \xrightarrow{\text{analizo casos} \atop 7 \mid n \circ 7 \mid n}$$

$$\begin{cases}
\text{(rama } 7 \mid n) & \xrightarrow{\text{7 es primo}} \\
 & \text{1} & \text{1} & \text{2} & \text{2} & \text{3} & \text{3}$$

Conclusión divisibilidad 7:

$$7 \mid n^{433} + 7n + 91 \Leftrightarrow n \equiv 0 \ (7)$$

Estudio la divisibilidad  $7^2 = 49$ :

Si 
$$7^2 \nmid n^{433} + 7n + 91 \iff n^{433} + 7n + 91 \not\equiv 0 (49) \iff n^{433} + 7n + 42 \not\equiv 0 (49)$$

Estimato la divisionitada 
$$T = 49$$
.  
Si  $7^2 \not\mid n^{433} + 7n + 91 \iff n^{433} + 7n + 91 \not\equiv 0 \ (49) \iff n^{433} + 7n + 42 \not\equiv 0 \ (49)$ 

$$\xrightarrow{\text{de } \bigstar^1 \text{ tengo que}} (7k)^{433} + 7 \cdot 7k + 42 \not\equiv 0 \ (49) \Leftrightarrow 7 \cdot (49)^{216} \cdot k^{433} + 49k + 42 \not\equiv 0 \ (49) \Leftrightarrow 42 \not\equiv 0 \ (49)$$

Conclusión divisibilidad 49:

$$49 \not\mid n^{433} + 7n + 91 \quad \forall n \in \mathbb{Z}$$

Estudio la divisibilidad 19:

Estudio la divisibilidad 19:   
Si 19 | 
$$n^{433} + 7n + 91 \iff n^{433} + 7n + 91 \equiv 0 \ (19) \iff n^{433} + 7n + 15 \equiv 0 \ (19) \xrightarrow[19]{\text{analizo casos}} \underbrace{19 \mid n \text{ o } 19 \mid n} \underbrace{19 \text{ es primo}}_{19 \mid n} \underbrace{(n^{18})^{24} \cdot n + 7n + 15 \equiv 0 \ (19) \Leftrightarrow 8n \equiv -15 \ (19) \Leftrightarrow n \equiv 10 \ (19)$$
 
$$\underbrace{(\text{rama } 19 \mid n) \xrightarrow{19 \text{ es primo}}_{19 \mid n} (n^{18})^{24} \cdot n + 7n + 15 \equiv 0 \ (19) \Leftrightarrow 8n \equiv -15 \ (19) \Leftrightarrow n \equiv 10 \ (19)$$
 
$$\underbrace{(\text{rama } 19 \mid n) \xrightarrow{19 \text{ es primo}}_{19 \mid n} 15 \equiv 0 \ (19) \Rightarrow \text{ningún } n}_{19 \mid n} \underbrace{(\text{rama } 19 \mid n) \xrightarrow{19 \text{ es primo}}_{19 \mid n} 15 \equiv 0 \ (19) \Rightarrow \text{ningún } n}_{19 \mid n}$$

Conclusión divisibilidad 19:

$$19 \mid n^{433} + 7n + 91 \Leftrightarrow n \equiv 10 \ (19)$$

$$\begin{cases} \bigstar^{1} n \equiv 0 \text{ (7)} & \xrightarrow{7 \perp 19 \text{ hay solución por}} \\ \bigstar^{2} n \equiv 10 \text{ (19)} & \xrightarrow{\text{THC} \bigstar, \text{ digo TCHR}} \end{cases} \begin{cases} \overset{\bigstar^{2}}{\text{en} \bigstar^{1}} n = 7(19k + 10) = 133k + 70 \rightarrow \boxed{n \equiv 70 \text{ (133)}} \end{cases} \checkmark$$

**♦**4. Determinar para cada  $n \in \mathbb{N}$  el resto de dividir a  $8^{3^n-2}$  por 20.

Quiero encontrar  $r_{20}(8^{3^n-2})$  entonces analizo congruecia:

$$8^{3^{n}-2} \equiv X (20) \xrightarrow{\text{quebrar}} \begin{cases} 8^{3^{n}-2} \equiv 3^{3^{n}-2} (5) \bigstar^{1} \\ 8^{3^{n}-2} \equiv 0 (4) \rightarrow \forall n \in \mathbb{N} \end{cases}$$

