

# Álgebra I

## Práctica 5 Resuelta

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

*Choose your destiny:*

*(doubleclick en los ejercicio para saltar)*

- [Notas teóricas](#)

- Ejercicios de la guía:

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

- Ejercicios Extras

 <a href="#">1.</a>	 <a href="#">3.</a>	 <a href="#">5.</a>	 <a href="#">7.</a>	 <a href="#">9.</a>
 <a href="#">2.</a>	 <a href="#">4.</a>	 <a href="#">6.</a>	 <a href="#">8.</a>	

**Notas teóricas:***Diofánticas:*

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

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

**¡Coprimitizar siempre que se pueda!**: Las soluciones de  $S$  son las mismas que las de  $S$  coprimitizado.

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

- Las solución general del sistema S coprimitizado :

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

*Ecuaciones de congruencia:*

- $aX \equiv c \pmod{b}$  con  $a, b \neq 0$

**¡Coprimitizar siempre que se pueda!**: Las soluciones de la ecuación original son las mismas que las de la ecuación coprimitizada.

$$aX \equiv c \pmod{b} \xleftrightarrow[\substack{c' = \frac{c}{(a:b)}}]{\substack{a' = \frac{a}{(a:b)} \text{ y } b' = \frac{b}{(a:b)}}} a'X \equiv c' \pmod{b'}$$

- 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:

$$aX \equiv c \pmod{b} \xleftrightarrow[\substack{d \perp b}]{daX \equiv dc \pmod{b}}$$

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

- Si te ponés a hacer cuentas en  $aX \equiv c \pmod{b}$  sin que  $a \perp b$ , la vas a cagar. Yo te avisé 🙌.

*Sistemas de ecuaciones de congruencia: Teorema chino del resto*

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

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

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

*Pequeño teorema de Fermat*

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

- 1)  $a^p \equiv a \pmod{p}$

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

- Sea  $p$  primo, entonces  $\forall a \in \mathbb{Z}$  tal que  $p \nmid a$  se tiene:

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

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  $\overbrace{(a:p)=1}^{p \nmid a}$ , y sea  $d \in \mathbb{N}$  con  $d \leq p-1$  el mínimo tal que:

$$a^d \equiv 1 \pmod{p} \Rightarrow d \mid (p-1)$$

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

*Nota:* Cuando  $p$  es primo y  $a$  un entero cualquiera, será obvio o no, pero:  $p \nmid a \Leftrightarrow p \perp a$ . Se usan indistintamente.

## Ejercicios de la guía:

## 1. 🤖... hay que hacerlo! 🤖

Si querés mandarlo: Telegram → 📧, o mejor aún si querés subirlo en L<sup>A</sup>T<sub>E</sub>X → 📄.

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

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

$$\left\{ \begin{array}{l} 4 \mid a \rightarrow a = 4k_1 \\ 8 \mid b \rightarrow b = 8k_2 \end{array} \right. \xrightarrow[33a + 9b = 120]{\text{meto en}} 132k_1 + 72k_2 = 120 \xrightarrow[\text{coprimizo}]{(132 : 72) = 12 \mid 120} 11k_1 + 6k_2 = 10$$

Busco solución particular con Euclides:

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

$\underbrace{-10}_{k_1} \quad \underbrace{20}_{k_2}$

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  $b$ :

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

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

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

3. 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  $A \geq 0$  y  $B \geq 0$ , dado que son productos 🧠.

$$\left\{ \begin{array}{l} 39A + 28B = 135 \\ \xleftrightarrow[(A : B) = 3]{\text{coprimizar}} \\ 13A + 16B = 45, \\ \text{tiene solución, ya que } \underbrace{(13 : 16)}_{=1} \mid 45 \\ \xrightarrow{\text{sale a ojo}} \\ \boxed{(A, B) = (1, 2)} \end{array} \right.$$

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

$$\text{i) } 17X \equiv 3 \pmod{11} \quad \text{ii) } 56X \equiv 28 \pmod{35} \quad \text{iii) } 56X \equiv 2 \pmod{884} \quad \text{iv) } 78X \equiv 30 \pmod{12126}$$

$$\text{i) } 17X \equiv 3 \pmod{11} \iff 6X \equiv 3 \pmod{11} \xleftrightarrow[(\Leftarrow) 2 \perp 11]{\times 2} X \equiv 6 \pmod{11} \quad \checkmark$$

$$\text{ii) } 56X \equiv 28 \pmod{35} \iff 21X \equiv 28 \pmod{35} \xleftrightarrow[(21 : 35) = 7]{\text{coprimizo}} 3X \equiv 4 \pmod{5} \xleftrightarrow[7 \perp 5]{\times 7} X \equiv 3 \pmod{5} \quad \checkmark$$

$$\text{iii) } 56X \equiv 2 \pmod{884} \iff 28X \equiv 1 \pmod{442} \text{ tiene solución } \xleftrightarrow[\text{pero } 2 \nmid 1]{(28 : 442) \mid 1} X = \emptyset \quad \checkmark$$

iv)

$$78X \equiv 30 \pmod{12126} \xleftrightarrow[(78:12126)=6]{\text{coprimizar}} 13X \equiv 5 \pmod{2021},$$

