Álgebra I

Práctica 5 Resuelta

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

Choose your destiny:

- Notas teóricas
- Ejercicios de la guía:

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

- Ejercicios Extras

1.	**3.**	**5.**	**7.**	**9.**
2.	**4.**	**6.**	**8.**	

Notas teóricas:

- Sea $aX + bY = c$ con a, b, $c \in \mathbb{Z}$, $a \neq 0 \wedge b \neq 0$ y sea $S = \{(x, y) \in \mathbb{Z}^2 : aX + bY = C\}$. Entonces $S \neq \varnothing \iff (a : b) \mid c$
- Las soluciones al sistema: $S = \left\{(x, y) \in \mathbb{Z}^2 \text{ con } \left\{ \begin{array}{l} x = x_0 + kb' \\ y = y_0 + kb' \end{array} \right\}, k \in \mathbb{Z}\right\}$
- $aX \equiv c\ (b)$ con a, $b \neq 0$ tiene solución $\iff (a : b) \mid c$ tiene solución $\iff (a : b) \mid c$. En ese caso, coprimizando:

Ecuaciones de congruencia

- Algoritmo de solución:
  1) reducir a, c módulo m. Podemos suponer $0 \leq a, c < m$
  2) tiene solución $\iff (a : m) \mid c$. Y en ese caso coprimizo:

$$aX \equiv c\ (m) \iff a'X \equiv c'\ (m), \quad \text{con } a' = \frac{a}{(a : m)}, m' = \frac{m}{(a : m)} \text{ y } c' = \frac{c}{(a : m)}$$

  3) Ahora que $a' \perp m'$, puedo limpiar los factores comunes entre a' y c' (los puedo simplificar)

$$a'X \equiv c'\ (m') \iff a''X \equiv c''\ (m') \text{ con } a'' = \frac{a'}{(a' : c')} \text{ y } c'' = \frac{c'}{(a' : c')}$$

  4) Encuentro una solución particular X_0 con $0 \leq X_0 < m'$ y tenemos

$$aX \equiv c\ (m) \iff X \equiv X_0\ (m')$$

Ecuaciones de congruencia Sean $m_1, \ldots m_n \in \mathbb{Z}$ <u>coprimos dos a dos</u> ($\forall i \neq j$, se tiene $m_i \perp m_j$). Entonces, dados $c_1, \ldots, c_n \in \mathbb{Z}$ cualesquiera, el sistema de ecuaciones de congruencia.

$$\left\{ \begin{array}{l} X \equiv c_1\ (m_1) \\ X \equiv c_2\ (m_2) \\ \qquad \vdots \\ X \equiv c_n\ (m_n) \end{array} \right.$$

es equivalente al sistema (tienen misma soluciones)

$$X \equiv x_0\ (m_1 \cdot m_2 \cdots m_n)$$

para algún x_0 con $0 \leq x_0 < m_1 \cdot m_2 \cdots m_n$
<u>Pequeño teorema de Fermat</u>

- Sea p primo, y sea $a \in \mathbb{Z}$. Entonces:
  1.) $a^p \equiv a\ (p)$
  2.) $p \nmid a \Rightarrow a^{p-1} \equiv 1\ (p)$
- Sea p primo, entonces $\forall a \in \mathbb{Z}$ tal que $p \nmid a$ se tiene:

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

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

$$a^d \equiv 1 \ (p) \Rightarrow d \,|\, (p-1)$$

<u>*Aritmética modular:*</u>

- Sea $n \in \mathbb{N}, n \geq 2$
  $\mathbb{Z}/_{n\mathbb{Z}} = \{\overline{0}, \overline{1}, \cdots, \overline{n-1}\}$
  $\overline{a}, \overline{b} \in \mathbb{Z}/_{n\mathbb{Z}} : \begin{cases} \overline{a} \overline{+} \overline{b} := \overline{r_n(a+b)} \\ \overline{a} \overline{\cdot} \overline{b} := \overline{r_n(a \cdot b)} \end{cases}$

