Práctica 5 de álgebra 1

D. Garraz

last update: 22/06/2024

1 Definiciones y fórmulas útiles

- 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 $S \neq \varnothing \iff (a : b) \,|\, c$
- 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 $\iff (a : b) \,|\, c$ 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:
  $$aX \equiv c\ (m) \iff a'X \equiv c'\ (m), \quad \text{con } a' = \frac{a}{(a : m)},\ m' = \frac{m}{(a : m)} \text{ y } c' = \frac{c}{(a : m)}$$
  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 $m_1, \ldots m_n \in \mathbb{Z}$ coprimos dos a dos ($\forall i \neq j$, se tiene $m_i \perp m_j$). Entonces, dados $c_1, \ldots, c_n \in \mathbb{Z}$ cualesquiera, el sistema de ecuaciones de congruencia.

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

es equivalente al sistema (tienen misma soluciones)

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

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

- 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 dados en clase:

---

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

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

$$
\begin{cases}
5\,|\,m \to a^{1081}+3a+\underbrace{17}_{\overset{(5)}{\equiv}2} \equiv 0\ (5) \to
\begin{cases}
\text{si}\quad 5\,|\,a \to 2 \equiv 0\ (5)\,\text{ningún } a☠ \\
\text{si}\quad 5 \not|\, a \xrightarrow[\text{5 primo y 5} \not|\, a\text{, fermateo}]{a^{1081}=a\cdot(a^4)^{270}} a+3a+2\equiv 0\ (5) \to a \equiv 2\ (5) \\
\qquad \text{si } 5\,|\,m \Rightarrow \boxed{a \equiv 2\ (5)} \quad \checkmark
\end{cases} \\
7\,|\,m \to a^{1081}+3a+\underbrace{17}_{\overset{(7)}{\equiv}3} \equiv 0\ (7) \to
\begin{cases}
\text{si}\quad 7\,|\,a \to 3 \equiv 0\ (7)\,\text{ningún } a☠ \\
\text{si}\quad 7 \not|\, a \xrightarrow[\text{7 primo y 7} \not|\, a\text{, fermateo}]{a^{1081}=a\cdot(a^6)^{180}} a+3a+3\equiv 0\ (7) \to 4a \equiv -3\ (7) \\
\qquad \text{si } 7\,|\,m \Rightarrow \boxed{a \equiv 1\ (7)} \quad \checkmark
\end{cases} \\
3 \not|\, m \to a^{1081}+3a+\underbrace{17}_{\overset{(3)}{\equiv}2} \equiv 0\ (3) \to
\begin{cases}
\text{si}\quad 3\,|\,a \to 2 \equiv 0\ (3)
\begin{cases}
\text{si } 3\,|\,m \to 2 \equiv 0\ (3) \to \text{ningún } a☠\text{, pero} \\
\text{quiero } 3 \not|\, m \Rightarrow \text{todo } a\text{, pero en esta rama} \\
3\,|\,a \Rightarrow \text{si } 3 \not|\, m \to \boxed{a \equiv 0\ (3)} \quad \checkmark
\end{cases} \\
\text{si}\quad 3 \not|\, a \xrightarrow[\text{3 primo y 3} \not|\, a\text{, fermateo}]{a^{1081}=a\cdot(a^2)^{540}} a+0+2\equiv 0\ (7) \to a \equiv -2\ (3) \\
\qquad \text{si } 3 \not|\, m \Rightarrow^{8^1} \boxed{a \not\equiv 1\ (3)} \quad \checkmark
\end{cases}
\end{cases}
$$

Debido a la última condición [8^1], el problema se ramifica en 2 sistemas:

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

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 $(a^{97} - 36 : 135)$

Tengo que dar posible valores para $(a^{97} - 36 : 135)$. Como $135 = 3^3 \cdot 5$, los posibles valores serán de la forma $3^\alpha \cdot 5^\beta$ con $\left\{\begin{array}{c} 0 \le \alpha \le 3 \\ 0 \le \beta \le 1 \end{array}\right\}$ potencialmente $\underbrace{8}_{(3+1)\cdot(1+1)}$ posibles valores distintos $\{1, 3, 9, 27, 5, 15, 45, 135\}$