1  
*dado que  $(13 : 2021) \mid 5$  hay solución.*

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

$$\begin{aligned} \begin{cases} 2021 = 13 \cdot 155 + 6 \\ 13 = 6 \cdot 2 + 1 \end{cases} & \xrightarrow[\text{de 13 y 2021}]{1 \text{ como combinación}} 1 = 13 \cdot 311 + 2021 \cdot (-2) \\ 1 = 13 \cdot 311 + 2021 \cdot (-2) & \xrightarrow[(\Leftarrow) 5 \perp 2021]{\times 5} 5 = 13 \cdot 1555 + 2021 \cdot (-10) \\ 13 \cdot \underbrace{1555}_{\text{Solución particular}} = 2021 \cdot 10 + 5 & \xrightarrow[\text{Solución general}]{!!} \boxed{X \equiv 1555 \pmod{2021}} \quad \checkmark \end{aligned}$$

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

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

Este es parecido al 2.

$$b \equiv 2a \pmod{5} \iff b = 5k + 2a \xrightarrow[28a + 10b = 26]{\text{meto en}} 48a + 50k = 26 \xrightarrow[2 \mid 26]{(48 : 59) = 2} 24a + 25k = 13 \xrightarrow[\text{ojo}]{a} \begin{cases} a = -13 + (-25)q \\ k = 13 + 24q \end{cases}$$

Let's corroborate:

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

6. 🙄... hay que hacerlo! 🙄

Si querés mandarlo: Telegram → , o mejor aún si querés subirlo en L<sup>A</sup>T<sub>E</sub>X → .

7. 🙄... hay que hacerlo! 🙄

Si querés mandarlo: Telegram → , o mejor aún si querés subirlo en L<sup>A</sup>T<sub>E</sub>X → .

8. 🙄... hay que hacerlo! 🙄

Si querés mandarlo: Telegram → , o mejor aún si querés subirlo en L<sup>A</sup>T<sub>E</sub>X → .

9. 🙄... hay que hacerlo! 🙄

Si querés mandarlo: Telegram → , o mejor aún si querés subirlo en L<sup>A</sup>T<sub>E</sub>X → .

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

$$\text{i) } \begin{cases} \star^1 a \equiv 3 \pmod{10} \\ \star^2 a \equiv 2 \pmod{7} \\ \star^3 a \equiv 5 \pmod{9} \end{cases}$$

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

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

$$\xrightarrow[a]{\text{actualizo}} a = 10 \cdot \underbrace{(7q + 2)}_k + 3 = 70q + 23 \stackrel{(9)}{\equiv} 7q \stackrel{(\star^3)}{\equiv} 5 \pmod{9} \xrightarrow[7 \perp 9]{\text{usando que}} q \equiv 0 \pmod{9} \rightarrow q = 9j$$

$$\xrightarrow[a]{\text{actualizo}} a = 70 \underbrace{(9j)}_q + 23 = 630j + 23 \rightarrow \boxed{a \equiv 23 \pmod{630}} \quad \checkmark$$

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)

$$\text{iii)} \quad \begin{cases} \star^1 a \equiv 1 \pmod{12} \\ \star^2 a \equiv 7 \pmod{10} \\ \star^3 a \equiv 4 \pmod{9} \end{cases}$$

11. 🙄... hay que hacerlo! 🙄

Si querés mandarlo: Telegram → , o mejor aún si querés subirlo en L<sup>A</sup>T<sub>E</sub>X → .

12. 🙄... hay que hacerlo! 🙄

Si querés mandarlo: Telegram → , o mejor aún si querés subirlo en L<sup>A</sup>T<sub>E</sub>X → .

13. 🙄... hay que hacerlo! 🙄

Si querés mandarlo: Telegram → , o mejor aún si querés subirlo en L<sup>A</sup>T<sub>E</sub>X → .

14. 🙄... hay que hacerlo! 🙄

Si querés mandarlo: Telegram → , o mejor aún si querés subirlo en L<sup>A</sup>T<sub>E</sub>X → .

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

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

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

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

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

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

$$\xrightarrow[p \nmid 8]{p \nmid 7} a \equiv 5 \cdot 7^3 + 3 \cdot 8^6 \pmod{13} \rightarrow a \equiv 5 \cdot (-6^3 + 3 \cdot 5^5) \pmod{13} \quad \text{consultar}$$

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

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

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

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

🙄... hay que hacerlo! 🙄

Si querés mandarlo: Telegram → , o mejor aún si querés subirlo en L<sup>A</sup>T<sub>E</sub>X → .

