

# Apunte único: Álgebra I - Práctica 5

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>	

### Disclaimer:

Dirigido para aquél que esté listo para leerlo, o no tanto. Va con onda.

## ¡Si usás este apunte vas a reprobar!

*Not really.* Dependerá de como lo uses, puede ser un arma de doble filo.

Ya sabés como se usa **esto** 📖. Depende de vos lo que hagás con él.

Si estás trabado, antes de ver la solución que hizo otra persona:

📖 Mirar la solución ni bien te trabás, te *condicionas pavlovianamente* a **no** pensar. Necesitás darle tiempo al cerebro para llegar a la solución.

📖 Intentá un ejercicio similar, pero **más fácil**.

📖 ¿No sale el fácil? Intentá uno **aún más fácil**.

📖 Fijate si tenés un ejercicio similar hecho en clase. Y mirá ese, así no quemás el ejercicio de la guía.

📖 Tomate 2 minutos para formular una pregunta que realmente sea lo que **no** entendés. Decir '*no me sale*' ≠ +. Escribí esa pregunta, vas a dormir mejor.

Ahora sí mirá la solución.

*Si no te salen los ejercicios fáciles* de un tema en particular, no te van a salir los ejercicios más difíciles: **Sentido común**.

¡Los más fáciles van a salir! Son el alimento de nuestra confianza.

Si mirás miles de soluciones a parciales en el afán de tener un ejemplo hecho de todas las variantes, estás apelando demasiado a la suerte de que te toque uno igual, *pero no estás aprendiendo nada*. Hacer un parcial bien lleva entre 3 y 4 horas. Así que si vos en 4 horas "hiciste" 3 o 4 parciales, *algo raro debe haber*. A los parciales se va a **pensar** y eso hay que practicarlo desde el primer día.

Mirá los videos de las teóricas de Teresa que son **buenísimos** 📺.

Videos de prácticas de pandemia, complemento extra: **Prácticas Pandemia** 📺.

Los ejercicios que se dan en clase suelen ser similares a los parciales, a veces más difíciles, repasalos siempre **Just Do IT** 🙌🙌🙌!

Eh, loco, fatalista, distópico, **relajá un toque te vas a quedar (más) pelado...** 🙌🙌🙌 *va a salir todo bien!*

El repo en [github](#)  para descargar las guías con los últimos updates.



<https://github.com/nad-garraz/algebraUno>

La Guía 5 se actualizó por última vez: 12/11/24 @ 13:35

Guía 5



<https://github.com/nad-garraz/algebraUno/blob/main/5-guia/5-sol.pdf>

Si querés mandar un ejercicio o avisar de algún error, lo más fácil es por

[Telegram](#) .



<https://t.me/+1znt2GV1i8cwMTNh>

**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.

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

- 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.

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

- 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:

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

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:

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

Amígate 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:

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

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:

$(a, b) = (2 + 3k, 6 - 11k)$  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 🧠.

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

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

- i)  $17X \equiv 3 \pmod{11}$       ii)  $56X \equiv 28 \pmod{35}$       iii)  $56X \equiv 2 \pmod{884}$       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:

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

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. Hallar todas las soluciones  $(x, y) \in \mathbb{Z}^2$  de la ecuación

$$110x + 250y = 100$$

que satisfacen simultáneamente que  $37^2 \mid (x - y)^{4321}$ .

La solución de la diofántica:

$$(x, y) = k \cdot (25, -11) + (410, -180) \xrightarrow{\star^1} \begin{cases} x = 25k + 410 \\ y = -11k - 180 \end{cases}$$

Entonces hay que ver para que valores de  $k$  se cumple que:

$$37^2 \mid (x - y)^{4321} \xrightarrow{\star^1} 37^2 \mid (590 + 36k)^{4321}$$

Buscamos posibles valores:

$$\star^2 37^2 \mid (590 + 36k)^{4321} \xrightarrow[\star^3]{\text{transitividad}} 37 \mid (590 + 36k)^{4321} \xleftrightarrow[p \text{ primo}]{p \mid a^n \Leftrightarrow p \mid a} 37 \mid 590 + 36k$$

Que como ecuación de congruencia queda:

$$-36k \equiv 590 \pmod{37} \Leftrightarrow k \equiv 35 \pmod{37}$$

Por lo tanto de  $\star^2$  solo faltaría probar la vuelta ( $\Leftarrow$ ) en  $\star^3$  se tiene que para los  $k$ :

$$k \equiv 35 \pmod{37} \Leftrightarrow 37^1 \mid (590 + 36k)^{4321} \stackrel{??}{\Leftrightarrow} 37^2 \mid (590 + 36k)^{4321}$$

Veamos:


$$\begin{aligned} 37^1 \mid (590 + 36k)^{4321} &\stackrel[primo]{37 \text{ es}}{\Rightarrow} 37 \mid 590 + 36k \stackrel{!}{\Rightarrow} 37^2 \mid (590 + 36k)^2 \\ &\Rightarrow 37^2 \mid (590 + 36k)^2 \cdot (50 + 36k)^{4319} \Leftrightarrow 37^2 \mid (590 + 36k)^{4321} \end{aligned}$$

De esa manera queda demostrado que

$$37^2 \mid (590 + 36k)^{4321} \Leftrightarrow 37 \mid (590 + 36k)^{4321} \Leftrightarrow 37 \mid 590 + 36k \Leftrightarrow 37 \mid 590 + 36k \Leftrightarrow k \equiv 35 \pmod{37}.$$

Por último el resultado serán los pares  $(x, y) \in \mathbb{Z}^2$  tales que

$$\begin{cases} x = 25k + 410 \\ y = -11k - 180 \end{cases} \quad \text{con} \quad k \equiv 35 \pmod{37}.$$

Dale las gracias y un poco de amor  a los que contribuyeron! Gracias por tu aporte:

 Ale Teran 

## 8. ... hay que hacerlo!

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

## 9. ... hay que hacerlo!

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

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

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

$$\text{ii) } \begin{cases} a \equiv 1 \pmod{6} \\ a \equiv 2 \pmod{20} \\ a \equiv 3 \pmod{9} \end{cases}$$

$$\text{iii) } \begin{cases} a \equiv 1 \pmod{12} \\ a \equiv 7 \pmod{10} \\ a \equiv 4 \pmod{9} \end{cases}$$