Como condición mínima para que no sea siempre $(a^{97} - 36 : 135) = 1$ es que $\left\{\begin{array}{c} 3\,|\,a^{97}-36 \\ \text{o bien,} \\ 5\,|\,a^{97}-36 \end{array}\right\}$ si no ocurre ninguna de éstas el MCD será 1.

$$
\begin{cases}
5\,|\,a^{97}-36 \to a^{97}-36 \overset{(5)}{\equiv} a^{97}-1 \overset{(5)}{\equiv} 0 \to
\begin{cases}
\xrightarrow[5\,|\,a]{\text{si}} \quad -1 \equiv 0\ (5) \xrightarrow[5\,|\,a\text{ logra que}]{\text{ningún } a \text{ tal que}} 5\,|\,a^{97}-36 \\
\xrightarrow[5 \not|\, a]{\text{si}} \quad (a^4)^{24}\cdot a - 1 \equiv 0\ (5) \xrightarrow[a^4 \equiv 1\ (5)]{5\text{ primo, } 5 \not|\, a} \boxed{a \equiv 1\ (5)}
\end{cases} \\
\text{Se concluye de esta rama que si } 5\,|\,a^{97}-36 \Rightarrow \boxed{a \equiv 1\ (5)}\ ^{8^3} \quad \checkmark \\
\hline
3\,|\,a^{97}-36 \to a^{97}-36 \overset{(3)}{\equiv} a^{97} \overset{(3)}{\equiv} 0 \to
\begin{cases}
\xrightarrow[3\,|\,a]{\text{si}} \quad 0 \equiv 0\ (3) \xrightarrow[\text{esta rama } a\,|\,3]{\text{dado que en}} \boxed{a \equiv 0\ (3)} \\
\xrightarrow[3 \not|\, a]{\text{si}} \quad (a^2)^{48}\cdot a \equiv 0\ (3) \xrightarrow[a^2 \equiv 1\ (3)]{3\text{ primo, } 3 \not|\, a} \boxed{a \equiv 0\ (3)}
\end{cases} \\
\text{Se concluye de esta rama que si } 3\,|\,a^{97}-36 \Rightarrow \boxed{a \equiv 0\ (3)}\ ^{8^4} \quad \checkmark
\end{cases}
$$

Todo muy lindo pero los valores de a están condicionados por $(a^{197} - 26 : 15) = 1$ una condición que "nada" tiene que ver con el MCD, pero que condiciona los valores que puede tomar a. Como $a^{197} - 26$ y $15 = 3 \cdot 5$ son coprimos sus factorizaciones en primos no pueden tener ningún número factor en común, dicho de otra forma: $\left\{\begin{array}{c} 5 \nmid a^{197}-26 \\ \text{y} \\ 3 \nmid a^{197}-26 \end{array}\right\}$ estudiar estas condiciones me va a restringir los valores de a que puedo usar para construir los posibles MCDs.

$$\left\{\begin{array}{l}
\xrightarrow[\text{quedo con el complemento}]{\text{supongo } 5\mid a^{197}-26 \text{ y me}} a^{197}-1 \overset{(5)}{\equiv} 0 \to \left\{\begin{array}{l}
\xrightarrow[5\mid a]{\text{si}} -1 \equiv 0\ (5) \xrightarrow[5\mid a \text{ logra que}]{\text{ningún } a \text{ tal que}} 5\mid a^{197}-26 \\
\xrightarrow[\text{todo } a \text{ pero como } 5\mid a]{\text{el complemento de "ningún" es}} a \equiv 0\ (5) \\
\hline
\xrightarrow[5\nmid a]{\text{si}} (a^4)^{49}\cdot a - 1 \equiv 0\ (5) \xrightarrow[a^4\equiv 1\ (5)]{5 \text{ primo, } 5\nmid a} a \equiv 1\ (5)\ 8^{1} \\
\xrightarrow[\text{complemento de } 8^{1}]{\text{agarro el}} \left\{\begin{array}{l} \cancel{a\equiv 0\ (5)} \to \text{rama } 5\nmid a \\ a\equiv 2\ (5) \\ a\equiv 3\ (5) \\ a\equiv 4\ (5) \end{array}\right.
\end{array}\right. \\
\hline
\xrightarrow[\text{quedo con el complemento}]{\text{supongo } 3\mid a^{197}-26 \text{ y me}} a^{197}-2 \overset{(3)}{\equiv} 0 \to \left\{\begin{array}{l}
\xrightarrow[3\mid a]{\text{si}} -2 \equiv 0\ (3) \xrightarrow[3\mid a \text{ logra que}]{\text{ningún } a \text{ tal que}} 3\mid a^{197}-26 \\
\xrightarrow[\text{todo } a \text{ pero como } 3\mid a]{\text{el complemento de "ningún" es}} a \equiv 0\ (3) \\
\hline
\xrightarrow[3\nmid a]{\text{si}} (a^2)^{93}\cdot a - 2 \equiv 0\ (3) \xrightarrow[a^2\equiv 2\ (3)]{3 \text{ primo, } 3\nmid a} a \equiv 2\ (3)\ 8^{2} \\
\xrightarrow[\text{complemento de } 8^{2}]{\text{agarro el}} \left\{\begin{array}{l} \cancel{a\equiv 0\ (3)} \to \text{rama } 3\nmid a \\ a\equiv 1\ (3) \end{array}\right.
\end{array}\right.
\end{array}\right.$$