17. Probar que para todo  $a \in \mathbb{Z}$  vale

i)  $728 \mid a^{27} - a^3$

ii)  $\frac{2a^7}{35} + \frac{a}{7} - \frac{a^3}{5} \in \mathbb{Z}$

i)  $728 = 2^3 \cdot 7 \cdot 13$

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

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

$$\left\{ \begin{array}{l} 2 \mid a^{27} - a^3 \xrightarrow{2 \nmid a} \underbrace{\binom{a}{2}}_{\equiv 1}^{27} - \underbrace{\binom{a}{2}}_{\equiv 1}^3 \equiv 0 \pmod{2} \Rightarrow 2 \mid a^{27} - a^3 \\ 2k \mid a^{27} - a^3 \Leftrightarrow (2k)^{27} - (2k)^3 \equiv 0 \pmod{8} \Leftrightarrow 2^3 \cdot \underbrace{\binom{2^3}{8}}_{\equiv 0}^8 \cdot k^{27} - \underbrace{2^3}_{\equiv 0} \cdot k^3 \equiv 0 \pmod{8} \quad \checkmark \\ 3 \mid a^{27} - a^3 \Leftrightarrow 3^{27} - 3^3 \equiv 0 \pmod{8} \Leftrightarrow \underbrace{\binom{3^2}{8}}_{\equiv 0}^{13} \cdot 3 - \underbrace{3^2}_{\equiv 0} \cdot 3 \equiv 0 \pmod{8} \quad \checkmark \\ 8 \mid a^{27} - a^3 \Leftrightarrow \left\{ \begin{array}{l} 5 \mid a^{27} - a^3 \Leftrightarrow 5^{27} - 5^3 \equiv 0 \pmod{8} \Leftrightarrow \underbrace{\binom{5^2}{8}}_{\equiv 1}^{13} \cdot 5 - \underbrace{5^2}_{\equiv 1} \cdot 5 \equiv 0 \pmod{8} \quad \checkmark \\ 7 \mid a^{27} - a^3 \Leftrightarrow 7^{27} - 7^3 \equiv 0 \pmod{8} \Leftrightarrow \underbrace{\binom{7}{8}}_{\equiv 1}^{27} - \underbrace{7^3}_{\equiv 1} \equiv 0 \pmod{8} \quad \checkmark \end{array} \right. \\ 7 \mid a^{27} - a^3 \Leftrightarrow a^{27} - a^3 \equiv 0 \pmod{7} \xrightarrow[\text{caso } 7 \nmid a]{7 \text{ primo}} a^{27} - a^3 \equiv 0 \pmod{7} \Leftrightarrow a^3 - a^3 \equiv 0 \pmod{7} \quad \checkmark \\ 13 \mid a^{27} - a^3 \Leftrightarrow a^{27} - a^3 \equiv 0 \pmod{13} \xrightarrow[\text{caso } 13 \nmid a]{13 \text{ primo}} a^{27} - a^3 \equiv 0 \pmod{13} \Leftrightarrow a^3 - a^3 \equiv 0 \pmod{13} \quad \checkmark \end{array} \right.$$

18. 🙄... hay que hacerlo! 🙄

Si querés mandarlo: Telegram → , o mejor aún si querés subirlo en L<sup>A</sup>T<sub>E</sub>X → .

19. 🙄... hay que hacerlo! 🙄

Si querés mandarlo: Telegram → , o mejor aún si querés subirlo en L<sup>A</sup>T<sub>E</sub>X → .

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) 🙄... hay que hacerlo! 🙄

Si querés mandarlo: Telegram → , o mejor aún si querés subirlo en L<sup>A</sup>T<sub>E</sub>X → .

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

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

Primero estudio la ecuación de módulo 7:

$$\begin{cases} \sum_{i=1}^{1759} i^{42} \equiv X \pmod{7} \quad \star^1 \xrightarrow[\text{si } p \nmid i \rightarrow i^{42} = (i^6)^7 \equiv 1 \pmod{7}]{7 \text{ es primo, uso Fermat}} \sum_{i=1}^{1759} i^{42} = \sum_{i=1}^{1759} (i^6)^7 \xrightarrow{251 \cdot 7 + 2 = 1759} \\ \sum_{i=1}^{1759} (i^6)^7 \stackrel{(7)}{\equiv} 251 \cdot ((1^6)^7 + (2^6)^7 + (3^6)^7 + (4^6)^7 + (5^6)^7 + (6^6)^7 + (7^6)^7) + ((1^6)^7 + (2^6)^7 + (3^6)^7 + (4^6)^7) \\ \sum_{i=1}^{1759} (i^6)^7 \stackrel{(7)}{\equiv} 251 \cdot (1 + 1 + 1 + 1 + 1 + 1 + 0) + (1 + 1 + 1 + 1) = 251 \cdot 6 + 4 \stackrel{(7)}{\equiv} 3 \\ \xrightarrow{\star^1} \boxed{X \equiv 3 \pmod{7}} \end{cases}$$

Ahora se labura el módulo 8.

$$\begin{cases} \sum_{i=1}^{1759} i^{42} \equiv X \pmod{8} \xrightarrow[\text{no uso Fermat}]{8 \text{ no es primo}} \text{Análisis a mano} \xrightarrow{219 \cdot 8 + 7 = 1759} X \equiv \sum_{i=1}^{1759} i^{42} \pmod{8} \stackrel{(8)}{\equiv} \\ \stackrel{(8)}{\equiv} 219 \cdot \underbrace{(1^{42} + 2^{42} + 3^{42} + 4^{42} + 5^{42} + 6^{42} + 7^{42} + 0^{42})}_{8 \text{ términos: } r_8(i^{42}) = (r_8(i))^{42}} + (1^{42} + 2^{42} + 3^{42} + 4^{42} + 5^{42} + 6^{42} + 7^{42}) \\ \rightarrow \left\{ \begin{array}{l} 2^{42} = (2^3)^{14} \stackrel{(8)}{\equiv} 0 \\ 4^{42} = (2^3)^{14} \cdot (2^3)^{14} \stackrel{(8)}{\equiv} 0 \\ 6^{42} = (2^3)^{14} \cdot 3^{42} \stackrel{(8)}{\equiv} 0 \\ 1^{42} = 1 \\ 3^{42} = (3^2)^{21} \stackrel{(8)}{\equiv} 1^{21} = 1 \\ 5^{42} = (5^2)^{21} \stackrel{(8)}{\equiv} 1^{21} = 1 \\ 7^{42} = (7^2)^{21} \stackrel{(8)}{\equiv} 1^{21} = 1 \end{array} \right\} \\ \xrightarrow[\text{esa en}]{\text{reemplazo}} \sum_{i=1}^{1759} i^{42} \stackrel{(8)}{\equiv} 219 \cdot 4 + 4 = 880 \stackrel{(8)}{\equiv} 0 \rightarrow \boxed{X \equiv 0 \pmod{8}} \end{cases}$$

El sistema  $\begin{cases} X \equiv 3 \pmod{7} \\ X \equiv 0 \pmod{8} \end{cases}$  tiene solución  $X \equiv 24 \pmod{56}$ , por lo tanto el *resto pedido*:  $r_{56} \left( \sum_{i=1}^{1759} i^{42} \right) = 24$

21. 🤔... hay que hacerlo! 🏠

Si querés mandarlo: Telegram → , o mejor aún si querés subirlo en L<sup>A</sup>T<sub>E</sub>X → .