- Sea p primo, en $\mathbb{Z}/_{p\mathbb{Z}}$ todo elemento no nulo tiene inverso multiplicativo, análogamente a $\mathbb{Z}$.
  Si $m \in \mathbb{N}$ es compuesto,
  - *No todo* $\overline{a} \in \mathbb{Z}/_{m\mathbb{Z}}$ con $\overline{a} \neq \overline{0}$ es inversible.
  - $\exists\, \overline{a}, \overline{b} \in \mathbb{Z}/_{m\mathbb{Z}}$ con $\overline{a}, \overline{b} \neq 0$ tal que $\overline{a} \cdot \overline{b} = \overline{0}$
  - $\text{Inv}(\mathbb{Z}/_{m\mathbb{Z}}) = \{\overline{a} \in \{\overline{0}, \overline{1}, \ldots, \overline{m-1}\}\}$ tales que $a \perp m$

- Si $m = p$, con p primo, todo elemento no nulo de $\mathbb{Z}/_{p\mathbb{Z}}$ tiene inverso:
  - $\text{Inv}(\mathbb{Z}/_{p\mathbb{Z}}) = \{\overline{1}, \ldots, \overline{p-1}\}$.
  - <u>p primo $\Rightarrow \mathbb{Z}/_{p\mathbb{Z}}$ es un cuerpo.</u>
  - en $\mathbb{Z}/_{p\mathbb{Z}}$: $(\overline{a} + \overline{b})^p = \overline{a}^p + \overline{b}^p$

Ejercicios de la guía:

1. Falta hacerlo!

Si querés mandarlo: Telegram →, o mejor aún si querés subirlo en LaTeX→.

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. $(33:9) = 3$, $3 \mid 120$ ✓

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

Busco solución particular con algo parecido a Euclides:

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

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

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

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

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?

$$\begin{cases} A \geq 0 \wedge B \geq 0. \text{ Dado que son productos.} \\ (A:B) = 3 \Rightarrow 39A + 28B = 135 \xrightarrow{\text{coprimizar}} 13A + 16B = 45 \\ \text{A ojo } \to (A, B) = (1, 2) \end{cases}$$

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

---

i) $17X \equiv 3\ (11) \xrightarrow{\text{respuesta}} X \equiv 6\ (11)$

pasar

ii) $56X \equiv 28\ (35)$

$$\begin{cases} 56X \equiv 28\ (35) \iff 7X \equiv 21\ (35) \overset{?}{\iff} 7X - 35K = 21 \\ \xrightarrow[\text{ojo}]{\text{a}} (X, K) = (-2, -1) + q \cdot (-5, 1) \\ X \equiv -2\ (5) \iff X \equiv 3\ (5) = \{\dots, -2, 3, 8, \dots, 5q + 3\} \end{cases}$$

$\xrightarrow{\text{respuesta}} X \equiv 3\ (5)$ corroborar

iii)

iv) $78X \equiv 30\ (12126) \to 78X - 12126Y = 30 \xrightarrow[\text{coprimizando}]{(78:12126)=6} 13X - 2021Y = 5$

Busco solución particular con algo parecido a Euclides:

$$\begin{cases} 2021 = 13 \cdot 155 + 6 \\ 13 = 6 \cdot 2 + 1 \end{cases} \xrightarrow[\text{combinación de } 13 \text{ y} 2021]{\text{Escribo al 1 como}} 1 = 13 \cdot 311 + 2021 \cdot (-2) \xrightarrow[\text{al } 5]{\text{quiero}} 5 = 13 \cdot 1555 + 2021 \cdot (-10)$$

Respuesta: $\boxed{78X \equiv 30\ (12126) \overset{?}{\iff} X \equiv 1555\ (2021)}$

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

Parecido al **2.**.

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

Let's corroborate:

$b = 5 \cdot \underbrace{(13 + 24q)}_{k} + 2 \cdot \underbrace{(-13 + (-25)q)}_{a} = 39 + 70q \left\{ \begin{array}{l} b = 39 + 70q \equiv 4\ (5) \quad \checkmark \\ 2a = -26 - 50q \equiv -1\ (5) \equiv 4\ (5) \quad \checkmark \end{array} \right.$

6. Falta hacerlo!

Si querés mandarlo: Telegram →, o mejor aún si querés subirlo en LaTeX→.