- i) Hay que resolver el sistema de ecuaciones de congruencia. Tengo divisores coprimos 2 a 2, así que por el **teorema chino del resto** hay solución:

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

El sistema tiene solución dado que 10, 7 y 9 son coprimos dos a dos. Resuelvo empezando por  $\star^1$  despejando y reemplazando en las demás ecuaciones:

$$a \equiv 3 \pmod{10} \stackrel{\text{def}}{\Leftrightarrow} a = 10k + 3 \stackrel{(7)}{\equiv}$$

Reemplazo ahora en  $\star^2$ :

$$10k + 3 \equiv 2 \pmod{7} \Leftrightarrow 3k \equiv 6 \pmod{7} \stackrel{3 \perp 7}{\Leftrightarrow} k \equiv 2 \pmod{7} \stackrel{\text{def}}{\Leftrightarrow} k = 7j + 2$$



Reemplazo el valor de  $k$  en  $a$ :

$$a = 10 \cdot (7j + 2) + 3 = 70j + 23$$

Y ahora reemplazo el valor de  $a$  en  $\star^3$ :

$$70j + 23 \equiv 5 \pmod{9} \Leftrightarrow 7j \equiv 0 \pmod{9} \xLeftrightarrow{7 \perp 9} j \equiv 0 \pmod{9} \xLeftrightarrow{\text{def}} j = 9h$$

Máquina de hacer chorizos y ahora reemplazo el valor de  $j$  en  $a$ :

$$a = 70(9h) + 23 = 630h + 23 \xLeftrightarrow{\text{def}} a \equiv 23 \pmod{630}$$

El TCH nos *aseguraba* una solución en el intervalo  $[0, 630)$  ✓

ii) Quebrando se ve que es *incompatible*. **DESARROLLAR**

iii) Quebrando se ve que es *compatible*. **DESARROLLAR**

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.

- i) Sabiendo que los restos de la división de un entero  $a$  por 6, 10 y 8 son 5, 3 y 5 respectivamente, hallar los posibles restos de la división de  $a$  por 480.
- ii) Hallar el menor entero positivo  $a$  tal que el resto de la división de  $a$  por 21 e 13 y el resto de la división de  $6a$  por 15 es 9.

i) Nos dicen que:

$$\begin{cases} a \equiv 5 \pmod{6} \\ a \equiv 3 \pmod{10} \\ a \equiv 5 \pmod{8} \end{cases}$$

Dado que los divisores no son coprimos, no se puede aplicar el TCH. Hay que quebrar.

$$\begin{cases} a \equiv 5 \pmod{6} & \rightsquigarrow & \begin{cases} a \equiv 2 \pmod{3} \\ a \equiv 1 \pmod{2} \end{cases} \\ a \equiv 3 \pmod{10} & \rightsquigarrow & \begin{cases} a \equiv 3 \pmod{5} \\ a \equiv 1 \pmod{2} \end{cases} \\ a \equiv 5 \pmod{8} & \rightsquigarrow & \begin{cases} a \equiv 1 \pmod{2} \\ a \equiv 1 \pmod{2} \\ a \equiv 1 \pmod{2} \end{cases} \end{cases}$$

La *buena* es que el sistema es compatible, dado que no tenemos restos distintos para un mismo cálculo. La cosa es ahora *¿cuáles agarro?*. Hay que pensar que queremos divisores *coprimos* y no tener soluciones de más. Esto último de *no tener soluciones de más* es la razón por la cual nos quedamos con  $a \equiv 5 \pmod{8}$  y no con  $a \equiv 1 \pmod{2}$ , porque en lo que a *coprimidad* respecta nada cambia, pero hay muchas soluciones de  $a \equiv 1 \pmod{2}$  que no están en  $a \equiv 5 \pmod{8}$ .

La cosa quedaría así:

$$\begin{cases} a \equiv 5 \pmod{6} \\ a \equiv 3 \pmod{10} \\ a \equiv 5 \pmod{8} \end{cases} \longleftrightarrow \begin{cases} a \equiv 2 \pmod{3} \star^1 \\ a \equiv 3 \pmod{5} \star^2 \\ a \equiv 5 \pmod{8} \star^3 \end{cases}$$

Por **Teorema Chino** el sistema tiene solución. Ahora es despejar, reemplazar y coso.

$$\begin{aligned} \star^1 a &= 3j + 2 \xrightarrow[\text{en } \star^2]{\text{reemplazo}} j \equiv 2 \pmod{5} \xleftrightarrow{\text{def}} j = 5k + 2 \\ \xrightarrow[\text{en } a]{\text{reemplazo}} a &= 3(5k + 2) + 2 = 15k + 8 \xrightarrow[\text{en } \star^3]{\text{reemplazo}} k \equiv 3 \pmod{8} \xleftrightarrow{\text{def}} k = 8i + 3 \\ \xrightarrow[\text{en } a]{\text{reemplazo}} a &= 15(8i + 3) + 8 = 120i + 53 \iff a \equiv 53 \pmod{120} \end{aligned}$$

Bueh, sacamos que los posibles valores de  $a$  son  $a \equiv 53 \pmod{120}$ , muy rico todo, pero nos pidieron los valores de restos:

$$a \equiv X \pmod{480}$$

Y dado que  $a = 120i + 53$ :

$$r_{480}(a) \in \{53, 173, 293, 413\}$$

valores para  $i = 0, 1, 2, 3$  respectivamente. Cumplen condición de resto, listo ganamos. Te mando un beso grande 😘.

ii) 😞... hay que hacerlo! 🙏

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

Dale las gracias y un poco de amor ❤️ a los que contribuyeron! Gracias por tu aporte:

👉 Nad Garraz 📄

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.