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

$$\begin{aligned} 7X^{45} &\equiv 1 \pmod{46} \xrightarrow[13]{\text{multiplico por}} 91X^{45} \equiv 13 \pmod{46} \rightarrow X^{45} \equiv -13 \pmod{46} \rightarrow X^{45} \equiv 33 \pmod{46} \\ &\rightarrow \begin{cases} X^{45} \equiv 33 \pmod{23} \rightarrow X^{45} \equiv 10 \pmod{23} \xrightarrow[X^{22} \equiv 1 \pmod{23}]{23 \text{ primo y } 23 \nmid X} X^{22} X^{22} X^1 \stackrel{(23)}{\equiv} X \equiv 10 \pmod{23} \\ X^{45} \equiv 10 \pmod{2} \rightarrow X^{45} \equiv 0 \pmod{2} \xrightarrow[\text{si mismo impar veces}]{X \text{ multiplicado por}} X \equiv 0 \pmod{2} \end{cases} \end{aligned}$$

La ecuación de congruencia  $\boxed{X \equiv 10 \pmod{46}}$  cumple las condiciones encontradas.

23. 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:  $\begin{cases} 25^{70} \equiv 0 \pmod{d} \rightarrow 5^{140} \equiv 0 \pmod{d} \\ d \equiv 2 \pmod{9} \\ d \equiv 3 \pmod{11} \end{cases}$ . De la primera ecuación queda que el divisor

$$d = 5^\alpha \text{ con } \alpha \text{ compatible con las otras ecuaciones.} \rightarrow \begin{cases} 5^\alpha \equiv 2 \pmod{9} \\ 5^\alpha \equiv 3 \pmod{11} \end{cases}$$

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

$$\left. \begin{array}{l} \text{Busco} \\ 5^\alpha \equiv 1 \end{array} \right\} \begin{cases} 5^\alpha \equiv 2 \pmod{9} \\ 5^3 \equiv -1 \pmod{9} \Leftrightarrow 5^6 \equiv 1 \pmod{9} \Leftrightarrow 5^{6k+r_6(\alpha)} = \overbrace{5^6}^{(9) \equiv 1}{}^k 5^{r_6(\alpha)}. \\ \text{Busco, posibles valores para } r_6(\alpha): \begin{array}{|c|c|c|c|c|c|c|} \hline r_6(\alpha) & 0 & 1 & 2 & 3 & 4 & 5 \\ \hline r_9(5^\alpha) & 1 & 5 & 7 & 8 & 4 & 2 \\ \hline \end{array} \\ \text{por lo tanto} \rightarrow \text{para que } 5^\alpha \equiv 2 \pmod{9} \Leftrightarrow \boxed{\alpha \equiv 5 \pmod{6}} \quad \checkmark \\ \hline 5^\alpha \equiv 3 \pmod{11} \xrightarrow[\text{periodicidad 11 es primo, } 11 \nmid 5]{\text{fermateo en búsqueda de}} 5^{10} \equiv 1 \pmod{11} \\ \text{El PTF no me asegura que no haya un } \alpha < 10 \text{ que también cumpla } 5^\alpha \equiv 1 \pmod{11} \\ \begin{array}{|c|c|c|c|c|c|c|} \hline r_{10}(\alpha) & 0 & 1 & 2 & 3 & 4 & 5 \\ \hline r_{11}(5^\alpha) & 1 & 5 & 3 & 4 & 9 & 1 \\ \hline \end{array} \\ \text{por lo tanto hay} \rightarrow \text{Se obtiene entoncees:} \\ \text{periodicidad de 5} \\ 5^\alpha \equiv 3 \pmod{11} \Leftrightarrow \boxed{\alpha \equiv 2 \pmod{5}} \quad \checkmark \end{cases}$$

El sistema  $\begin{cases} \alpha \equiv 5 \pmod{6} \\ \alpha \equiv 2 \pmod{5} \end{cases}$  6 y 5 son coprimos, se resuelve para  $\alpha \equiv 17 \pmod{30}$  y además  $0 < \alpha \leq 140$  lo que se

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

#### 24. 🤖... hay que hacerlo! 🤖

Si querés mandarlo: Telegram → , o mejor aún si querés subirlo en L<sup>A</sup>T<sub>E</sub>X → .

#### 25. 🤖... hay que hacerlo! 🤖

Si querés mandarlo: Telegram → , o mejor aún si querés subirlo en L<sup>A</sup>T<sub>E</sub>X → .

#### 26. 🤖... hay que hacerlo! 🤖

Si querés mandarlo: Telegram → , o mejor aún si querés subirlo en L<sup>A</sup>T<sub>E</sub>X → .

#### 27. 🤖... hay que hacerlo! 🤖

Si querés mandarlo: Telegram → , o mejor aún si querés subirlo en L<sup>A</sup>T<sub>E</sub>X → .

#### 28. 🤖... hay que hacerlo! 🤖

Si querés mandarlo: Telegram → , o mejor aún si querés subirlo en L<sup>A</sup>T<sub>E</sub>X → .

#### 29. 🤖... hay que hacerlo! 🤖

Si querés mandarlo: Telegram → , o mejor aún si querés subirlo en L<sup>A</sup>T<sub>E</sub>X → .

