

Práctica 5 de álgebra 1

Comunidad algebraica

Última compilación: 29/06/2024 a las 22:02

- 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 extras:

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

$$\underbrace{(a^{1081} + 3a + 17 : 105)}_m = \underbrace{35}_{3 \cdot 5 \cdot 7} \xrightarrow[\text{que}]{\text{notar}} \begin{cases} 5 \mid m \\ 7 \mid m \\ 3 \nmid m \rightarrow \text{¡He aquí la más importante info!} \end{cases}$$

$$\left\{ \begin{array}{l} 5 \mid m \rightarrow a^{1081} + 3a + \underbrace{17}_{\equiv 2 (5)} \equiv 0 (5) \rightarrow \begin{cases} \text{si } 5 \mid a \rightarrow 2 \equiv 0 (5) \text{ ningún } a \text{ ☠} \\ \text{si } 5 \nmid a \xrightarrow[5 \text{ primo y } 5 \nmid a, \text{ fermateo}]{a^{1081} = a \cdot (a^4)^{270}} a + 3a + 2 \equiv 0 (5) \rightarrow a \equiv 2 (5) \\ \text{si } 5 \mid m \Rightarrow \boxed{a \equiv 2 (5)} \quad \checkmark \end{cases} \\ 7 \mid m \rightarrow a^{1081} + 3a + \underbrace{17}_{\equiv 3 (7)} \equiv 0 (7) \rightarrow \begin{cases} \text{si } 7 \mid a \rightarrow 3 \equiv 0 (7) \text{ ningún } a \text{ ☠} \\ \text{si } 7 \nmid a \xrightarrow[7 \text{ primo y } 7 \nmid a, \text{ fermateo}]{a^{1081} = a \cdot (a^6)^{180}} a + 3a + 3 \equiv 0 (7) \rightarrow 4a \equiv -3 (7) \\ \text{si } 7 \mid m \Rightarrow \boxed{a \equiv 1 (7)} \quad \checkmark \end{cases} \\ 3 \nmid m \rightarrow a^{1081} + 3a + \underbrace{17}_{\equiv 2 (3)} \equiv 0 (3) \rightarrow \begin{cases} \text{si } 3 \mid a \rightarrow 2 \equiv 0 (3) \begin{cases} \text{si } 3 \mid m \rightarrow 2 \equiv 0 (3) \rightarrow \text{ningún } a \text{ ☠, pero} \\ \text{quiero } 3 \nmid m \Rightarrow \text{todo } a, \text{ pero en esta rama} \\ 3 \mid a \Rightarrow \text{si } 3 \nmid m \rightarrow \boxed{a \equiv 0 (3)} \quad \checkmark \end{cases} \\ \text{si } 3 \nmid a \xrightarrow[3 \text{ primo y } 3 \nmid a, \text{ fermateo}]{a^{1081} = a \cdot (a^2)^{540}} a + 0 + 2 \equiv 0 (7) \rightarrow a \equiv -2 (3) \\ \text{si } 3 \nmid m \Rightarrow \star^1 \boxed{a \not\equiv 1 (3)} \quad \checkmark \end{cases} \end{array} \right.$$

Debido a la última condición \star^1 , el problema se ramifica en 2 sistemas:

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

Veo que para el conjunto de posibles $a \begin{cases} a = 105k_1 + 22 \\ o \\ a = 105k_2 + 92 \end{cases} \xrightarrow[(70)]{\text{calculo}} a \equiv 22 (35) \xrightarrow[\text{pedidos del enunciado}]{\text{quiero los restos}} r_{70}(a) = \{22, 57\}$, 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 $(a^{97} - 36 : 135)$

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

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

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

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

Estudio la divisibilidad 5:

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

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

Conclusión divisibilidad 5:

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

Estudio la divisibilidad 3:

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

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

Conclusión divisibilidad 3:

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

Análisis de $(a^{97} - 36 : 135)$:

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

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

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

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

Conclusión divisibilidad 5:

$$\boxed{5 \nmid a^{97} - 36 \quad \forall a \in \mathbb{Z}}$$

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

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

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

Conclusión divisibilidad 3:

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

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

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

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

Conclusión divisibilidad 9:

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

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

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

Conclusión divisibilidad 27:

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

Finalmente: el mcd es 9

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

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

Expresar las soluciones mediante una única ecuación.