a)  $a = 33^{1427}, p = 5$

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

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

a) Escribo como ecuación de congruencia:

$$33^{1427} \equiv 3^{1427} \pmod{5}$$

Dado que 5 es primo puedo usar el PTF, notar que  $r_4(1427) = 3$

$$33^{1427} \equiv 3^{1427} \pmod{5} \xleftrightarrow{\text{PTF}} 3^{1427} \equiv 3^3 \pmod{5} \quad \text{y} \quad 3^3 = 27 \equiv 2 \pmod{5}$$

Por lo tanto:

$$r_5(33^{1427}) = 2$$

b) Rescribo:  $22283 = 22280 + 3$  y notar que el  $r_{10}(22280) = 0$

$$a = 71^{22283} = 71^{22280+3} = 71^{22280} \cdot 71^3 \stackrel{PTF}{\equiv} 71^3 (11) \Leftrightarrow a \equiv 5^3 \equiv 4 (11)$$

Por lo tanto:

$$r_{11}(a) = 4$$

c) Acomodo un poco la expresión, pensando en el PTF. Los exponentes tienen que quedar lindos para encontrar los restos de  $p - 1$

$$a \equiv 5 \cdot 7^{2448+3} + 0 - 10 \cdot 8^{132+6} (13) \stackrel{PTF}{\Leftrightarrow} a \equiv 5 \cdot 7^3 - 10 \cdot 8^6 (13) \stackrel{!!}{\Leftrightarrow} a \equiv 5 \cdot 5 - 23 \cdot 12 (13)$$

📊 *Nota que puede ser de interés:*

Con la calculadora salen fácil los cálculos, pero está bueno poder calcularlos a mano masajeando las potencias, onda  $8^6 = 64^3 \stackrel{(13)}{\equiv} (-1)^3 = -1 \stackrel{(13)}{\equiv} 12$

📊 *Fin Nota que puede ser de interés.*

Un par de cuentas y calcular congruencia y queda:

$$a \equiv 9 (13)$$

Dale las gracias y un poco de amor ❤️ a los que contribuyeron! Gracias por tu aporte:

👉 Nad Garraz 🔄

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

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

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

i) Hay que *toquetear* ese exponente feo, para que sea algo útil para usar PTF con ese 97 que está en el divisor.

Propiedades de exponente:

$$2^{194} \stackrel{!}{=} (2^2)^{97} = 4^{97}$$

La ecuación queda:

$$4^{97}X \equiv 7 (97) \stackrel{PTF}{\Leftrightarrow} 4X \equiv 7 (97) \stackrel{24 \perp 97}{\Leftrightarrow} X \equiv -168 (97) \Leftrightarrow X \equiv 26 (97)$$

ii) Hay que pensar como podemos modificar la ecuación para aplicar PTF:

$$5^{86}X \equiv 3 (89) \stackrel{89 \perp 5^2}{\Leftrightarrow} 5^{88}X \equiv 75 (89) \stackrel{89 \nmid 5}{\Leftrightarrow} X \equiv 75 (89)$$

Dale las gracias y un poco de amor  a los que contribuyeron! Gracias por tu aporte:

 Nad Garraz 

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

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

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

a) Escribiendo la consigna como ecuación de congruencia:

$$728 \mid a^{27} - a^3 \stackrel{\text{def}}{\iff} a^{27} - a^3 \equiv 0 \pmod{728}$$

Reescribo al divisor como:  $728 = 2^3 \cdot 7 \cdot 13$ . Los primos son nuestros aliados en estos ejercicios para poder usar PTF. Reescribo la ecuación a un sistema equivalente:

$$a^{27} - a^3 \equiv 0 \pmod{728} \iff \begin{cases} a^{27} - a^3 \equiv 0 \pmod{8} \text{ (8) } \star^1 \\ a^{27} - a^3 \equiv 0 \pmod{7} \text{ (7) } \star^2 \\ a^{27} - a^3 \equiv 0 \pmod{13} \text{ (13) } \star^3 \end{cases}$$

Empiezo analizando  $\star^1$ . Como el 8 no es primo, no se puede usar el PTF, así que lo encaramos *old style* con propiedades de exponentes y pensando que en congruencia módulo 8,  $r_8(a) \in \{0, 1, 2, 3, 4, 5, 6, 7\}$ : A ver que pasa si  $r_8(a)$  es par:

$$a^{27} - a^3 \stackrel{!}{=} (2k)^3 \cdot ((2k)^{24} - 1) = 8k^3 \cdot ((2k)^{24} - 1) \equiv 0 \pmod{8}$$

Por lo que cuando  $a$  es par,  $\star^1$  es válida. Ahora estudio los casos con  $r_8(a)$  impar, que por suerte no son muchos:

$$a^{27} - a^3 = a^3 \cdot (a^{24} - 1) \equiv 0 \pmod{8} \stackrel{!!!}{\iff} \begin{cases} 1^3 \cdot (1^{24} - 1) \equiv 0 \pmod{8} & \text{si } a = 1 \\ 3^3 \cdot (9^{12} - 1) \equiv 0 \pmod{8} & \text{si } a = 3 \\ 5^3 \cdot (25^{12} - 1) \equiv 0 \pmod{8} & \text{si } a = 5 \\ 7^3 \cdot (49^{12} - 1) \equiv 0 \pmod{8} & \text{si } a = 7 \end{cases}$$

Por lo que si  $r_8(a)$  es impar, también mostramos que  $\star^1$  es válida:

$$a^{27} - a^3 \equiv 0 \pmod{8} \quad \forall a \in \mathbb{Z}$$

Ahora vienen casos más agradables (espero) con divisores primos que nos permiten usar el PTF.

Analizo  $\star^2$

$$a^3 \cdot (a^{24} - 1) \equiv 0 \pmod{7} \Leftrightarrow \begin{cases} 0^3 \cdot (0^{24} - 1) \equiv 0 \pmod{7} & \text{si } 7 \mid a \\ \stackrel{\text{PTF}}{\stackrel{!}{\iff}} a^3 \cdot (a^0 - 1) \equiv 0 \pmod{7} \Leftrightarrow 0 \equiv 0 \pmod{7} & \text{si } 7 \nmid a \end{cases}$$

Por lo que  $\star^2$  se cumple para todo valor de  $a$ .

