

# Práctica 5 de álgebra 1

Comunidad algebraica

---

Última compilación: 05/07/2024 a las 16:21

---

- 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  $S \neq \emptyset \iff (a : b) | c$
- Las soluciones al sistema:  $S = \left\{ (x, y) \in \mathbb{Z}^2 \text{ con } \begin{cases} x = x_0 + kb' \\ y = y_0 + kb' \end{cases}, k \in \mathbb{Z} \right\}$
- $aX \equiv c \pmod{b}$  con  $a, b \neq 0$  tiene solución  $\iff (a : b) | c$  tiene solución  $\iff (a : b) | c$ . 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  $\iff (a : m) | c$ . Y en ese caso coprimizo:

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

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

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

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

$$aX \equiv c \pmod{m} \iff X \equiv X_0 \pmod{m'}$$

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

$$\begin{cases} X \equiv c_1 \pmod{m_1} \\ X \equiv c_2 \pmod{m_2} \\ \vdots \\ X \equiv c_n \pmod{m_n} \end{cases}$$

es equivalente al sistema (tienen misma soluciones)

$$X \equiv x_0 \pmod{m_1 \cdot m_2 \cdots m_n}$$

para algún  $x_0$  con  $0 \leq x_0 < m_1 \cdot m_2 \cdots m_n$

Pequeño teorema de Fermat

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

$$1.) \quad a^p \equiv a \pmod{p}$$

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

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

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

- 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:

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

### Aritmética modular:

- Sea  $n \in \mathbb{N}, n \geq 2$   
 $\mathbb{Z}/n\mathbb{Z} = \{\bar{0}, \bar{1}, \dots, \overline{n-1}\}$   
 $\bar{a}, \bar{b} \in \mathbb{Z}/n\mathbb{Z} : \begin{cases} \bar{a} + \bar{b} := \overline{r_n(a+b)} \\ \bar{a} \cdot \bar{b} := \overline{r_n(a \cdot b)} \end{cases}$
- 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  $\bar{a} \in \mathbb{Z}/m\mathbb{Z}$  con  $\bar{a} \neq \bar{0}$  es inversible.
- $\exists \bar{a}, \bar{b} \in \mathbb{Z}/m\mathbb{Z}$  con  $\bar{a}, \bar{b} \neq \bar{0}$  tal que  $\bar{a} \cdot \bar{b} = \bar{0}$
- $\text{Inv}(\mathbb{Z}/m\mathbb{Z}) = \{\bar{a} \in \{\bar{0}, \bar{1}, \dots, \overline{m-1}\}\}$  tales que  $a \perp m$

- Si  $m = p$ , con  $p$  primo, todo elemento no nulo de  $\mathbb{Z}/p\mathbb{Z}$  tiene inverso:

- $\text{Inv}(\mathbb{Z}/p\mathbb{Z}) = \{\bar{1}, \dots, \overline{p-1}\}$ .
- $p$  primo  $\Rightarrow \mathbb{Z}/p\mathbb{Z}$  es un cuerpo.
- en  $\mathbb{Z}/p\mathbb{Z} : (\bar{a} + \bar{b})^p = \bar{a}^p + \bar{b}^p$

## Ejercicios de la guía:

---

### 1. Hacer!

---

### 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.  $(33 : 9) = 3, 3 \mid 120 \quad \checkmark$

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

Busco solución particular con algo parecido a Euclides:

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

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  $k \equiv 2 \pmod{8}$

---

### 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?

---

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

---

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

---

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

ii)  $56X \equiv 28 \pmod{35}$   

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

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

iii)

iv)  $78X \equiv 30 \pmod{12126} \rightarrow 78X - 12126Y = 30 \xrightarrow[\text{coprimizando}]{(78 : 12126) = 6} 13X - 2021Y = 5$   
 Busco solución particular con algo parecido a Euclides:  

$$\begin{cases} 2021 = 13 \cdot 155 + 6 \\ 13 = 6 \cdot 2 + 1 \end{cases} \xrightarrow[\text{combinación de 13 y 2021}]{\text{Escribo al 1 como}} 1 = 13 \cdot 311 + 2021 \cdot (-2) \xrightarrow[\text{al 5}]{\text{quiero}} 5 = 13 \cdot 1555 + 2021 \cdot (-10)$$
  
 Respuesta: 
$$78X \equiv 30 \pmod{12126} \xrightarrow{?} X \equiv 1555 \pmod{2021}$$

---

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

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. Hacer!