Laburo con \*:

$$8^{3^{n}-2} \equiv \underbrace{3^{3^{n}-2}}_{(5)} (5)$$

$$\stackrel{(5)}{=}_{3^{r_{4}(3^{n}-2)}} \star^{2}$$

$$\star^{2} \xrightarrow{n \text{ impar}} \begin{cases} \text{si } n \text{ par } 3^{r_{4}(3^{n}-2)} \stackrel{(5)}{\equiv} 3^{1-2} \stackrel{(5)}{\equiv} 3^{3} \equiv 2 \text{ (5)} \\ \text{si } n \text{ impar } 3^{1} \stackrel{(5)}{\equiv} 3 \text{ (5)} \end{cases} \stackrel{(5)}{=} 3^{1-2} \stackrel{(5)}{\equiv} 3^{3} \equiv 2 \text{ (5)} \end{cases}$$

$$\begin{cases} 8^{3^{n}-2} \equiv 0 \text{ (4)} \star^{4} & \text{si } \forall n \in \text{naturales} \\ 8^{3^{n}-2} \equiv 2 \text{ (5)} \star^{5} & \text{si } n \equiv 0 \text{ (2)} \\ 8^{3^{n}-2} \equiv 3 \text{ (5)} \star^{6} & \text{si } n \equiv 1 \text{ (2)} \end{cases}$$

$$\text{Si } n \equiv 0 \text{ (2)} \overset{\star^{4}}{\star^{5}} \begin{cases} 8^{3^{n}-2} = 4j \rightarrow 4j \equiv 2 \text{ (5)} \Leftrightarrow j \equiv 3 \text{ (5)} \\ \Leftrightarrow j = 5k + 3 \Rightarrow 8^{3^{n}-2} = 4(5k + 3) \Leftrightarrow 8^{3^{n}-2} \equiv 12 \text{ (20)} \Leftrightarrow n \equiv 0 \text{ (2)}. \end{cases} \checkmark$$

$$\text{Se concluye que } \begin{cases} r_{20}(8^{3^{n}-2}) = 12 \text{ si } n \text{ par y } r_{20}(8^{3^{n}-2}) = 8 \text{ si } n \text{ impar con } n \in \mathbb{N} \end{cases}$$

**♦5.** Sea  $n \in \mathbb{N}$  tal que  $(n^{109} + 37 : 52) = 26$  y  $(n^{63} - 21 : 39) = 39$ . Calcular el resto de dividir a n por 156.

$$(n^{109} + 37 : \underbrace{52}_{13\cdot 2^2}) = \underbrace{26}_{13\cdot 2} y (n^{63} - 21 : \underbrace{39}_{13\cdot 3}) = \underbrace{39}_{13\cdot 3}.$$

Info de los MCD:

Para que  $(n^{109} + 37 : 52) = 26$  debe ocurrir que:

$$\begin{cases} 13 \mid n^{109} + 37 \\ 2 \mid n^{109} + 37 \\ 4 \not\mid n^{109} + 37 \end{cases}$$
 Para que  $(n^{63} - 21 : 39) = 39$  debe ocurrir que: 
$$\begin{cases} 13 \mid n^{63} - 21 \\ 3 \mid n^{63} - 21 \end{cases}$$

$$\begin{cases}
 n \equiv 1 & (2) \\
 n \equiv 2 & (13) \\
 n \not\equiv 3 & (4) \\
 n \equiv 0 & (3)
\end{cases}
\iff
\begin{cases}
 n \equiv 1 & (2) \\
 n \equiv 2 & (13) \\
 n \equiv 1 & (4) \\
 n \equiv 0 & (3)
\end{cases}
\iff
\begin{cases}
 n \equiv 2 & (13) \\
 n \equiv 1 & (4) \\
 n \equiv 0 & (3)
\end{cases}$$
Completar R:  $r_{156}(n) = 93$ 

**♦6.** Hallar el resto de la división de  $12^{2^n}$  por 7 para cada  $n \in \mathbb{N}$ 

R:

$$12^{2^n} \equiv 4 \ (7) \text{ si } n \text{ impar}$$

$$12^{2^n} \equiv 2 \ (7)$$
 si  $n$  par

pasar

Hallar todos los primos  $p \in \mathbb{N}$  tales que

$$3^{p^2+3} \equiv -84 \ (p) \ y \ (7p+8)^{2024} \equiv 4 \ (p).$$

A lo largo del ejercicio se va a usar fuerte el colorario del pequeño teorema de Fermat, 🐣

si p primo y 
$$p \not\mid a$$
, con  $a \in \mathbb{Z} \Rightarrow a^n \equiv a^{r_{p-1}}(p)$ 

$$3^{p^{2}+3} \equiv -84 \quad (p) \begin{cases} 3^{p^{2}+3} \stackrel{(p)}{\underset{\bigstar}{=}} 3^{r_{(p-1)}(p^{2}+3)} \\ \xrightarrow{\text{división}} p^{2} + 3 = (p-1)(p+1) + 4 \Rightarrow 3^{p^{2}+3} \stackrel{(p)}{\underset{\bigstar}{=}} 3^{4} \stackrel{\bigstar}{\underset{\$}{=}} 2^{2} \\ 3^{p^{2}+3} \equiv -84 \quad (p) \stackrel{\bigstar}{\Leftrightarrow} 81 \equiv -84 \quad (p) \Leftrightarrow 165 \equiv 0 \quad (p) \stackrel{p/3}{\underset{5\cdot 3\cdot 11}{=}} p = 5 \quad o \quad p = 11 \end{cases}$$