Analizo  $\star^3$  muuuy parecido:

$$a^3 \cdot (a^{24} - 1) \equiv 0 \pmod{13} \Leftrightarrow \begin{cases} 0^3 \cdot (0^{24} - 1) \equiv 0 \pmod{13} & \text{si } 13 \mid a \\ \stackrel{\text{PTF}}{\stackrel{!}{\iff}} a^3 \cdot (a^0 - 1) \equiv 0 \pmod{13} \Leftrightarrow 0 \equiv 0 \pmod{13} & \text{si } 13 \nmid a \end{cases}$$

Por lo que  $\star^3$  se cumple para todo valor de  $a$ .

Queda así demostrado que:

$$\begin{cases} a^{27} - a^3 \equiv 0 \pmod{8} \\ a^{27} - a^3 \equiv 0 \pmod{7} \\ a^{27} - a^3 \equiv 0 \pmod{13} \end{cases} \iff a^{27} - a^3 \equiv 0 \pmod{728} \stackrel{\text{def}}{\iff} 728 \mid a^{27} - a^3 \quad \forall a \in \mathbb{Z}$$

b) El enunciado puede pensarse como una ecuación de congruencia:

$$\frac{2a^7}{35} + \frac{a}{7} - \frac{a^3}{5} \in \mathbb{Z} \stackrel{!!}{\iff} 2a^7 + 5a - 7a^3 \equiv 0 \pmod{35}$$

Quizás conviene usar un sistema *equivalente*, con divisores primos que nos permitan usar el PTF:

$$2a^7 + 5a - 7a^3 \equiv 0 \pmod{35} \iff \begin{cases} 2a^7 + 5a - 7a^3 \equiv 0 \pmod{7} \star^1 \\ 2a^7 + 5a - 7a^3 \equiv 0 \pmod{5} \star^2 \end{cases}$$

Empiezo por  $\star^1$ :

$$2a^7 + 5a - 7a^3 \equiv 0 \pmod{7} \iff 2a^7 + 5a \equiv 0 \pmod{7} \iff \begin{cases} \text{si } 7 \mid a \Rightarrow 0 \equiv 0 \pmod{7} \\ \text{si } 7 \nmid a \stackrel{\text{PTF}}{\underset{!}{\Rightarrow}} 7a \equiv 0 \pmod{7} \iff 0 \equiv 0 \pmod{7} \end{cases}$$

De este último resultado, concluimos que no importa el valor de  $a$ , es decir:

$$2a^7 + 5a - 7a^3 \equiv 0 \pmod{7} \quad \forall a \in \mathbb{Z}$$

Ahora analizo  $\star^2$ :

$$2a^7 + 5a - 7a^3 \equiv 0 \pmod{5} \iff 2a^7 - 2a^3 \equiv 0 \pmod{5} \iff \begin{cases} \text{si } 5 \mid a \Rightarrow 0 \equiv 0 \pmod{5} \\ \text{si } 5 \nmid a \stackrel{\text{PTF}}{\underset{!}{\Rightarrow}} 2a^3 - 2a^3 \equiv 0 \pmod{5} \iff 0 \equiv 0 \pmod{5} \end{cases}$$

Al igual que en el caso anterior, concluimos que no importa el valor de  $a$ , es decir:

$$2a^7 + 5a - 7a^3 \equiv 0 \pmod{5} \quad \forall a \in \mathbb{Z}$$

Se concluye entonces que la expresión:

$$2a^7 + 5a - 7a^3 \equiv 0 \pmod{35} \iff \frac{2a^7}{35} + \frac{a}{7} - \frac{a^3}{5} \in \mathbb{Z} \quad \forall a \in \mathbb{Z}$$

Dale las gracias y un poco de amor  $\heartsuit$  a los que contribuyeron! Gracias por tu aporte:

$\text{👤}$  Nad Garraz  $\text{👤}$

18.  $\text{😬}$ ... hay que hacerlo!  $\text{👤}$

Si querés mandarlo: Telegram  $\rightarrow$   $\text{👤}$ , o mejor aún si querés subirlo en L<sup>A</sup>T<sub>E</sub>X  $\rightarrow$   $\text{👤}$ .

$\text{👤}$  ¿Errores? Avisá así se corrige y ganamos todos.

Ir a índice  $\uparrow$   
12/11/24 @ 13:35

## 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:

$$X \equiv \sum_{i=1}^{1759} i^{42} \pmod{56}$$

que será aún más simple si quiebro en la forma:

$$X \equiv \sum_{i=1}^{1759} i^{42} \pmod{56} \iff \begin{cases} X \equiv \sum_{i=1}^{1759} i^{42} \pmod{7} \star^1 \\ X \equiv \sum_{i=1}^{1759} i^{42} \pmod{8} \star^2 \end{cases}$$

Primero estudio  $\star^1$ .

Acomodo la sumatoria, voy a abrirla y separar los términos *convenientemente*:

$$\sum_{i=1}^{1759} i^{42} = 1^{42} + 2^{42} + 3^{42} + \dots + 1759^{42}$$

Le calculo el módulo 7 a todos los términos y obtengo:

$$\sum_{i=1}^{1759} i^{42} \equiv 1^{42} + 2^{42} + 3^{42} + 4^{42} + 5^{42} + 6^{42} + 0^{42} + 1^{42} + 2^{42} + 3^{42} + 4^{42} + 5^{42} + 6^{42} + 0^{42} + 1^{42} + 2^{42} + 3^{42} + 4^{42} + 5^{42} \dots$$

La sumatoria tiene un total de 1759 términos, que se puede agrupar en  $1759 = 251 \cdot 7 + 2$ .

$$\sum_{i=1}^{1759} i^{42} \equiv 251 \cdot (1^{42} + 2^{42} + 3^{42} + 4^{42} + 5^{42} + 6^{42} + 0^{42}) + (1^{42} + 2^{42})$$

$$\begin{array}{c} \xleftrightarrow{7 \text{ primo y } 7 \nmid i} \\ \text{PTF en cada término} \end{array}$$

$$\sum_{i=1}^{1759} i^{42} \equiv 251 \cdot (1 + 1 + 1 + 1 + 1 + 1 + 0) + (1 + 1) = 251 \cdot 6 + 2 \equiv 3 \pmod{7}$$