7. Falta hacerlo!

Si querés mandarlo: Telegram →, o mejor aún si querés subirlo en LaTeX→.

8. Falta hacerlo!

Si querés mandarlo: Telegram →, o mejor aún si querés subirlo en LaTeX→.

9. Falta hacerlo!

Si querés mandarlo: Telegram →, o mejor aún si querés subirlo en LaTeX→.

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

i) $\left\{ \begin{array}{l} \star^1\ a \equiv 3\ (10) \\ \star^2\ a \equiv 2\ (7) \\ \star^3\ a \equiv 5\ (9) \end{array} \right.$

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

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

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

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

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

ii)

iii) $\left\{ \begin{array}{l} \star^1\ a \equiv 1\ (12) \\ \star^2\ a \equiv 7\ (10) \\ \star^3\ a \equiv 4\ (9) \end{array} \right.$

11. Falta hacerlo!

Si querés mandarlo: Telegram →, o mejor aún si querés subirlo en LaTeX→.

12. Falta hacerlo!

Si querés mandarlo: Telegram →, o mejor aún si querés subirlo en LaTeX→.

13. Falta hacerlo!

Si querés mandarlo: Telegram →, o mejor aún si querés subirlo en LaTeX→.

14. Falta hacerlo!

Si querés mandarlo: Telegram →, o mejor aún si querés subirlo en LaTeX→.

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

---

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

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

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

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

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

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

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

---

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

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

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

Falta hacerlo!

Si querés mandarlo: Telegram →, o mejor aún si querés subirlo en LaTeX→.

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

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

18. Falta hacerlo!
Si querés mandarlo: Telegram →, o mejor aún si querés subirlo en LaTeX→.

19. Falta hacerlo!
Si querés mandarlo: Telegram →, o mejor aún si querés subirlo en LaTeX→.

20. Hallar el resto de la división de:

i) $43 \cdot 7^{135} + 24^{78} + 11^{222}$ por 70

ii) $\sum\limits_{i=1}^{1759} i^{42}$ por 56

---

i) Falta hacerlo!

Si querés mandarlo: Telegram →, o mejor aún si querés subirlo en LaTeX→.

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

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

Primerlo estudio la ecuación de módulo 7:

$$\begin{cases} \displaystyle\sum_{i=1}^{1759} i^{42} \equiv X\ (7)\bigstar^{1} \xrightarrow[\text{si } p \not| \ i \to i^{42}=(i^6)^7 \equiv 1\ (7)]{7 \text{ es primo, uso Fermat}} \sum_{i=1}^{1759} i^{42} = \sum_{i=1}^{1759} (i^6)^7 \xrightarrow{251\cdot 7+2=1759} \\ \displaystyle\sum_{i=1}^{1759} (i^6)^7 \overset{(7)}{\equiv} 251\cdot((1^6)^7+(2^6)^7+(3^6)^7+(4^6)^7+(5^6)^7+(6^6)^7+(7^6)^7)+((1^6)^7+(2^6)^7+(3^6)^7+(4^6)^7) \\ \displaystyle\sum_{i=1}^{1759} (i^6)^7 \overset{(7)}{\equiv} 251\cdot(1+1+1+1+1+1+0)+(1+1+1+1) = 251\cdot 6+4 \overset{(7)}{\equiv} 3 \\ \xrightarrow{\bigstar^{1}} \boxed{X \equiv 3\ (7)} \end{cases}$$

Ahora se labura el módulo 8.

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

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

21. Falta hacerlo!

Si querés mandarlo: Telegram →, o mejor aún si querés subirlo en LaTeX→.