$$\xrightarrow{\text{caso}} \begin{cases} p \mid 3 \Leftrightarrow p = 3 \Rightarrow 3^{p^{2}+3} \stackrel{(3)}{\underset{\$}{=}} 0 \equiv -84 \quad (3) \Rightarrow p = 3 \end{cases}$$

Tengo entonces 3 posibles valores para  $p \in \{3, 5, 11\}$ . Los uso para ver cuál o cuáles verifican la segunda condición  $(7 \cdot p + 8)^{2024} \equiv 4 (p)$ .

Con p = 3:

$$(7 \cdot 3 + 8)^{2024} \stackrel{\text{(3)}}{=} 2^{2024} \stackrel{\text{(3)}}{=} 2^{r_2(2024)} \stackrel{\text{(3)}}{=} 2^0 \stackrel{\text{(3)}}{=} 1 \Rightarrow p = 3$$

Con p=5:

$$(7 \cdot 5 + 8)^{2024} \stackrel{\text{(5)}}{\equiv} 3^{2024} \stackrel{\text{(5)}}{\equiv} 3^{r_4(2024)} \stackrel{\text{(5)}}{\equiv} 3^0 \stackrel{\text{(5)}}{\equiv} 1 \not\equiv 4 \pmod{8}$$

Con p = 11:

$$(7 \cdot 11 + 8)^{2024} \stackrel{\text{(11)}}{\equiv} 8^{2024} \stackrel{\text{(11)}}{\equiv} 8^{r_{10}(2024)} \stackrel{\text{(11)}}{\equiv} 8^4 = \underbrace{4096}_{r_{11}(4096)=4} \equiv 4 \text{ (11)} \quad \checkmark$$
Por lo tanto los valores de  $p$  que cumplen lo pedido son: 
$$p = 3$$

$$y \qquad \checkmark \qquad 7 = 11$$

$$\begin{array}{|c|c|}
\hline
p = 3 \\
y \\
p = 11
\end{array}$$

Un coleccionista de obras de arte compró un lote compuesto por pinturas y dibujos. Cada pintura le costó 649 dólares y cada dibujo 132 dólares. Cuando el coleccionista llega a su casa no recuerda si gastó 9779 o 9780 dólares. Deducir cuánto le costó el lote y cuántas pinturas y dibujos compró.

Del enunciado se deduce que el coleccionista no sabe si gastó:

$$\begin{cases} 649P + 132D = 9779 \\ 0 \\ 649P + 132D = 9780 \end{cases}$$

Dos ecuaciones diofánticas que no pueden estar bien a la vez, porque el tipo gastó o 9779 o bien 9780, seguramente alguna no tenga solución. Let's see.

El  $(\underline{649}:\underline{132})=11$  tiene que dividir al número independiente. En este caso 11 / 9780 y 11 | 9779, así que gastó un total de 9779 dólares.

Lo que resta hacer es resolver la ecuación teniendo en cuenta que estamos trabajando con variables que modelan algo físico por lo que  $P \ge 0$  y  $D \ge 0$ .

$$649P + 132D = 9779 \stackrel{\text{comprimizar}}{\longleftrightarrow} 59P + 12D = 889.$$

Para buscar la solución particular uso a *Euclides*, dado que entre 2 números coprimos siempre podemos escribir al número una como una combinación entera.

$$\begin{cases} 59 = 4 \cdot 12 + 11 \\ 12 = 1 \cdot 11 + 1 \end{cases} \rightarrow 1 = 12 - 1 \cdot \underbrace{11}_{59 - 4 \cdot 12} = (-1) \cdot 59 + 5 \cdot 12. \text{ Por lo que se obtiene que:} \\ 1 = (-1) \cdot 59 + 5 \cdot 12 \xrightarrow{\times 889} \underbrace{889 = (-889) \cdot 59 + 4445 \cdot 12}_{Combineta\ entera\ buscada} \xrightarrow{\text{particular}} (P, D)_{\text{part}} = (-889, 4445).$$

La solución del homogéneo sale fácil. Sumo las soluciones y obtengo la solución general:

$$(P, D)_k = k \cdot (12, -59) + (-889, 4445) \quad \text{con } k \in \mathbb{Z}.$$

Observación totalmente innecesaria, pero está buena: Esa ecuación es una recta común y corriente. Si quiero puedo ahora encontrar algún punto más bonito, para expresarla distinto, por ejemplo si  $k = 75 \Rightarrow$  $(P,D)_{\text{part}} = (11,20)$ , lo cual me permite reescribir a la solución general como:

$$(P, D)_h = h \cdot (12, -59) + (11, 20) \quad \text{con } h \in \mathbb{Z}.$$

Fin de observación totalmente innecesaria, pero está buena.