---

7. Hacer!

---

8. Hacer!

---

9. Hacer!

---

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

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

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

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

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

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

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

ii)

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

---

11. Hacer!

---

12. Hacer!

---

13. Hacer!

---

14. Hacer!

---

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

---

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

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

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

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

$$a \equiv 5 \cdot 7^{204 \cdot 12 + 3} + 3 \cdot 8^{11 \cdot 12 + 6} (13) \rightarrow a \equiv 5 \cdot (7^{12})^{204} \cdot 7^3 + 3 \cdot (8^{12})^{11} \cdot 8^6 (13)$$
$$\xrightarrow[p \nmid 8]{p \nmid 7} a \equiv 5 \cdot 7^3 + 3 \cdot 8^6 (13) \rightarrow a \equiv 5 \cdot (-6^3 + 3 \cdot 5^5) (13) \text{ consultar}$$

---

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

---

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

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

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

---

Hacer!

---

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

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

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

---

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

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

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

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


---

18. **Hacer!**

---

19. **Hacer!**

---

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) **Hacer!**

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

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

Primero estudio la ecuación de módulo 7:

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

Ahora se labura el módulo 8.

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

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

**21. Hacer!**

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

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



$$\rightarrow \begin{cases} X^{45} \equiv 33 \pmod{23} \rightarrow X^{45} \equiv 10 \pmod{23} \xrightarrow[X^{22} \equiv 1 \pmod{23}]{23 \text{ primo y } 23 \nmid X} X^{22} X^{22} X^1 \overset{(23)}{\equiv} X \equiv 10 \pmod{23} \\ X^{45} \equiv 10 \pmod{2} \rightarrow X^{45} \equiv 0 \pmod{2} \xrightarrow[\text{si mismo impar veces}]{X \text{ multiplicado por}} X \equiv 0 \pmod{2} \end{cases}$$

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

---

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

---

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

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

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

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

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

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


---

**24.** Hacer!

---

25. Hacer!

26. Hacer!

27. Hacer!

28. Hacer!

29. Hacer!

30. Hacer!

## Ejercicios extras:

---

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

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

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

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

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

Las condiciones marcan 2 sistemas:

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

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

Veo que para el conjunto de posibles  $a \left\{ \begin{matrix} a = 105k_1 + 22 \\ o \\ a = 105k_2 + 92 \end{matrix} \right\} \xrightarrow[(70)]{\text{calculo}} a \equiv 22 \pmod{35} \xrightarrow[\text{pedidos del enunciado}]{\text{quiero los restos}} r_{70}(a) = \{22, 57\}$ , valores de  $a$  que cumplan condición de  $r_{70}(a)$

---

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

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

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

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

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

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

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

Conclusión divisibilidad 5:

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

Estudio la divisibilidad 3:

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

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

Conclusión divisibilidad 3:

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

Análisis de  $(a^{97} - 36 : 135)$ :

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

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

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

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

Conclusión divisibilidad 5:

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

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

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

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

Conclusión divisibilidad 3:

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

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  $\star^4$ :

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

Conclusión divisibilidad 9:

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

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

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

Conclusión divisibilidad 27:

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

Finalmente: el mcd es 9

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

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

Expresar las soluciones mediante una única ecuación.

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

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

Estudio la divisibilidad 7:

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

$$n^{433} \equiv 0 \pmod{7} \Leftrightarrow \begin{cases} (\text{rama } 7 \nmid n) \xrightarrow[7 \nmid n]{7 \text{ es primo}} (\underbrace{n^6}_{\equiv 1})^{72} \cdot n \equiv 0 \pmod{7} \Leftrightarrow n \equiv 0 \pmod{7}, \text{ pero esta rama } 7 \nmid n \rightarrow \text{no} \\ (\text{rama } 7 \mid n) \xrightarrow[7 \mid n]{7 \text{ es primo}} 0 \equiv 0 \pmod{7} \text{ y como esta rama } 7 \mid n \rightarrow \boxed{n \equiv 0 \pmod{7}} \quad \checkmark \star^1 \end{cases}$$

Conclusión divisibilidad 7:

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

Estudio la divisibilidad  $7^2 = 49$ :

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

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

Conclusión divisibilidad 49:

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

Estudio la divisibilidad 19:

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

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

Conclusión divisibilidad 19:

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

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

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.

Pasar

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:

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

$$\begin{cases} 13 \mid n^{63} - 21 \\ 3 \mid n^{63} - 21 \end{cases} \iff \begin{cases} n \equiv 1 \pmod{2} \\ n \equiv 2 \pmod{13} \\ n \not\equiv 3 \pmod{4} \\ n \equiv 0 \pmod{3} \end{cases} \iff \begin{cases} n \equiv 1 \pmod{2} \\ n \equiv 2 \pmod{13} \\ n \equiv 1 \pmod{4} \\ n \equiv 0 \pmod{3} \end{cases} \iff \begin{cases} n \equiv 2 \pmod{13} \\ n \equiv 1 \pmod{4} \\ n \equiv 0 \pmod{3} \end{cases} \quad \text{Completar R: } r_{156}(n) = 93$$


---

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

---

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

pasar