Apunte Único: Álgebra I - Práctica 5

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

última actualización 23/01/26 @ 22:38

Choose your destiny:

(dobleclick en los ejercicio para saltar)

- Notas teóricas
- Ejercicios de la guía:

- Ejercicios de Parciales

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

¡Recomendación para sacarle jugo al apunte!

Estudiar con resueltos puede ser un arma de doble filo. Si estás trabado, antes de saltar a la solución que hizo otra persona:

1. Mirar la solución ni bien te trabás, te *condicionas pavlovianamente* a **no** pensar. Necesitás darle tiempo al cerebro para llegar a la solución.
2. Intentá un ejercicio similar, pero **más fácil**.
3. ¿No sale el fácil? Intentá uno **aún más fácil**.
4. Fijate si tenés un ejercicio similar hecho en clase. Y mirá ese, así no quemás el ejercicio de la guía.
5. Tomate 2 minutos para formular una pregunta que realmente sea lo que **no** entendés. Decir *'no me sale'* ♯+. Escribí esa pregunta, vas a dormir mejor.

Ahora sí mirá la solución.

Si no te salen los ejercicios fáciles sin ayuda, no te van a salir los ejercicios más difíciles: Sentido común.

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

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

Mirá los videos de las teóricas:
de Teresa que son buenísimos.

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

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

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

Esta Guía 5 que tenés se actualizó por última vez:
23/01/26 @ 22:38
Escaneá el QR para bajarte (quizás) una versión más nueva:

Guía 5

El resto de las guías repo en github para descargar las guías con los últimos updates.

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

Notas teóricas:

Diofánticas:

- Sea $aX + bY = c$ con $a, b, c \in \mathbb{Z}$, $a \neq 0 \quad$ y $\quad b \neq 0$ y sea

$$\boxed{S = \{(X,Y) \in \mathbb{Z}^2 : aX + bY = c\} \neq \varnothing \iff (a:b) \,|\, c}$$

¡Coprimizar siempre que se pueda!: Las soluciones de S son las mismas que las de S coprimizado.

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

- Las solución general del sistema S coprimizado :

$$\boxed{S = \left\{(X,Y) \in \mathbb{Z}^2 : (X,Y) = \underbrace{(X_0, Y_0)}_{\text{Solución particular}} + k \cdot \overbrace{(-b', a')}^{\text{Solución homogéneo}}, \text{ con } k \in \mathbb{Z}\right\}}$$

Ecuaciones de congruencia:

- $aX \equiv c\ (b)$ con $a, b \neq 0$

¡Coprimizar siempre que se pueda!: Las soluciones de la ecuación original son las mismas que las de la ecuación coprimizada.

$$\boxed{aX \equiv c\ (b) \xleftrightarrow[c' = \frac{c}{(a:b)}]{a' = \frac{a}{(a:b)} \quad \text{y} \quad b' = \frac{b}{(a:b)}} a'X \equiv c'\ (b')}$$

- Ojo con el " $\iff$ ": Si vas a multiplicar la ecuación por algún número d y se te ocurre poner un $\iff$ conectando la operación justificá así:

$$\boxed{aX \equiv c\ (b) \underset{d \perp b}{\iff} daX \equiv dc\ (b)}$$

Porque si $d \not\perp b$ no vale la vuelta ($\Leftarrow$) en el " $\iff$ ", y la cagás.

- Si te ponés a hacer cuentas en $aX \equiv c\ (b)$ *sin que* $a \perp b$, la vas a cagar. Yo te avisé .

Sistemas de ecuaciones de congruencia: Teorema chino del resto

- Sean $m_1, \dots m_n \in \mathbb{Z}$ coprimos dos a dos, es decir que $\forall i \neq j$, se tiene $m_i \perp m_j$, entonces, dados $c_1, \dots, c_n \in \mathbb{Z}$ cualesquiera, el sistema de ecuaciones de congruencia

$$\begin{cases} X \equiv c_1\ (m_1) \\ X \equiv c_2\ (m_2) \\ \quad\vdots \\ X \equiv c_n\ (m_n) \end{cases} \rightsquigarrow X \equiv x_0\ (m_1 \cdot m_2 \cdots m_n),$$

tiene solución y esa solución, x_0 cumple $0 \leq x_0 < m_1 \cdot m_2 \cdots m_n$.