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

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

$$\to \begin{cases} X^{45} \equiv 33\ (23) \to X^{45} \equiv 10\ (23) \xrightarrow[X^{22}\equiv 1\ (23)]{23 \text{ primo y } 23 \not| \ X} X^{22}X^{22}X^{1} \overset{(23)}{\equiv} X \equiv 10\ (23) \\ X^{45} \equiv 10\ (2) \to X^{45} \equiv 0\ (2) \xrightarrow[\text{si mismo impar veces}]{X \text{ multiplicado por}} X \equiv 0\ (2) \end{cases}$$

La ecuación de congruencia $\boxed{X \equiv 10\ (46)}$ 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: $\begin{cases} 25^{70} \equiv 0\ (d) \to 5^{140} \equiv 0\ (d) \\ d \equiv 2\ (9) \\ d \equiv 3\ (11) \end{cases}$. De la primera ecuación queda que el divisor

$d = 5^{\alpha}$ con α compatible con las otras ecuaciones. $\to \begin{cases} 5^{\alpha} \equiv 2 \ (9) \\ 5^{\alpha} \equiv 3 \ (11) \end{cases}$

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

$\xrightarrow[5^{a} \overset{(d)}{\equiv} 1]{\text{Busco}}$

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

$5^3 \equiv -1 \ (9) \Leftrightarrow 5^6 \equiv 1 \ (9) \Leftrightarrow 5^{6k + r_6(\alpha)} = (\overbrace{5^6}^{\overset{(9)}{\equiv} 1})^k 5^{r_6(\alpha)}$.

Busco, posibles valores para $r_6(\alpha)$:

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

$\xrightarrow[\text{tanto}]{\text{por lo}}$ para que $5^{\alpha} \equiv 2 \ (9) \Leftrightarrow \boxed{\alpha \equiv 5 \ (6)}$ ✓

$5^{\alpha} \equiv 3 \ (11) \xrightarrow[\text{periodicidad 11 es primo, } 11 \not| \, 5]{\text{fermateo en búsqueda de}} 5^{10} \equiv 1 \ (11$

El PTF no me asegura que no haya un $\alpha < 10$ que también cumpla $5^{\alpha} \equiv 1 \ (11)$

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

$\xrightarrow[\text{periodicidad de 5}]{\text{por lo tanto hay}}$ Se obtiene enteonces:

$5^{\alpha} \equiv 3 \ (11) \Leftrightarrow \boxed{\alpha \equiv 2 \ (5)}$ ✓

El sistema $\begin{cases} \alpha \equiv 5 \ (6) \\ \alpha \equiv 2 \ (5) \end{cases}$ 6 y 5 son coprimos, se resuelve para $\alpha \equiv 17 \ (30)$ y además $0 < \alpha \leq 140$ lo que se cumple para $\alpha = 30k + 17 = \left\{ \begin{array}{lll} 17 & \text{si} & k = 0 \\ 47 & \text{si} & k = 1 \\ 77 & \text{si} & k = 2 \\ 107 & \text{si} & k = 3 \\ 137 & \text{si} & k = 4 \end{array} \right\} \to \boxed{\mathcal{D}_+(25^{70}) = \left\{5^{17}, 5^{47}, 5^{77}, 5^{107}, 5^{137}\right\}}$

24. Falta hacerlo!

Si querés mandarlo: Telegram →, o mejor aún si querés subirlo en LATEX→.

25. Falta hacerlo!

Si querés mandarlo: Telegram →, o mejor aún si querés subirlo en LATEX→.

26. Falta hacerlo!

Si querés mandarlo: Telegram →, o mejor aún si querés subirlo en LATEX→.

27. Falta hacerlo!

Si querés mandarlo: Telegram →, o mejor aún si querés subirlo en LATEX→.

28. Falta hacerlo!

Si querés mandarlo: Telegram →, o mejor aún si querés subirlo en LATEX→.

29. Falta hacerlo!

Si querés mandarlo: Telegram →, o mejor aún si querés subirlo en LATEX→.

30. Falta hacerlo!

Si querés mandarlo: Telegram →, o mejor aún si querés subirlo en LATEX→.