La solución tiene que cumplir  $\bigstar^1$ :  $\begin{cases} P = 12h + 11 \ge 0 \iff h \ge -\frac{11}{12} \iff h \ge 0 \\ D = -59h + 20 \ge 0 \iff h \le \frac{20}{59} \iff h \le 0 \end{cases} \Leftrightarrow h = 0, \text{ Entonces: } (P, D) = (11, 20) \checkmark$ 

El coleccionista compró once pinturas y veinte dibujos.

Determinar todos los  $a \in \mathbb{Z}$  que satisfacen simultáneamente

$$\begin{cases} 3a \equiv 12 \ (24) \\ a \equiv 10 \ (30) \\ 20a \equiv 50 \ (125) \end{cases}$$

Ejercicio de sistema de ecuaciones de congreuencias. Los divisores no son coprimos 2 a 2, así que hay que coprimizar y quebrar y analizar lo que queda.

Recordar que siempre que se pueda hay que comprimizar:

$$\begin{cases} 3a \equiv 12 \ (24) \iff a \equiv 4 \ (8) \\ a \equiv 10 \ (30) \\ 20a \equiv 50 \ (125) \iff 4a \equiv 10 \ (25) \iff^{\times 6}_{\text{para } (\Leftarrow) \ 6 \ \perp \ 25} 24a \equiv 60 \ (25) \Leftrightarrow a \equiv 15 \ (25) \\ \begin{cases} 3a \equiv 12 \ (24) \\ a \equiv 10 \ (30) \\ 20a \equiv 50 \ (125) \end{cases} \iff \begin{cases} a \equiv 4 \ (8) \\ a \equiv 10 \ (30) \\ a \equiv 15 \ (25) \end{cases}$$

Todavía no tenemos los divisores coprimos 2 a 2. Ahora quebramo

$$\begin{cases} a \equiv 4 \ (8) & \checkmark \\ a \equiv 10 \ (30) & \longleftrightarrow \end{cases} \begin{cases} a \equiv 0 \ (2) & \checkmark \\ a \equiv 1 \ (3) \\ a \equiv 0 \ (5) & \checkmark \end{cases}$$
$$a \equiv 15 \ (25) & \checkmark \end{cases}$$

Observamos que todo es compatible. El  $\checkmark$  es porque 2 | 8 y 4  $\stackrel{(2)}{\equiv}$  0. El  $\checkmark$  sale de 5 | 25 y 15  $\stackrel{(5)}{\equiv}$  0. Me quedo con las ecuaciones de mayor divisor, dado que sino obtendría soluciones de más.

$$\begin{cases} a \equiv 4 \ (8) \\ a \equiv 10 \ (30) \\ a \equiv 15 \ (25) \end{cases} \longleftrightarrow \begin{cases} a \equiv 4 \ (8) \bigstar^{1} \\ a \equiv 1 \ (3) \bigstar^{2} \\ a \equiv 15 \ (25) \bigstar^{3} \end{cases}$$

Ahora logramos tener el sistema con los divisores coprimos 2 a 2. Por T≰R este sistema va a tener una

Anora logramos tener el sistema con los divisores coprimos 2 a 2. Por 1 k este sistema solución particular 
$$x_0 / 0 \le x_0 < \underbrace{3 \cdot 8 \cdot 25}_{600}$$

$$\begin{cases} \stackrel{\text{de}}{\underset{\text{to a}}{\Rightarrow}} a = 8k + 4 & \stackrel{\text{reemplazo a } a}{\underset{\text{en } \bigstar^2}{\Rightarrow}} 8k + 4 \equiv 1 \ (3) \Leftrightarrow k \equiv 0 \ (3) \Leftrightarrow k = 3j \\ \stackrel{\text{reemplazo } k}{\underset{\text{en } a = 8k + 4}{\Rightarrow}} a = 24j + 4 & \stackrel{\text{reemplazo a } a}{\underset{\text{en } \bigstar^3}{\Rightarrow}} 24j + 4 \equiv 15 \ (25) \Leftrightarrow j \equiv 14 \ (25) \Leftrightarrow j = 25h + 14 \end{cases}$$

$$\begin{cases} \stackrel{\text{reemplazo } j}{\underset{\text{en } a = 24j + 4}{\Rightarrow}} a = 600h + 340 \Leftrightarrow \boxed{a \equiv 340 \ (600)} \end{cases} \checkmark$$