Pequeño teorema de Fermat

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

1) $a^p \equiv a\ (p)$

2) $p \nmid a \implies a^{p-1} \equiv 1 \ (p)$

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

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

Amigate con ésta porque se usa mucho. Marco el $p-1$ en rojo, porque por alguna razón uno se olvida.

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

$$\boxed{a^d \equiv 1 \ (p) \implies d \,|\, (p-1)}$$

Atento a esto que en algún que otro ejercicio uno encuentra un valor usando PTF, pero eso no quiere decir que no haya otro valor menor! Que habrá que encontrar con otro método.

Nota: Cuando p es primo y a un entero cualquiera, será obvio o no, pero: $\boxed{p \nmid a \Leftrightarrow p \perp a}$. Se usan indistintamente.

Ejercicios de la guía:

---

1. Determinar, cuando existan, todos los $(a, b) \in \mathbb{Z}^2$ que satisfacen

i) $7a + 11b = 10$ ii) $20a + 16b = 36$ iii) $39a - 24b = 6$ iv) $1555a - 300b = 11$

---

i) Tiene solución, pues $(7 : 11) = 1 \mid 10$
Una solución particular es $(a_0, b_0) = (3, -1)$. Luego, la solución general es

$$\boxed{(a, b) = (-11k + 3, 7k - 1), k \in \mathbb{Z}}$$

ii) Tiene solución, pues $(20 : 16) = 4 \mid 36$
Coprimizando la ecuación:

$$20a + 16b = 36 \leftrightsquigarrow 5a + 4b = 9$$

Una solución particular de la ecuación equivalente es $(a_0, b_0) = (1, 1)$. Luego, la solución general es

$$\boxed{(a, b) = (4k + 1, -5k + 1), k \in \mathbb{Z}}$$

iii) Tiene solución, pues $(39 : -24) = 3 \mid 6$
Coprimizando la ecuación:

$$39a - 24b = 6 \leftrightsquigarrow 13a - 8b = 2$$

Una solución particular de la ecuación equivalente es $(a_0, b_0) = (2, 3)$. Luego, la solución general es

$$\boxed{(a, b) = (8k + 2, 13k + 3), k \in \mathbb{Z}}$$

iv) No tiene solución, pues $(1555 : -300) = 5 \nmid 11$

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

---

2. Determinar todos los (a, b) que simultáneamente $4 \mid a$, $8 \mid b$ y $33a + 9b = 120$.

Para que la ecuación tenga solución necesito que el MCD entre 33 y 9 divida al 120, es decir:

$$(33 : 9) \mid 120 \implies 33a + 9b = 120$$

y dado que $(33 : 9) = 3$ y $3 \mid 120$ sé que puedo encontrar dicha solución. Pero tengo más restricciones sobre los valores de a y b.

$$\begin{cases} 4 \mid a \overset{\text{def}}{\iff} a = 4k_1 \\ 8 \mid b \overset{\text{def}}{\iff} b = 8k_2 \end{cases} \quad \bigstar^1$$

Pongo esa info en la ecuación:

$$\xrightarrow{\bigstar^1} 33a + 9b = 120 \to 132k_1 + 72k_2 = 120$$

Siempre que puedo tengo que coprimizar:

$$132k_1 + 72k_2 = 120 \overset{\text{coprimizo}}{\iff} 11k_1 + 6k_2 = 10$$

Busco *solución particular* con Euclides, busco escribir al número 1 como combinación entera de 11 y 6:

$$\begin{cases} 11 &= 6 \cdot 1 + 5 \\ 6 &= 5 \cdot 1 + 1 \end{cases} \implies 1 = 11 \cdot (-1) + 6 \cdot 2 \text{★}^2$$