Encontramos entonces que  $\star^1$ :

$$X \equiv 3 \pmod{7}$$

Ahora se labura la expresión  $\star^2$ . Es la misma idea de antes, pero cuidado que como 8 no es primo, no se puede usar el PTF. Haciendo lo mismo de antes, abriendo la sumatoria y aplicando el módulo 8 a cada término:

$$\sum_{i=1}^{1759} i^{42} \equiv 1^{42} + 2^{42} + 3^{42} + 4^{42} + 5^{42} + 6^{42} + 7^{42} + 0^{42} + 1^{42} + 2^{42} + 3^{42} + 4^{42} + 5^{42} + 6^{42} + 7^{42} + 0^{42} + 1^{42} + 2^{42} + 3^{42} + 4^{42} + 5^{42} \dots$$

La sumatoria tiene un total de 1759 términos, que se puede agrupar en  $1759 = 219 \cdot 8 + 7$ .

$$\sum_{i=1}^{1759} i^{42} \equiv_{(8)} 219 \cdot (1^{42} + 2^{42} + 3^{42} + 4^{42} + 5^{42} + 6^{42} + 7^{42} + 0^{42}) + (1^{42} + 2^{42} + 3^{42} + 4^{42} + 5^{42} + 6^{42} + 7^{42})$$

Para analizar los términos a mano, se puede jugar con el exponente, buscando que el cálculo quede simple:

$$\begin{cases} 2^{42} = (2^3)^{14} \equiv_{(8)} 0 \\ 4^{42} = (2^3)^{14} \cdot (2^3)^{14} \equiv_{(8)} 0 \\ 6^{42} = (2^3)^{14} \cdot 3^{42} \equiv_{(8)} 0 \end{cases} \quad \begin{cases} 1^{42} = 1 \\ 3^{42} = (3^2)^{21} \equiv_{(8)} 1^{21} = 1 \\ 5^{42} = (5^2)^{21} \equiv_{(8)} 1^{21} = 1 \\ 7^{42} = (7^2)^{21} \equiv_{(8)} 1^{21} = 1 \end{cases}$$

Y por alguna razón *matemática*, la cual no podría importarme menos, los pares dieron 0 y los impares 1. 🚫

$$\sum_{i=1}^{1759} i^{42} \equiv_{(8)} 219 \cdot (1 + 0 + 1 + 0 + 1 + 0 + 1 + 0) + (1 + 0 + 1 + 0 + 1 + 0 + 1) = 219 \cdot 4 + 4 = 880 \equiv_{(8)} 0$$

Encontramos entonces que ★<sup>2</sup>:

$$X \equiv 0 \pmod{8}$$

Para resolver el ejercicio solo falta resolver el sistema que queda de juntar los resultados de ★<sup>1</sup> y ★<sup>2</sup>:

$$\begin{cases} X \equiv 3 \pmod{7} \\ X \equiv 0 \pmod{8} \end{cases}$$

tiene solución por TCH, dado que 8 y 7 son coprimos. La solución da  $X \equiv 24 \pmod{56}$ , por lo tanto el *resto pedido*:

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

Dale las gracias y un poco de amor 🧡 a los que contribuyeron! Gracias por tu aporte:

👋 Nad Garraz 🐸

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  $7X^{45} \equiv 1 \pmod{46}$ .

Acomodo un poco la ecuación que esta fea:

$$7X^{45} \equiv 1 \pmod{46} \xleftrightarrow{13 \perp 46} 91X^{45} \equiv 13 \pmod{46} \xleftrightarrow{!} X^{45} \equiv 33 \pmod{46}$$

La idea es quebrar para poder el PTF:

$$\xrightarrow[\text{!}]{\text{quiebro}} \begin{cases} X^{45} \equiv 10 \pmod{23} \xleftrightarrow[!!!]{23 \nmid X} X^{22} X^{22} X^1 \stackrel{(23)}{\underset{\text{PTF}}{\equiv}} X \equiv 10 \pmod{23} \\ X^{45} \equiv 1 \pmod{2} \xleftrightarrow[\text{entonces X también}]{X^{45} \text{ es impar}} X \equiv 1 \pmod{2} \end{cases}$$

En el !!! acomodo  $X^{45}$  para poder usar el PTF y  $X^{22} \equiv X^0 \pmod{23}$

📍 ¿Errores? Avisá así se corrige y ganamos todos.

Ir a índice ↑  
12/11/24 @ 13:35

Se tiene hasta el momento:

$$7X^{45} \equiv 1 \pmod{46} \iff \begin{cases} X \equiv 10 \pmod{23} \\ X \equiv 1 \pmod{2} \end{cases}$$

Sacar de acá, meter allá y coso:

$$X = 23k + 10 \stackrel{(2)}{\equiv} k \equiv 1 \pmod{2} \stackrel{\text{def}}{\iff} k = 2j + 1$$

Por lo tanto:

$$X = 23(2j + 1) + 10 = 46j + 33 \stackrel{\text{def}}{\iff} X \equiv 33 \pmod{46}$$

Dale las gracias y un poco de amor  a los que contribuyeron! Gracias por tu aporte:

 Nad Garraz 

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

Escribiendo el enunciado en ecuaciones queda algo así:

$$\begin{cases} 25^{70} \equiv 0 \pmod{d} \Leftrightarrow 5^{140} \equiv 0 \pmod{d} \\ d \equiv 2 \pmod{9} \\ d \equiv 3 \pmod{11}. \end{cases}$$

De la primera ecuación queda que el divisor  $d = 5^\alpha$  con  $\alpha$  compatible con las otras ecuaciones.

$$\begin{cases} 5^{140} \equiv 0 \pmod{5^\alpha} \\ 5^\alpha \equiv 2 \pmod{9} \star^1 \\ 5^\alpha \equiv 3 \pmod{11} \star^2 \end{cases}$$

Estudio la periodicidad que aparece al calcular los restos de las exponenciales. ¿Para qué valor de  $\alpha$  tendré  $5^\alpha \equiv 1$ ? Empiezo con  $\star^1$ . Notar que:

$$5^3 \equiv -1 \pmod{9} \stackrel{!}{\iff}_{(\Leftarrow) 5^3 \perp 9} 5^6 \equiv 1 \pmod{9}$$