Se concluye del estudio que si $5 \nmid a^{197}-26$ y $3 \nmid a^{197}-26 \to \boxed{\left\{\begin{array}{ll} a\equiv 0\ (5) & \text{o} \\ a\equiv 2\ (5) & \text{o} \\ a\equiv 3\ (5) & \text{o} \\ a\equiv 4\ (5) & \\ \quad \text{y} & \\ a\equiv 0\ (3) & \text{o} \\ a\equiv 1\ (3) & \end{array}\right.}$, 8 sistemas ☠

Para que el MCD *no sea 1*, se deben satisfacer 8^{3} o 8^{4}, lo cual no ocurre nunca con 8^{3}. Eso acota los valores de $(a^{97}-36 : 135)$ a $\{1, 3, 9, 27\}$
De los 4 sistemas útiles:

$$\left\{\begin{array}{l} a\equiv 0\ (5) \\ a\equiv 0\ (3) \end{array}\right. \xrightarrow{\text{solución}} a \equiv 0\ (15) \xrightarrow{\text{con } a=0} \left\{\begin{array}{l} 0^{97}-36 \overset{(3)}{\equiv} 0 \\ 0^{97}-36 \overset{(9)}{\equiv} 0 \quad \checkmark \\ 0^{97}-36 \overset{(27)}{\equiv} -9 \overset{(27)}{\not\equiv} 0 \end{array}\right.$$

$$\left\{\begin{array}{l} a\equiv 2\ (5) \\ a\equiv 0\ (3) \end{array}\right. \xrightarrow{\text{solución}} a \equiv 12\ (15) \xrightarrow{\text{con } a=12} \left\{\begin{array}{l} 12^{97}-36 \overset{(3)}{\equiv} 0 \\ 12^{97}-36 \overset{(9)}{\equiv} 4^{97}\cdot(3^2)^{48}\cdot 3 \overset{(9)}{\equiv} 0 \quad \checkmark \\ 12^{97}-36 \overset{(27)}{\equiv} 4^{97}\cdot(3^3)^{32}\cdot 3^1 - 9 \overset{(27)}{\equiv} -9 \overset{(27)}{\not\equiv} 0 \end{array}\right.$$

$$\left\{\begin{array}{l} a\equiv 3\ (5) \\ a\equiv 0\ (3) \end{array}\right. \xrightarrow{\text{solución}} a \equiv 3\ (15)$$

$$\left\{\begin{array}{l} a\equiv 4\ (5) \\ a\equiv 0\ (3) \end{array}\right. \xrightarrow{\text{solución}} a \equiv 9\ (15) \xrightarrow{\text{con } a=9} \left\{\begin{array}{l} 9^{97}-36 \overset{(3)}{\equiv} 0 \\ 9^{97}-36 \overset{(9)}{\equiv} 0 \to (9^{97}-36 : 135) = 9 \quad \checkmark \\ 9^{97}-36 \overset{(27)}{\equiv} (3^3)^{64}\cdot 3^2 - 9 \overset{(27)}{\equiv} -9 \overset{(27)}{\not\equiv} 0 \end{array}\right.$$

Después de fumarme eso: $(a^{97} - 36 : 135) \in \{1, 9\}$, porque todas las soluciones cumplen que:
$3 \mid a^{97} \Rightarrow 9 \mid a^{97} \Rightarrow 27 \mid a^{97}$ y como $9 \mid 36$ y $27 \nmid 36$ siempre el mayor divisor de la expresión va a ser 9.
No estoy súper convencido. ¿Podría ocurrir que en algún caso de 27?