Obtengo así la *solución particular*:

$$\xrightarrow{\text{★}^2 \times 10} 10 = 11 \cdot (-10) + 6 \cdot 20 \implies (k_1, k_2) = (-10, 20)$$

La solución del homogéneo queda:

$$11k_{1_h} + 6k_{2_h} = 0 \implies (k_{1_h}, k_{2_h}) = (-6, 11)$$

Por lo que la solución general:

$$(k_{1_g}, k_{2_g}) = (k_{1_p}, k_{2_p}) + k \cdot (k_{1_h}, k_{2_h}) = (-10, 20) + k \cdot (-6, 11) = (-10 - 6k, 20 + 11k)$$

Pero me pidieron los pares (a, b) con $a \mid 4$ y $b \mid 8$:

$$\xrightarrow{\text{★}^1} \boxed{(a, b) = (-40 - 24k, 160 + 88k)}$$

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

---

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

Armo diofántica con enunciado, tengo en cuenta que $A \geq 0$ y $B \geq 0$, dado que son productos físicos 🧠.
La ecuación *presupuestaria* queda:

$$39A + 48B = 135$$

Siempre que puedo coprimizar lo hago:

$$(A : B) = 3 \implies 13A + 16B = 45,$$

Veo que hay solución dado que,

$$(13 : 16) \mid 45$$

Resuelvo a ojo. Si no lo ves hacé Euclides combinación entera y zarasa:

$$\boxed{(A, B) = (1, 2)}$$

Dale las gracias y un poco de amor ♥ a los que contribuyeron! Gracias por tu aporte:
naD GarRaz Román LG

---

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

i) $17X \equiv 3\ (11)$ ii) $56X \equiv 28\ (35)$ iii) $56X \equiv 2\ (884)$ iv) $78X \equiv 30\ (12126)$

- Algunos cálculos salen a ojo. Recordar que una ecuación de congruencia se puede pensar expresar como una diofántica:

$$aX \equiv r\ (b) \leftrightsquigarrow a \cdot X + b \cdot Y = r$$

- Coprimizar siempre que se pueda.

i)
$$17X \equiv 3\ (11) \iff 6X \equiv 3\ (11) \underset{(\Leftarrow)2 \perp 11}{\overset{\times 2}{\Longleftrightarrow}} \boxed{X \equiv 6\ (11)}$$

ii)
$$56X \equiv 28\ (35) \iff 21X \equiv 28\ (35) \underset{(21:35)=7}{\overset{\text{coprimizo}}{\Longleftrightarrow}} 3X \equiv 4\ (5) \underset{(\Leftarrow)7 \perp 5}{\overset{\times 7}{\Longleftrightarrow}} \boxed{X \equiv 3\ (5)}$$

iii) Empiezo coprimizando:
$$56X \equiv 2\ (884) \iff 28X \equiv 1\ (442)$$
Esa ecuación tiene solución, si y solo si $(28:442) \mid 1$, peeeeero no es el caso *cause* $28 \not\perp 442$ así que:
$$\boxed{X = \varnothing}$$

iv) Empiezo coprimizando:
$$78X \equiv 30\ (12126) \underset{(78:12126)=6}{\overset{\text{coprimizar}}{\Longleftrightarrow}} 13X \equiv 5\ (2021),$$
Dado que $\overbrace{(13:2021)}^{1} \mid 5$ hay solución ☺.