Este último resultado me dice que como mucho hay 6 posibles valores distintos para  $r_9(5^\alpha)$  y eso se ve fácil escribiendo *genérica, pero convenientemente*, el exponente:

$$5^{6k+r_6(\alpha)} = (5^6)^k \cdot 5^{r_6(\alpha)} \stackrel{(9)}{\equiv} 5^{r_6(\alpha)}$$

Los valores del conjunto  $r_6(\alpha)$  son solo  $\{0, 1, 2, 3, 4, 5\}$ , calculo a mano los posibles resultados de  $\star^1$ :

$r_6(\alpha)$	0	1	2	3	4	5
$r_9(5^\alpha)$	1	5	7	8	4	2

Concluyo que:

$$5^\alpha \equiv 2 \pmod{9} \Leftrightarrow \alpha \equiv 5 \pmod{6}$$

El estudio de  $\star^2$  es un poco más feliz, porque 11 es primo y podemos usar PTF ([teoría acá](#)), entonces se encuentra la periodicidad de los restos de la exponencial más rápido:

$$5^\alpha \equiv 3 \pmod{11} \stackrel{11 \nmid 5}{\xrightarrow[\text{PTF, con } \alpha=10]{}} 5^{10} \stackrel{!}{\equiv} 5^{r_{10}(10)} \equiv 1 \pmod{11}$$



Con ese resultado uno se tiente a repetir lo que se hizo para  $\star^1$ , pero ahí está *la trampa del ejercicio*. El PTF nos da un resultado, pero no quiere decir que no haya otro de valor menor. Es decir que puede haber un  $\alpha < 10$  tal que cumpla que  $5^\alpha \equiv 1 \pmod{11}$ . Veamos si eso es así:

$r_{10}(\alpha)$	0	1	2	3	4	5	...
$r_{11}(5^\alpha)$	1	5	3	4	9	1	...

y sí, estaba ese número ahí para molestar. De no haber encontrado ese 1 ahí, se hubieran perdido soluciones. Para que se cumpla  $\star^2$ :

$$5^\alpha \equiv 3 \pmod{11} \Leftrightarrow \alpha \equiv 2 \pmod{5}$$

Los valores de  $\alpha$  deben cumplir el sistema:

$$\begin{cases} \alpha \equiv 5 \pmod{6} \\ \alpha \equiv 2 \pmod{5}, \end{cases}$$

con 6 y 5 coprimos hay solución por TCH. La solución:  $\alpha \equiv 17 \pmod{30}$  y además  $0 < \alpha \leq 140$  (si no vuela todo por los aires) lo que se cumple para:

$$\alpha = 30k + 17 = \begin{cases} 17 & \text{si } k = 0 \\ 47 & \text{si } k = 1 \\ 77 & \text{si } k = 2 \\ 107 & \text{si } k = 3 \\ 137 & \text{si } k = 4 \end{cases}$$

Finalmente los divisores positivos pedidos del enunciado son:

$$\mathcal{D}_+(25^{70}) = \{5^{17}, 5^{47}, 5^{77}, 5^{107}, 5^{137}\}$$

Dale las gracias y un poco de amor  a los que contribuyeron! Gracias por tu aporte:

 Nad Garraz 

**24.** Hallar todos los  $p \in \mathbb{N}$  que satisfacen:

a)  $2p \mid 38^{2p^2-p-1} + 3p + 171$

b)  $3p \mid 5^{p-1} + 3^{p^2+2} + 833$

a) Para poder usar PTF tengo que tener un primo en el divisor, quiebro:

$$38^{2p^2-p-1} + 3p + 171 \equiv 0 \pmod{2p} \iff \begin{cases} p \equiv 1 \pmod{2} \star^1 \\ 38^{2p^2-p-1} + 3p + 171 \equiv 0 \pmod{p} \star^2 \end{cases}$$

$$38^{2p^2-p-1} + 3p + 171 \equiv 0 \pmod{p} \Leftrightarrow \begin{cases} \xleftrightarrow[\Rightarrow p=19]{\text{si } p \mid 38} 38^{2p^2-p-1} + 3p + 171 \stackrel{(19)}{\equiv} 0 \equiv 0 \pmod{p} \star^3 \\ \xleftrightarrow[p \nmid 38]{\text{PTF}} 38^0 + 0 + 171 = \underbrace{172}_{2^2 \cdot 43} \equiv 0 \pmod{p} \star^4 \end{cases}$$

Cálculo para hacer el PTF:

$$\begin{array}{r} 2p^2 - p - 1 \mid p - 1 \\ - 2p^2 + 2p \quad \mid 2p + 1 \\ \hline p - 1 \\ - p + 1 \\ \hline 0 \end{array}$$

Después de hacer todo eso, sacamos de  $\star^1$  que  $p$  es impar. De  $\star^3$  obtenemos que un posible valor sería  $p = 19$  y luego del caso  $p \nmid 38$  sale que debe ocurrir que  $172 \stackrel{(p)}{\equiv} 0$ , y dado que  $p$  tiene que ser impar,  $p = 43$ .

b) 🤩... hay que hacerlo! 🙏

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

Dale las gracias y un poco de amor ❤️ a los que contribuyeron! Gracias por tu aporte:

👋 Nad Garraz 📄

**25.** Hallar los posibles restos de dividir a un entero  $a$  por 44 sabiendo que  $(a^{760} + 11a + 10 : 88) = 2$ .

$88 = 2^3 \cdot 11$ , y dado que el MCD es 2, podemos inferir que:

$$\begin{cases} 2 \mid a^{760} + 11a + 10 \star^1 \\ 4 \nmid a^{760} + 11a + 10 \star^2 \\ 11 \nmid a^{760} + 11a + 10 \star^3 \end{cases}$$

Vamos a buscar info sobre  $a$ . De  $\star^1$  tenemos que:

$$a^{760} + 11a + 10 \equiv a^{760} + a \equiv 0 \pmod{2} \Leftrightarrow \begin{cases} \text{si } a \equiv 0 \pmod{2} \Rightarrow 0^{760} + 0 \equiv 0 \pmod{2} \\ \text{si } a \equiv 1 \pmod{2} \Rightarrow 1^{760} + 1 \equiv 0 \pmod{2} \end{cases}$$

De donde no sacamos nada relevante respecto de  $a$ , dado que  $a$  podría ser par o impar, que es lo mismo que decir que  $a$  puede ser cualquier número 😊.