Ejercicios extras:

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

$$(\underbrace{a^{1081}+3a+17}_{m} : \underbrace{105}_{3\cdot5\cdot7}) = \underbrace{35}_{5\cdot7} \xrightarrow[\text{que}]{\text{debe ocurrir}} \begin{cases} 5 \mid m \\ \text{y} \\ 7 \mid m \\ \text{y} \\ 3 \nmid m \end{cases}$$

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

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

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

Las condiciones marcan 2 sistemas:

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

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

$\xrightarrow[\text{pedidos del enunciado}]{\text{quiero los restos}} r_{70}(a) = \{22, 57\}$, 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 $(a^{97}-36 : 135)$

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

$$(a^{97}-36 : \overbrace{135}^{3^3\cdot5}) = 3^\alpha \cdot 5^\beta \text{ con } \star^1 \left\{ \begin{array}{c} 0 \le \alpha \le 3 \\ 0 \le \beta \le 1 \end{array} \right\}.$$

Luego $(a^{197}-26 : \underbrace{15}_{3\cdot5}) = 1$ se debe cumplir que: $\begin{cases} 5 \nmid a^{197}-26 \\ 3 \nmid a^{197}-26 \end{cases}$

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

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

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

Conclusión divisilidad 5:

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

Estudio la divisibilidad 3:

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

$$a^{197} \not\equiv 2\ (3) \Leftrightarrow \begin{cases} (\text{rama } 3 \nmid a) \xrightarrow[5 \nmid a]{3 \text{ es primo}} a \cdot (\overbrace{a^2}^{\overset{(3)}{\equiv} 1})^{98} \not\equiv 2\ (3) \Leftrightarrow a \not\equiv 2\ (3) \quad \checkmark \\ (\text{rama } 3 \mid a) \xrightarrow[3 \mid a]{3 \text{ es primo}} 0 \not\equiv 2\ (3) \to a \equiv 0\ (3) \end{cases}$$

Conclusión divisilidad 3:

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

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 $\bigstar^2$ *y* $\bigstar^3$*):*

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

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

Conclusión divisilidad 5:

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

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

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

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

Conclusión divisilidad 3:

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

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

Estudio la divisibilidad 9 en $a = 3k$ por $\bigstar^4$*:*
$9 \mid (3k)^{97} - 36 \iff 3k^{97} \equiv 0\ (9) \iff 3 \cdot (3^2)^{48} \cdot k^{97} \equiv 0\ (9) \iff 0 \equiv 0\ (9) \quad \checkmark\ \forall k \in \mathbb{Z}$

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

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

Conclusión divisilidad 27:
Si $a \equiv 0\ (3) \Rightarrow 27 \nmid a^{97} - 36$

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

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

Conclusión divisibilidad 7:

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

Estudio la divisibilidad $7^2 = 49$:
Si $7^2 \nmid n^{433} + 7n + 91 \iff n^{433} + 7n + 91 \not\equiv 0\ (49) \iff n^{433} + 7n + 42 \not\equiv 0\ (49)$
$\xrightarrow[n \equiv 0\ (7) \Leftrightarrow n = 7k]{\text{de } \bigstar^1 \text{ tengo que}} (7k)^{433} + 7 \cdot 7k + 42 \not\equiv 0\ (49) \Leftrightarrow 7 \cdot (49)^{216} \cdot k^{433} + 49k + 42 \not\equiv 0\ (49) \Leftrightarrow 42 \not\equiv 0\ (49)$

Conclusión divisibilidad 49:

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

Estudio la divisibilidad 19:
Si $19 \mid n^{433} + 7n + 91 \iff n^{433} + 7n + 91 \equiv 0\ (19) \iff n^{433} + 7n + 15 \equiv 0\ (19) \xrightarrow[19 \mid n \text{ o } 19 \nmid n]{\text{analizo casos}}$

$$n^{433}+7n+15 \equiv 0\ (19) \Leftrightarrow \begin{cases} (\text{rama } 19 \not| \ n) \xrightarrow[19 \not| \ n]{19 \text{ es primo}} (\overbrace{n^{18}}^{\overset{(19)}{\equiv} 1})^{24} \cdot n + 7n + 15 \equiv 0\ (19) \Leftrightarrow 8n \equiv -15\ (19) \Leftrightarrow \\ \overset{\times 7}{\Longleftrightarrow} \boxed{n \equiv 10\ (19)} \quad \checkmark \bigstar^2 \\ (\text{rama } 19 \,|\, n) \xrightarrow[19 \,|\, n]{19 \text{ es primo}} 15 \equiv 0\ (19) \to \text{ningún } n \end{cases}$$