Busco solución particular con Euclides. Escribo al 5 como combinación entera de 13 y 2021:
$$\begin{cases} 2021 = 13 \cdot 155 + 6 \\ 13 = 6 \cdot 2 + 1 \end{cases} \underset{\text{de } 13 \text{ y } 2021}{\overset{1 \text{ como combinación}}{\Longrightarrow}} 1 = 13 \cdot 311 + 2021 \cdot (-2) 1 = 13 \cdot 311 + 2021 \cdot (-2) \bigstar^1$$

Multiplico $\bigstar^1$ por 5 para obtener la expresión que buscaba:
$$\bigstar^1 \underset{(\Leftarrow)5 \perp 2021}{\overset{\times 5}{\Longleftrightarrow}} 5 = 13 \cdot 1555 + 2021 \cdot (-10)$$

De donde obtengo la *solución particular*:
$$13 \cdot \underbrace{1555}_{\substack{\text{Solución} \\ \text{particular}}} = 2021 \cdot 10 + 5 \underset{!!}{\overset{\text{Solución general, } X}{\Longrightarrow}} \boxed{X \equiv 1555\ (2021)}$$

Si no ves el paso !!, hacé el procedimiento para resolver la diofántica, $13X + 2021Y = 5$ que es equivalente a $13X \equiv 5\ (2021)$.

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

---

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

Este es parecido al **2.**. Voy a despejar de una ecuación y meter en la otra:
Despejo:
$$b \equiv 2a\ (5) \underset{}{\overset{\text{def}}{\Longleftrightarrow}} b = 5k + 2a \bigstar^1$$

Meto ahora en la otra ecuación:
$$28a + 10b = 26 \overset{\bigstar^1}{\Longleftrightarrow} 48a + 50k = 26$$

¿Esta última ecuación tiene solución? Sí, dado que: $(48:50) = 2$ y $2 \mid 26$.
Coprimizo:
$$24a + 25k = 13$$

A ojo veo que (si no se ve a ojo, se puede hacer Euclides):

$$(a,k) = q\cdot(-25,24)+(-13,13) \Leftrightarrow \begin{cases} a &= -13+(-25)q \\ k &= 13+24q \end{cases}$$

Let's corroborate: Uso esos valores para comprobar que se cumplen las ecuaciones del enunciado:

$$b = 5\cdot\underbrace{(13+24q)}_{k}+2\cdot\underbrace{(-13+(-25)q)}_{a} = 39+70q \xrightarrow[5]{\text{módulo}} b = 39+70q \equiv 4\ (5) \Leftrightarrow \boxed{b\equiv 4\ (5)}$$

Por otro lado:

$$2a = -26-50q \equiv -1\ (5)\ \equiv\ 4\ (5) \Leftrightarrow \boxed{2a\equiv 4\ (5)}$$

Concluyendo que efectivamente:

$$b \equiv 2a\ (5)$$

Dale las gracias y un poco de amor ♥ a los que contribuyeron! Gracias por tu aporte:
naD GarRaz M Poncini

---

6. Hallar el resto de la división de un entero a por 18, sabiendo que el resto de la división de $7a$ por 18 es 5.

Buscamos $r_{18}(a)$ sabiendo que $r_{18}(7a)=5$. Entonces, partimos de lo que sabemos:

$$r_{18}(7a)=5 \iff 7a\equiv 5\ (18) \xleftrightarrow{(5:18)=1} 5.7a \equiv 5.5\ (18) \iff 35a\equiv 25\ (18) \xleftrightarrow[25\equiv 7\ (18)]{35\equiv -1\ (18)} -a\equiv 7\ (18)$$

$$-a\equiv 7\ (18) \iff a\equiv -7\ (18) \iff a\equiv 11\ (18) \iff \boxed{r_{18}(a)=11}$$

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

---

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

$$110x+250y=100$$

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

La solución de la diofántica:

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

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

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

Buscamos posibles valores:

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

Que como ecuación de congruencia queda:

$$-36k \equiv 590\ (37) \Leftrightarrow k \equiv 35\ (37)$$

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

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

Veamos:

$$37^1 \mid (590+36k)^{4321} \xrightarrow[\text{primo}]{37 \text{ es}} 37 \mid 590+36k \overset{!}{\Rightarrow} 37^2 \mid (590+36k)^2$$
$$\Longrightarrow\ 37^2 \mid (590+36k)^2 \cdot (50+36k)^{4319} \Leftrightarrow 37^2 \mid (590+36k)^{4321}$$