Ahora estudio  $\star^2$  para distintos valores de  $a$ . Vamos a poder usar PTF? NO, porque 4 no es primo chequea la teoría [acá](#):

$$a^{760} + 11a + 10 \equiv a^{760} - a + 2 \equiv 0 \pmod{4} \Leftrightarrow \begin{cases} \text{si } a \equiv 0 \pmod{4} \Rightarrow 2 \equiv 0 \pmod{4} \\ \text{si } a \equiv 1 \pmod{4} \Rightarrow 2 \equiv 0 \pmod{4} \\ \text{si } a \equiv 2 \pmod{4} \Rightarrow 2^{760} = (2^2)^{380} \stackrel{(4)}{\equiv} 0 \equiv 0 \pmod{4} \\ \text{si } a \equiv 3 \pmod{4} \Rightarrow 3^{760} - 1 \stackrel{(4)}{\equiv} (-1)^{760} - 1 = 0 \equiv 0 \pmod{4} \end{cases}$$

Qué se concluye de esa cosa? Tenemos que  $4 \nmid a^{760} + 11a + 10$ , entonces elijo los valores de  $a$  que justamente logren eso:

$$a \equiv 0 \pmod{4} \quad \text{o} \quad a \equiv 1 \pmod{4}$$

Misma historia con  $\star^3$ , y si estás despierto todavía, finalmente vamos a poder usar el PTF, porque 11 es un número primo ([teoría acá](#)):

$$a^{760} + 11a + 10 \equiv a^{760} - 1 \equiv 0 \pmod{11} \Leftrightarrow \begin{cases} \text{si } 11 \mid a \Rightarrow -1 \equiv 0 \pmod{11} \\ \text{si } 11 \nmid a \xrightarrow[\text{!}]{\text{PTF}} a^{r_{10}(760)} - 1 = 0 \equiv 0 \pmod{11} \end{cases}$$

Como en el caso anterior voy a elegir el conjunto de los  $a$  que haga que  $11 \nmid a^{760} + 11a + 10$ . En este caso me quedo con los  $a$  que cumplen:

$$11 \mid a \stackrel{\text{def}}{\iff} a \equiv 0 \pmod{11}$$

Con estos resultados puedo formar 2 sistemas:

$$\star^4 \begin{cases} a \equiv 0 \pmod{4} \\ a \equiv 0 \pmod{11} \end{cases} \quad \text{y} \quad \star^5 \begin{cases} a \equiv 1 \pmod{4} \\ a \equiv 0 \pmod{11} \end{cases}$$


Por TCH los sistemas tienen solución, porque los divisores son coprimos 2 a 2.

El sistema  $\star^4$  sale fácil  $\boxed{a \equiv 0 \pmod{44}}$

El sistema  $\star^5$ :

$$\begin{aligned} a \equiv 1 \pmod{4} &\stackrel{\text{def}}{\iff} a = 4k + 1 \\ 4k + 1 \equiv 0 \pmod{11} &\stackrel{11 \perp 3}{\iff} k \equiv 8 \pmod{11} \stackrel{\text{def}}{\iff} k = 11j + 8 \\ a &= 4(11j + 8) + 1 = 44j + 33 \\ &\boxed{a \equiv 33 \pmod{44}} \end{aligned}$$

Los posibles restos que nos pedían son 0 y 33.

Dale las gracias y un poco de amor  a los que contribuyeron! Gracias por tu aporte:

 Nad Garraz 

26. ... hay que hacerlo! 

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

27. ... hay que hacerlo! 

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

28. ... hay que hacerlo! 

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

29. ... hay que hacerlo! 

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

30. ... hay que hacerlo! 

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

## 🔥 Ejercicios extras:

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

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

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

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

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

Las condiciones marcan 2 sistemas:

$$\begin{cases} a \equiv 2 (5) \\ a \equiv 1 (7) \\ a \equiv 0 (3) \end{cases} \rightarrow \boxed{a \equiv 57 (105)}$$

$$\begin{cases} a \equiv 2 (5) \\ a \equiv 1 (7) \\ a \equiv 2 (3) \end{cases} \rightarrow \boxed{a \equiv 92 (105)}$$

Veo que para el conjunto de posibles  $a$

$$\begin{cases} a = 105k_1 + 57 \star^1 \\ \text{o} \\ a = 105k_2 + 92 \star^2 \end{cases}$$

Con los valores de  $a$  hallados, calculo el resto 70,  $r_{70}(a)$ :

$$\xrightarrow{(70)} \begin{cases} \star^1 a \equiv 57 (35) \\ \star^2 a \equiv 22 (35) \end{cases}$$

Los restos pedidos:

$$r_{70}(a) = \{22, 57\}$$

Dale las gracias y un poco de amor 🧡 a los que contribuyeron! Gracias por tu aporte:

👉 Nad Garraz 🍷

👉 Nacho 🍷

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:  $\left\{ \begin{array}{l} 5 \nmid a^{197} - 26 \\ 3 \nmid a^{197} - 26 \end{array} \right.$

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

Estudio la divisibilidad 5:

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

$$a^{197} \not\equiv 1 \pmod{5} \iff \left\{ \begin{array}{l} (\text{rama } 5 \nmid a) \xrightarrow[5 \nmid a]{5 \text{ es primo}} a \cdot \overbrace{(a^4)^{49}}^{(5) \equiv 1} \not\equiv 1 \pmod{5} \iff a \not\equiv 1 \pmod{5} \quad \checkmark \\ (\text{rama } 5 \mid a) \xrightarrow[5 \mid a]{5 \text{ es primo}} 0 \not\equiv 1 \pmod{5} \rightarrow a \equiv 0 \pmod{5} \end{array} \right.$$