**30.** 😬... hay que hacerlo! 😬

Si querés mandarlo: Telegram → 📎, o mejor aún si querés subirlo en  $\text{L}^{\text{A}}\text{T}_{\text{E}}\text{X}$  → 📄.

---

## Ejercicios extras:

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

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

$$5 \mid m \rightarrow a^{1081} + 3a + \underbrace{17}_{\substack{(5) \\ \equiv 2}} \equiv 0 \pmod{5} \rightarrow \begin{cases} \text{si } 5 \mid a \rightarrow 2 \equiv 0 \pmod{5} \Rightarrow a \not\equiv 0 \pmod{5} \\ \text{o} \\ \text{si } 5 \nmid a \xrightarrow[5 \text{ primo y } 5 \nmid a]{a^{1081} = a(a^4)^{270}} a + 3a + 2 \equiv 0 \pmod{5} \Rightarrow \boxed{a \equiv 2 \pmod{5}} \end{cases}$$

$$7 \mid m \rightarrow a^{1081} + 3a + \underbrace{17}_{\substack{(7) \\ \equiv 3}} \equiv 0 \pmod{7} \rightarrow \begin{cases} \text{si } 7 \mid a \rightarrow 3 \equiv 0 \pmod{7} \Rightarrow a \not\equiv 0 \pmod{7} \\ \text{o} \\ \text{si } 7 \nmid a \xrightarrow[7 \text{ primo y } 7 \nmid a]{a^{1081} = a(a^6)^{180}} a + 3a + 3 \equiv 0 \pmod{7} \rightarrow 4a \equiv -3 \pmod{7} \Rightarrow \boxed{a \equiv 1 \pmod{7}} \end{cases}$$

$$3 \nmid m \rightarrow a^{1081} + \underbrace{3a}_{=0} + \underbrace{17}_{\substack{(3) \\ \equiv 2}} \not\equiv 0 \pmod{3} \rightarrow \begin{cases} \text{si } 3 \mid a \rightarrow 2 \not\equiv 0 \pmod{3} \Rightarrow a \equiv 0 \pmod{3} \\ \text{o} \\ \text{si } 3 \nmid a \xrightarrow[3 \text{ primo y } 3 \nmid a]{a^{1081} = a(a^2)^{540}} a + 2 \not\equiv 0 \pmod{3} \Rightarrow \begin{cases} a \not\equiv 1 \pmod{3} \\ a \not\equiv 0 \pmod{3} \end{cases} \Rightarrow \boxed{a \equiv 2 \pmod{3}} \end{cases}$$

Las condiciones marcan 2 sistemas:

$$\begin{cases} a \equiv 2 \pmod{5} \\ a \equiv 1 \pmod{7} \\ a \equiv 0 \pmod{3} \end{cases} \rightarrow \boxed{a \equiv 22 \pmod{105}} \qquad \begin{cases} a \equiv 2 \pmod{5} \\ a \equiv 1 \pmod{7} \\ a \equiv 2 \pmod{3} \end{cases} \rightarrow \boxed{a \equiv 92 \pmod{105}}$$

Veo que para el conjunto de posibles  $a$   $\begin{cases} a = 105k_1 + 22 \\ \text{o} \\ a = 105k_2 + 92 \end{cases} \xrightarrow[\equiv (70)]{\text{calculo}} a \equiv 22 \pmod{35}$

$\xrightarrow[\text{pedidos del enunciado}]{\text{quiero los restos}} r_{70}(a) = \{22, 57\}$ , valores de  $a$  que cumplan condición de  $r_{70}(a)$  ✓

2. 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.

$$(a^{97} - 36 : \overbrace{135}^{3^3 \cdot 5}) = 3^\alpha \cdot 5^\beta \text{ con } \star^1 \left\{ \begin{array}{l} 0 \leq \alpha \leq 3 \\ 0 \leq \beta \leq 1 \end{array} \right\}.$$

Luego  $(a^{197} - 26 : \underbrace{15}_{3 \cdot 5}) = 1$  se debe cumplir que:  $\begin{cases} 5 \nmid a^{197} - 26 \\ 3 \nmid a^{197} - 26 \end{cases}$

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

$$5 \nmid a^{197} - 26 \iff a^{197} - 26 \not\equiv 0 \pmod{5} \iff a^{197} - 1 \not\equiv 0 \pmod{5} \xrightarrow[5 \mid a \text{ o } 5 \nmid a]{\text{analizo casos}}$$

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

Conclusión divisibilidad 5:

Para que  $5 \nmid a^{197} - 26 \iff a \not\equiv 1 (5) \star^2$

Estudio la divisibilidad 3:

$$3 \nmid a^{197} - 26 \iff a^{197} - 2 \not\equiv 0 (3) \iff a^{197} - 2 \not\equiv 0 (3) \xrightarrow[3 \mid a \text{ o } 3 \nmid a]{\text{analizo casos}}$$

$$a^{197} \not\equiv 2 (3) \Leftrightarrow \begin{cases} (\text{rama } 3 \nmid a) \xrightarrow[3 \nmid a]{3 \text{ es primo}} a \cdot \overbrace{(a^2)^{98}}^{(3) \equiv 1} \not\equiv 2 (3) \Leftrightarrow a \not\equiv 2 (3) \quad \checkmark \\ (\text{rama } 3 \mid a) \xrightarrow[3 \mid a]{3 \text{ es primo}} 0 \not\equiv 2 (3) \rightarrow a \equiv 0 (3) \end{cases}$$

Conclusión divisibilidad 3:

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

Análisis de  $(a^{97} - 36 : 135)$ :

Necesito que  $\begin{cases} 3 \mid a^{97} - 36 \\ \text{o bien,} \\ 5 \mid a^{97} - 36 \end{cases}$ , para obtener valores distintos de 1 para el MCD.