Ejercicios de la guía:

1.

---

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

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

Busco solución particular con algo parecido a Euclides:

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

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?

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

---

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

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

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

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

---

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

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

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

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

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

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

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) $\begin{cases} ^{1}\ a \equiv 1\ (12) \\ ^{2}\ a \equiv 7\ (10) \\ ^{3}\ a \equiv 4\ (9) \end{cases}$

---

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 $p \perp 71$, $\to 71^{22283} \equiv 71^{r_{10}(22283)}\ (11) \equiv 71^3\ (11) \to a \equiv 5^3\ (11) \quad \checkmark$

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

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

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

---

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

---

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

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

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

Hacer!

---

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) Hacer!

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:

$$\begin{cases} \sum\limits_{i=1}^{1759} i^{42} \equiv X\ (7) \ 8^1 \xrightarrow[\text{si } p\nmid i \to i^{42} = (i^6)^7 \equiv 1\ (7)]{7 \text{ es primo, uso Fermat}} \sum\limits_{i=1}^{1759} i^{42} = \sum\limits_{i=1}^{1759} (i^6)^7 \xrightarrow{251\cdot 7 + 2 = 1759} \\ \sum\limits_{i=1}^{1759} (i^6)^7 \overset{(7)}{\equiv} 251\cdot((1^6)^7 + (2^6)^7 + (3^6)^7 + (4^6)^7 + (5^6)^7 + (6^6)^7 + (7^6)^7) + ((1^6)^7 + (2^6)^7 + (3^6)^7 + (4^6)^7) \\ \sum\limits_{i=1}^{1759} (i^6)^7 \overset{(7)}{\equiv} 251\cdot(1+1+1+1+1+1+0) + (1+1+1+1) = 251\cdot 6 + 4 \overset{(7)}{\equiv} 3 \\ \xrightarrow{8^1} \boxed{X \equiv 3\ (7)} \end{cases}$$

Ahora se labura el módulo 8.

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

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

---

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

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

$$\to \left\{\begin{array}{l}
X^{45} \equiv 33\ (23) \to X^{45} \equiv 10\ (23) \xrightarrow[X^{22}\equiv 1\ (23)]{23 \text{ primo y } 23 \nmid X} X^{22}X^{22}X^1 \overset{(23)}{\equiv} X \equiv 10\ (23) \\
X^{45} \equiv 10\ (2) \to X^{45} \equiv 0\ (2) \xrightarrow[\text{si mismo impar veces}]{X \text{ multiplicado por}} X \equiv 0\ (2)
\end{array}\right.$$

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

---

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

Quiero que ocurra algo así: $\left\{\begin{array}{l} 25^{70} \equiv 0\ (d) \to 5^{140} \equiv 0\ (d) \\ d \equiv 2\ (9) \\ d \equiv 3\ (11) \end{array}\right.$. De la primera ecuación queda que el divisor $d = 5^{\alpha}$ con α compatible con las otras ecuaciones. $\to \left\{\begin{array}{l} 5^{\alpha} \equiv 2\ (9) \\ 5^{\alpha} \equiv 3\ (11) \end{array}\right.$

$\to$ Usaré viejo truco de exponenciales de módulo periódicas:

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

El sistema $\left\{ \begin{array}{l} \alpha \equiv 5\ (9) \\ \alpha \equiv 2\ (5) \end{array} \right.$ se resuelve para $\alpha \equiv 32\ (45)$ y además $0 < \alpha \leq 140$ lo que se cumple para $\alpha = 45k + 32 = \left\{ \begin{array}{lll} 32 & \text{si} & k=0 \\ 77 & \text{si} & k=1 \\ 122 & \text{si} & k=2 \end{array} \right\} \to \boxed{\mathcal{D}_+(25^{70}) = \{5^{32}, 5^{77}, 5^{122}\}}$