Conclusión divisibilidad 5:

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

Estudio la divisibilidad 3:

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

$$a^{197} \not\equiv 2 \pmod{3} \iff \left\{ \begin{array}{l} (\text{rama } 3 \nmid a) \xrightarrow[3 \nmid a]{3 \text{ es primo}} a \cdot \overbrace{(a^2)^{98}}^{(3) \equiv 1} \not\equiv 2 \pmod{3} \iff a \not\equiv 2 \pmod{3} \quad \checkmark \\ (\text{rama } 3 \mid a) \xrightarrow[3 \mid a]{3 \text{ es primo}} 0 \not\equiv 2 \pmod{3} \rightarrow a \equiv 0 \pmod{3} \end{array} \right.$$

Conclusión divisibilidad 3:

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

Análisis de  $(a^{97} - 36 : 135)$ :

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

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

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

$$a^{97} \equiv 1 \pmod{5} \iff \left\{ \begin{array}{l} (\text{rama } 5 \nmid a) \xrightarrow[5 \nmid a]{5 \text{ es primo}} a \cdot \overbrace{(a^4)^{24}}^{(5) \equiv 1} \equiv 1 \pmod{5} \iff a \equiv 1 \pmod{5}, \text{ absurdo con } \star^2 \text{ ☹} \\ (\text{rama } 5 \mid a) \xrightarrow[5 \mid a]{5 \text{ es primo}} 0 \equiv 1 \pmod{5} \rightarrow \text{si } a \equiv 0 \pmod{5} \Rightarrow a^{97} \not\equiv 1 \pmod{5} \end{array} \right.$$

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  $\star^3$ ):

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

$$a^{97} \equiv 0 \pmod{3} \Leftrightarrow \begin{cases} (\text{rama } 3 \nmid a) \xrightarrow[3 \nmid a]{3 \text{ es primo}} a \cdot \overbrace{(a^2)^{48}}^{(5) \equiv 1} \equiv 0 \pmod{3} \Leftrightarrow a \equiv 0 \pmod{3} \quad \checkmark \\ (\text{rama } 3 \mid a) \xrightarrow[3 \mid a]{3 \text{ es primo}} a \equiv 0 \pmod{3} \Leftrightarrow 0 \equiv 0 \pmod{3} \rightarrow \text{si } a \equiv 0 \pmod{3} \Rightarrow a^{97} \equiv 0 \pmod{3} \end{cases}$$

Conclusión divisibilidad 3:

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

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  $\star^4$ :

$$9 \mid (3k)^{97} - 36 \xLeftrightarrow{\text{def}} (3k)^{97} \equiv 0 \pmod{9} \xLeftrightarrow[3^2 \cdot 3^{95} \cdot k^{97} \equiv 0 \pmod{9}]{\overset{!}{3^2 \cdot 3^{95} \cdot k^{97} \equiv 0 \pmod{9}}} 0 \equiv 0 \pmod{9} \quad \checkmark \quad \forall k \in \mathbb{Z}$$

Conclusión divisibilidad 9:

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


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

$$27 \mid (3k)^{97} - 36 \iff (3k)^{97} \equiv 0 \pmod{27} \xLeftrightarrow[3^3 \cdot 3^{94} \cdot k^{97} \equiv 0 \pmod{27}]{\overset{!}{3^3 \cdot 3^{94} \cdot k^{97} \equiv 0 \pmod{27}}} 0 \equiv 0 \pmod{27}$$

Conclusión divisibilidad 27:

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

Finalmente: el mcd es 9

Dale las gracias y un poco de amor  a los que contribuyeron! Gracias por tu aporte:

 Nad Garraz 

 Ale Teran 

 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:

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

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

Conclusión divisibilidad 7:

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

Estudio la divisibilidad  $7^2 = 49$ :

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

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

Conclusión divisibilidad 49:

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

Estudio la divisibilidad 19:

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

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

Conclusión divisibilidad 19:

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

$$\begin{cases} \star^1 n \equiv 0 \pmod{7} \\ \star^2 n \equiv 10 \pmod{19} \end{cases} \xrightarrow[7 \perp 19 \text{ hay solución por T chino R}]{7 \perp 19 \text{ hay solución por}} \begin{cases} \star^2 \\ \text{en } \star^1 \end{cases} n = 7(19k + 10) = 133k + 70 \rightarrow \boxed{n \equiv 70 \pmod{133}} \quad \checkmark$$

 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:

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

Laburo con  $\star^1$ :

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

$$\xrightarrow[\substack{n \text{ par} \\ n \text{ impar}}]{\star^2} 3^{r_4(3^n-2)} \begin{cases} \text{si } n \text{ par } & 3^{r_4(3^n-2)} \stackrel{(5)}{\equiv} 3^{1-2} \stackrel{(5)}{\equiv} 3^3 \equiv 2 \pmod{5} \\ \text{si } n \text{ impar } & 3^1 \stackrel{(5)}{\equiv} 3 \pmod{5} \end{cases}$$

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


$\star^3$

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

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

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

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.

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

Info de los MCD:

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

$$\begin{cases} 13 \mid n^{109} + 37 \\ 2 \mid n^{109} + 37 \\ 4 \nmid n^{109} + 37 \end{cases} \text{ Para que } (n^{63} - 21 : 39) = 39 \text{ debe ocurrir que: } \begin{cases} 13 \mid n^{63} - 21 \\ 3 \mid n^{63} - 21 \end{cases}$$

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

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

R:  
 $12^{2^n} \equiv 4 \pmod{7}$  si  $n$  impar  
 $12^{2^n} \equiv 2 \pmod{7}$  si  $n$  par

pasar

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

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

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

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

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

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:

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

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  $(\underbrace{649}_{11 \cdot 59} : \underbrace{132}_{2^2 \cdot 3 \cdot 11}) = 11$  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  $D \geq 0$  ★<sup>1</sup>.

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

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

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

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

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  $\star^1$  :

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

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:

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

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

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 **teorema chino del resto** este sistema va a tener una solución particular  $x_0$  con  $0 \leq x_0 < \underbrace{3 \cdot 8 \cdot 25}_{600}$

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