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

$$\text{Si } 5 \mid a^{97} - 36 \iff a^{97} - 1 \equiv 0 (5) \iff a^{97} \equiv 1 (5) \xrightarrow[5 \mid a \text{ o } 5 \nmid a]{\text{analizo casos}}$$

$$a^{97} \equiv 1 (5) \Leftrightarrow \begin{cases} (\text{rama } 5 \nmid a) \xrightarrow[5 \nmid a]{5 \text{ es primo}} a \cdot \overbrace{(a^4)^{24}}^{(5) \equiv 1} \equiv 1 (5) \Leftrightarrow a \equiv 1 (5), \text{ absurdo con } \star^2 \text{ ☠} \\ (\text{rama } 5 \mid a) \xrightarrow[5 \mid a]{5 \text{ es primo}} 0 \equiv 1 (3) \rightarrow \text{si } a \equiv 0 (5) \Rightarrow a^{97} \not\equiv 1 (5) \end{cases}$$

Conclusión divisibilidad 5:

$5 \nmid a^{97} - 36 \quad \forall a \in \mathbb{Z} \rightarrow$  el MCD no puede tener un 5 en su factorización.

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

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

$$a^{97} \equiv 0 (3) \Leftrightarrow \begin{cases} (\text{rama } 3 \nmid a) \xrightarrow[3 \nmid a]{3 \text{ es primo}} a \cdot \overbrace{(a^2)^{48}}^{(3) \equiv 1} \equiv 0 (3) \Leftrightarrow a \equiv 0 (3) \quad \checkmark \\ (\text{rama } 3 \mid a) \xrightarrow[3 \mid a]{3 \text{ es primo}} a \equiv 0 (3) \Leftrightarrow 0 \equiv 0 (3) \rightarrow \text{si } a \equiv 0 (3) \Rightarrow a^{97} \equiv 0 (3) \end{cases}$$

Conclusión divisibilidad 3:

$3 \mid a^{97} - 36 \iff a \equiv 0 (3) \star^4$

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

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

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

Conclusión divisibilidad 9:

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

Estudio la divisibilidad 27 en  $a = 3k$  por  $\star^4$ :

$$27 \mid (3k)^{97} - 36 \iff (3k)^{97} \equiv 9 \pmod{27} \iff 3 \cdot (3^3)^{32} \cdot k^{97} \equiv 9 \pmod{27} \iff 0 \equiv 9 \pmod{27}$$

Conclusión divisibilidad 27:

$$\text{Si } a \equiv 0 \pmod{3} \Rightarrow 27 \nmid a^{97} - 36$$

Finalmente: el mcd es 9

 3. 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  $(n^{433} + 7n + 91 : \underbrace{931}_{7^2 \cdot 19}) = \underbrace{133}_{7 \cdot 19}$  deben ocurrir las siguientes condiciones:

$$\begin{cases} 7 \mid n^{433} + 7n + 91 \\ 19 \mid n^{433} + 7n + 91 \\ 7^2 \nmid n^{433} + 7n + 91 \end{cases}$$

Estudio la divisibilidad 7:

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

$$n^{433} \equiv 0 \pmod{7} \Leftrightarrow \begin{cases} (\text{rama } 7 \nmid n) \xrightarrow[7 \nmid n]{7 \text{ es primo}} (\underbrace{n^6}_{\equiv 1})^{72} \cdot n \equiv 0 \pmod{7} \Leftrightarrow n \equiv 0 \pmod{7}, \text{ pero esta rama } 7 \nmid n \rightarrow \text{💀} \\ (\text{rama } 7 \mid n) \xrightarrow[7 \mid n]{7 \text{ es primo}} 0 \equiv 0 \pmod{7} \text{ y como esta rama } 7 \mid n \rightarrow \boxed{n \equiv 0 \pmod{7}} \quad \checkmark \star^1 \end{cases}$$

Conclusión divisibilidad 7:

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

Estudio la divisibilidad  $7^2 = 49$ :

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

$$\xrightarrow[n \equiv 0 \pmod{7} \Leftrightarrow n = 7k]{\text{de } \star^1 \text{ tengo que}} (7k)^{433} + 7 \cdot 7k + 42 \not\equiv 0 \pmod{49} \Leftrightarrow 7 \cdot (49)^{216} \cdot k^{433} + 49k + 42 \not\equiv 0 \pmod{49} \Leftrightarrow 42 \not\equiv 0 \pmod{49}$$

Conclusión divisibilidad 49:

$$49 \nmid n^{433} + 7n + 91 \quad \forall n \in \mathbb{Z}$$

Estudio la divisibilidad 19:

$$\text{Si } 19 \mid n^{433} + 7n + 91 \iff n^{433} + 7n + 91 \equiv 0 \pmod{19} \iff n^{433} + 7n + 15 \equiv 0 \pmod{19} \xrightarrow[19 \mid n \text{ o } 19 \nmid n]{\text{analizo casos}}$$

$$n^{433} + 7n + 15 \equiv 0 \pmod{19} \Leftrightarrow \begin{cases} (\text{rama } 19 \nmid n) \xrightarrow[19 \nmid n]{19 \text{ es primo}} (\underbrace{n^{18}}_{\equiv 1})^{24} \cdot n + 7n + 15 \equiv 0 \pmod{19} \Leftrightarrow 8n \equiv -15 \pmod{19} \Leftrightarrow \\ \xrightarrow{\times 7} \boxed{n \equiv 10 \pmod{19}} \quad \checkmark \star^2 \\ (\text{rama } 19 \mid n) \xrightarrow[19 \mid n]{19 \text{ es primo}} 15 \equiv 0 \pmod{19} \rightarrow \text{ningún } n \end{cases}$$