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

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

Estudio la divisibilidad 7:

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

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

Conclusión divisibilidad 7:

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

Estudio la divisibilidad $7^2 = 49$:

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

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

Conclusión divisibilidad 49:

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

Estudio la divisibilidad 19:

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

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

Conclusión divisibilidad 19:

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

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

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

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

Busco solución particular con algo parecido a Euclides:

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

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:

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

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

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

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

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

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

iii)

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

Busco solución particular con algo parecido a Euclides:

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

Respuesta: $\boxed{78X \equiv 30 \pmod{12126} \stackrel{?}{\iff} X \equiv 1555 \pmod{2021}}$

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

Parecido al 2..

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

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:

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

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

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

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

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

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

ii)

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

11. Hacer!

12. Hacer!

13. Hacer!

14. Hacer!

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

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

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

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

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

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

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

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

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

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

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

Hacer!

17. Hacer!

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:

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

Primerlo estudio la ecuación de módulo 7:

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

Ahora se labura el módulo 8.

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

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

21. **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

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

\rightarrow Usaré viejo truco de exponenciales de módulo periódicas:

$$\left\{ \begin{array}{l} 5^\alpha \equiv 2 \pmod{9} \\ 5^3 \equiv -1 \pmod{9} \xrightarrow[\text{cuadrado}]{\text{al}} 5^6 \equiv 1 \pmod{9} \xrightarrow[\text{tabla de restos}]{5^\alpha = 5^{6k+r_6(\alpha)} = \overset{(9)}{5^6}^k 5^{r_6(\alpha)}} \begin{array}{|c|c|c|c|c|c|c|} \hline r_6(\alpha) & 0 & 1 & 2 & 3 & 4 & 5 \\ \hline r_9(5^\alpha) & 1 & 5 & 7 & 8 & 4 & 2 \\ \hline \end{array} \\ \text{por lo tanto} \rightarrow \text{para que } 5^\alpha \equiv 2 \pmod{9} \Rightarrow \boxed{\alpha \equiv 5 \pmod{9}} \quad \checkmark \\ \hline 5^\alpha \equiv 3 \pmod{11} \xrightarrow[\alpha=2]{\text{a ojo}} 5^2 \equiv 3 \pmod{11} \\ \xrightarrow[\text{fermateo}]{\text{para no perder soluciones de } 5^\alpha \equiv 3 \pmod{11}} 5^{10} \equiv 1 \pmod{11} \xrightarrow[\text{cuando hago } 5^{12}]{\text{noto que tengo otro}} 5^2 \cdot 5^{10} \equiv 3 \pmod{11} \\ \xrightarrow[\text{tabla de restos por las dudas}]{\text{para no perder soluciones de } 5^\alpha \equiv 3 \pmod{11}} \begin{array}{|c|c|c|c|c|c|c|} \hline r_{10}(\alpha) & 0 & 1 & 2 & 3 & 4 & 5 \\ \hline r_{11}(5^\alpha) & 1 & 5 & 3 & 4 & 9 & 1 \\ \hline \end{array} \\ \text{por lo tanto hay} \rightarrow \text{para que } 5^\alpha \equiv 3 \pmod{11} \Rightarrow \boxed{\alpha \equiv 2 \pmod{5}} \quad \checkmark \end{array} \right.$$

El sistema $\begin{cases} \alpha \equiv 5 \pmod{9} \\ \alpha \equiv 2 \pmod{5} \end{cases}$ se resuelve para $\alpha \equiv 32 \pmod{45}$ y además $0 < \alpha \leq 140$ lo que se cumple para

$$\alpha = 45k + 32 = \begin{cases} 32 & \text{si } k = 0 \\ 77 & \text{si } k = 1 \\ 122 & \text{si } k = 2 \end{cases} \rightarrow \boxed{\mathcal{D}_+(25^{70}) = \{5^{32}, 5^{77}, 5^{122}\}}$$

24. **Hacer!**

25. Hacer!

26. Hacer!

27. Hacer!

28. Hacer!

29. Hacer!

30. Hacer!