Conclusión divisibilidad 19:

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

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

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 congruecia:

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

Laburo con $\bigstar^1$:

$$8^{3^n-2} \equiv \underbrace{3^{3^n-2}}_{\overset{(5)}{\equiv} 3^{r_4(3^n-2)} \bigstar^2} (5)$$

$$\xrightarrow{\bigstar^2} 3^{r_4(3^n-2)} \xrightarrow[n \text{ impar}]{n \text{ par}} \begin{cases} \text{si } n \text{ par} \quad 3^{r_4(3^n-2)} \underset{\bigstar^3}{\overset{(5)}{\equiv}} 3^{1-2} \overset{(5)}{\equiv} 3^3 \equiv 2\ (5) \\ \text{si } n \text{ impar} \quad 3^1 \overset{(5)}{\equiv} 3\ (5) \end{cases}$$

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

$\bigstar^3$

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

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

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

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.

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

Info de los MCD:

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

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

$$\begin{cases} 13 \mid n^{63} - 21 \\ 3 \mid n^{63} - 21 \end{cases}$$

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

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

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

pasar

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

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

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

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

$$3^{p^2+3} \equiv -84 \ (p) \begin{cases} \xrightarrow[p \nmid 3]{\text{caso}} \begin{cases} 3^{p^2+3} \overset{(p)}{\underset{\star}{\equiv}} 3^{r_{(p-1)}(p^2+3)} \\ \xrightarrow[\text{polinomio}]{\text{división}} p^2 + 3 = (p-1)(p+1) + \overbrace{4}^{\star^1 \, r_{(p-1)}(p^2+3)} \Rightarrow 3^{p^2+3} \overset{(p)}{\underset{\star^1}{\equiv}} \underbrace{3^4}_{81} \star^2 \\ 3^{p^2+3} \equiv -84 \ (p) \overset{\star^2}{\Leftrightarrow} 81 \equiv -84 \ (p) \Leftrightarrow \underbrace{165}_{5\cdot3\cdot11} \equiv 0 \ (p) \overset{p \nmid 3}{\Longleftrightarrow} \boxed{p=5} \text{ o } \boxed{p=11} \end{cases} \\ \xrightarrow[p \mid 3]{\text{caso}} \begin{cases} p \mid 3 \Leftrightarrow p = 3 \Rightarrow 3^{p^2+3} \overset{(3)}{\equiv} 0 \equiv \underbrace{-84}_{\overset{(3)}{\equiv} 0} \ (3) \Rightarrow \boxed{p=3} \end{cases} \end{cases}$$

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

Con $p = 3$:

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

Con $p = 5$:

$$(7 \cdot 5 + 8)^{2024} \overset{(5)}{\equiv} 3^{2024} \underset{\star}{\overset{(5)}{\equiv}} 3^{r_4(2024)} \overset{(5)}{\equiv} 3^0 \overset{(5)}{\equiv} 1 \not\equiv 4 \ (5)$$

Con $p = 11$:

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

Por lo tanto los valores de p que cumplen lo pedido son: $\boxed{\begin{array}{c} p = 3 \\ \text{y} \\ p = 11 \end{array}}$ ✓

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:

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

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 $11 \not| \ 9780$ y $11 \,|\, 9779$, así que gastó un total de 9779 dólares.

Lo que resta hacer es resolver la ecuación teniendo en cuenta que estamos trabajando con variables que modelan algo físico por lo que $P \geq 0$ y $D \geq 0$★[1].

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

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

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

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

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 $\bigstar^1$:

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

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

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

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

Ejercicio de sistema de ecuaciones de congreuencias. Los divisores no son coprimos 2 a 2, así que hay que coprimizar y quebrar y analizar lo que queda.
Recordar que siempre que se pueda hay que comprimizar:

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

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

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

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

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

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

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

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