Conclusión divisibilidad 19:

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

$$\left\{ \begin{array}{l} \star^1 n \equiv 0 \pmod{7} \\ \star^2 n \equiv 10 \pmod{19} \end{array} \right. \xrightarrow[\text{THC } \star, \text{ digo TCHR}]{7 \perp 19 \text{ hay solución por}} \left\{ \begin{array}{l} \star^2 \\ \text{en } \star^1 \end{array} \right. \rightarrow n = 7(19k + 10) = 133k + 70 \rightarrow \boxed{n \equiv 70 \pmod{133}} \quad \checkmark$$

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 congruencia:

$$8^{3^n-2} \equiv X \pmod{20} \xrightarrow{\text{quebrar}} \left\{ \begin{array}{l} 8^{3^n-2} \equiv 3^{3^n-2} \pmod{5} \star^1 \\ 8^{3^n-2} \equiv 0 \pmod{4} \rightarrow \forall n \in \mathbb{N} \end{array} \right.$$

Laburo con  $\star^1$ :

$$8^{3^n-2} \equiv \underbrace{3^{3^n-2}}_{\stackrel{(5)}{\equiv} 3^{r_4(3^n-2)} \star^2} \pmod{5}$$

$$\xrightarrow{\star^2} 3^{r_4(3^n-2)} \xrightarrow[n \text{ impar}]{n \text{ par}} \left\{ \begin{array}{l} \text{si } n \text{ par } 3^{r_4(3^n-2)} \stackrel{(5)}{\equiv} 3^{1-2} \stackrel{(5)}{\equiv} 3^3 \equiv 2 \pmod{5} \\ \text{si } n \text{ impar } 3^1 \stackrel{(5)}{\equiv} 3 \pmod{5} \end{array} \right.$$

$r_4(n)$	0	1	2	3
$r_4(3^n)$	1	3	1	3

 $\star^3$

$$\left\{ \begin{array}{ll} 8^{3^n-2} \equiv 0 \pmod{4} \star^4 & \text{si } \forall n \in \text{naturales} \\ 8^{3^n-2} \equiv 2 \pmod{5} \star^5 & \text{si } n \equiv 0 \pmod{2} \\ 8^{3^n-2} \equiv 3 \pmod{5} \star^6 & \text{si } n \equiv 1 \pmod{2} \end{array} \right.$$

$$\text{Si } n \equiv 0 \pmod{2} \xrightarrow[\star^5]{\star^4} \left\{ \begin{array}{l} 8^{3^n-2} = 4j \rightarrow 4j \equiv 2 \pmod{5} \Leftrightarrow j \equiv 3 \pmod{5} \\ \Leftrightarrow j = 5k + 3 \Rightarrow 8^{3^n-2} = 4(5k + 3) \Leftrightarrow \boxed{8^{3^n-2} \equiv 12 \pmod{20} \Leftrightarrow n \equiv 0 \pmod{2}} \end{array} \right. \quad \checkmark$$

$$\text{Si } n \equiv 1 \pmod{2} \xrightarrow[\star^6]{\star^4} \left\{ \begin{array}{l} 8^{3^n-2} = 4j \rightarrow 4j \equiv 3 \pmod{5} \Leftrightarrow j \equiv 2 \pmod{5} \\ \Leftrightarrow j = 5k + 2 \Rightarrow 8^{3^n-2} = 4(5k + 2) \Leftrightarrow \boxed{8^{3^n-2} \equiv 8 \pmod{20} \Leftrightarrow n \equiv 1 \pmod{2}} \end{array} \right. \quad \checkmark$$

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

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.

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

Info de los MCD:

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

$$\left\{ \begin{array}{l} 13 \mid n^{109} + 37 \\ 2 \mid n^{109} + 37 \\ 4 \nmid n^{109} + 37 \end{array} \right. \text{ Para que } (n^{63} - 21 : 39) = 39 \text{ debe ocurrir que:}$$

$$\left\{ \begin{array}{l} 13 \mid n^{63} - 21 \\ 3 \mid n^{63} - 21 \end{array} \right.$$

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

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

R:

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

$$12^{2^n} \equiv 2 \pmod{7} \text{ si } n \text{ par}$$

pasar

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

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

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

$$\text{si } p \text{ primo y } p \nmid a, \text{ con } a \in \mathbb{Z} \Rightarrow a^n \equiv a^{r_{p-1}} \pmod{p}$$

$$3^{p^2+3} \equiv -84 \pmod{p} \left\{ \begin{array}{l} \xrightarrow[p \nmid 3]{\text{caso}} \left\{ \begin{array}{l} 3^{p^2+3} \stackrel{(p)}{\equiv} 3^{r_{(p-1)}(p^2+3)} \\ \xrightarrow[\text{polinomio}]{\text{división}} p^2+3 = (p-1)(p+1) + \overbrace{4}^{\star^1 r_{(p-1)}(p^2+3)} \Rightarrow 3^{p^2+3} \stackrel{(p)}{\equiv} \underbrace{3^4}_{81} \star^2 \\ 3^{p^2+3} \equiv -84 \pmod{p} \stackrel{\star^2}{\Leftrightarrow} 81 \equiv -84 \pmod{p} \Leftrightarrow \underbrace{165}_{5 \cdot 3 \cdot 11} \equiv 0 \pmod{p} \xrightarrow[p \nmid 3]{\Leftrightarrow} \boxed{p=5} \text{ o } \boxed{p=11} \end{array} \right. \\ \xrightarrow[p \mid 3]{\text{caso}} \left\{ \begin{array}{l} p \mid 3 \Leftrightarrow p=3 \Rightarrow 3^{p^2+3} \stackrel{(3)}{\equiv} 0 \equiv \underbrace{-84}_{\stackrel{(3)}{\equiv} 0} \pmod{3} \Rightarrow \boxed{p=3} \end{array} \right. \end{array} \right.$$

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

Con  $p=3$ :

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

Con  $p=5$ :


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

Con  $p=11$ :

$$(7 \cdot 11 + 8)^{2024} \stackrel{(11)}{\equiv} 8^{2024} \stackrel{(11)}{\equiv} 8^{r_{10}(2024)} \stackrel{(11)}{\equiv} 8^4 = \underbrace{4096}_{r_{11}(4096)=4} \equiv 4 \pmod{11} \quad \checkmark$$

Por lo tanto los valores de  $p$  que cumplen lo pedido son:

$$\boxed{\begin{array}{c} p=3 \\ \text{y} \\ p=11 \end{array}} \quad \checkmark$$


 8. 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:

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

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  $\underbrace{(649 : 132)}_{\substack{11 \cdot 59 \quad 2^2 \cdot 3 \cdot 11}} = 11$  tiene que dividir al número independiente. En este caso  $11 \nmid 9780$  y  $11 \mid 9779$ , 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  $P \geq 0$  y  $D \geq 0$  .

$$649P + 132D = 9779 \xleftrightarrow{\text{comprimizar}} 59P + 12D = 889,$$

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

$$\begin{cases} 59 = 4 \cdot 12 + 11 \\ 12 = 1 \cdot 11 + 1 \end{cases} \rightarrow 1 = \underbrace{12 - 1 \cdot 11}_{59 - 4 \cdot 12} = (-1) \cdot 59 + 5 \cdot 12. \text{ Por lo que se obtiene que:}$$

$$1 = (-1) \cdot 59 + 5 \cdot 12 \xrightarrow{\times 889} 889 = \underbrace{(-889) \cdot 59 + 4445 \cdot 12}_{\text{Combineta entera buscada } \checkmark} \xrightarrow[\text{particular}]{\text{solución}} (P, D)_{\text{part}} = (-889, 4445).$$


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  :

$$\begin{cases} P = 12h + 11 \geq 0 \iff h \geq -\frac{11}{12} \xleftrightarrow{h \in \mathbb{Z}} h \geq 0 \\ D = -59h + 20 \geq 0 \iff h \leq \frac{20}{59} \xleftrightarrow{h \in \mathbb{Z}} h \leq 0 \end{cases} \Leftrightarrow h = 0, \text{ Entonces: } (P, D) = (11, 20) \quad \checkmark$$

El coleccionista compró *once* pinturas y *veinte* dibujos.

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

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



Ejercicio de sistema de ecuaciones de congruencias. 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:

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

$$\begin{cases} 3a \equiv 12 \pmod{24} \\ a \equiv 10 \pmod{30} \\ 20a \equiv 50 \pmod{125} \end{cases} \iff \begin{cases} a \equiv 4 \pmod{8} \\ a \equiv 10 \pmod{30} \\ a \equiv 15 \pmod{25} \end{cases}$$

Todavía no tenemos los divisores coprimos 2 a 2. Ahora quebramos:

$$\begin{cases} a \equiv 4 \pmod{8} \quad \checkmark \\ a \equiv 10 \pmod{30} \iff \begin{cases} a \equiv 0 \pmod{2} \quad \checkmark \\ a \equiv 1 \pmod{3} \\ a \equiv 0 \pmod{5} \quad \checkmark \end{cases} \\ a \equiv 15 \pmod{25} \quad \checkmark \end{cases}$$

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

$$\begin{cases} a \equiv 4 \pmod{8} \\ a \equiv 10 \pmod{30} \\ a \equiv 15 \pmod{25} \end{cases} \iff \begin{cases} a \equiv 4 \pmod{8} \star^1 \\ a \equiv 1 \pmod{3} \star^2 \\ a \equiv 15 \pmod{25} \star^3 \end{cases}$$

Ahora logramos tener el sistema con los divisores coprimos 2 a 2. Por T $\star$ R este sistema va a tener una solución particular  $x_0$  /  $0 \leq x_0 < \underbrace{3 \cdot 8 \cdot 25}_{600}$

$$\begin{cases} \xrightarrow[\star^1]{\text{de}} a = 8k + 4 \xrightarrow[\text{en } \star^2]{\text{reemplazo a } a} 8k + 4 \equiv 1 \pmod{3} \Leftrightarrow k \equiv 0 \pmod{3} \Leftrightarrow k = 3j \\ \xrightarrow[\text{en } a = 8k + 4]{\text{reemplazo } k} a = 24j + 4 \xrightarrow[\text{en } \star^3]{\text{reemplazo a } a} 24j + 4 \equiv 15 \pmod{25} \Leftrightarrow j \equiv 14 \pmod{25} \Leftrightarrow j = 25h + 14 \\ \xrightarrow[\text{en } a = 24j + 4]{\text{reemplazo } j} a = 600h + 340 \Leftrightarrow \boxed{a \equiv 340 \pmod{600}} \quad \checkmark \end{cases}$$