De esa manera queda demostrado que

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

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

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

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

---

8. Hallar todos los $a \in \mathbb{Z}$ para los cuales $(2a-3 : 4a^2+10a-10) \neq 1$

Sea $d = (2a-3 : 4a^2+10a-10)$. Entonces:

$$\begin{cases} d \mid 2a-3 \xrightarrow{\times 2a} d \mid 4a^2-6a \\ d \mid 4a^2+10a-10 \end{cases} \quad \begin{cases} d \mid 4a^2-6a \\ d \mid 4a^2+10a-10 \end{cases} \xrightarrow{F_2-F_1} d \mid 16a-10$$

Luego, tenemos

$$\begin{cases} d \mid 16a-10 \\ d \mid 2a-3 \xrightarrow{\times(-8)} d \mid -16a+24 \end{cases} \xrightarrow{F_1+F_2} d \mid 14 \implies d \in \{1,2,7,14\}$$

Veo tabla de restos con $d=2$ con la expresión $2a-3$

$r_2(a)$	0	1
$r_2(2a-3)$	1	1

Entonces, como $2 \nmid 2a-3\ \ \forall a \in \mathbb{Z}$, tenemos que $d \neq 2$ y $d \neq 14\ \ \forall a \in \mathbb{Z}$.
De modo que queremos hallar los valores de a para los cuales $d=7$.
Veo la tabla de restos con $d=7$ con ambas expresiones.

$r_7(a)$	0	1	2	3	4	5	6
$r_7(2a-3)$	4	6	1	3	5	0	2
$r_7(4a^2+10a-10)$	4	4	5	0	3	0	5

Entonces, $d=7 \iff a \equiv 5\ (7)$. Particularmente, $d \neq 1 \iff \boxed{a \equiv 5\ (7)}$.

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

---

9. Describir los valores de $(5a+8 : 7a+3)$ en funcion de los valores de $a \in \mathbb{Z}$

Sea $d = (5a+8 : 7a+3)$. Entonces:

$$\begin{cases} d \mid 5a+8 \xrightarrow{\times 7} d \mid 35a+56 \\ d \mid 7a+3 \xrightarrow{\times 5} d \mid 35a+15 \end{cases} \xrightarrow{F_1-F_2} d \mid 41 \implies d \in \{1,41\}$$

Ahora debemos ver cuando $41 \mid 5a+8 \ \wedge \ 41 \mid 7a+3$ simultáneamente. Veamos primero cuando $41 \mid 7a+3$:

$$41 \mid 7a+3 \iff 7a+3 \equiv 0 \ (41) \iff 7a \equiv -3 \ (41) \xleftrightarrow{(6:41)=1} 6 \cdot 7a \equiv 6 \cdot (-3) \ (41) \iff 42a \equiv -18 \ (41) \iff$$

$$\iff a \equiv 23 \ (41)$$

Ahora debemos ver si cuando $a \equiv 23 \ (41)$ se verifica que $41 \mid 5a+8$. Veamoslo:

$$41 \mid 5a+8 \iff 5a+8 \equiv 0 \ (41) \xleftrightarrow{a \equiv 23 \ (41)} 5 \cdot 23 + 8 \equiv 0 \ (41) \iff 123 \equiv 0 \ (41) \iff 41 \mid 123 \quad \checkmark$$

Luego, $41 \mid 5a+8 \ \wedge \ 41 \mid 7a+3 \iff a \equiv 23 \ (41)$
De modo que

$$\begin{cases} \boxed{d = 41} \ si \ a \equiv 23 \ (41) \\ \boxed{d = 1} \ si \ a \not\equiv 23 \ (41) \end{cases}$$

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

---

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

i) $\begin{cases} a \equiv 3 \ (10) \\ a \equiv 2 \ (7) \\ a \equiv 5 \ (9) \end{cases}$ ii) $\begin{cases} a \equiv 1 \ (6) \\ a \equiv 2 \ (20) \\ a \equiv 3 \ (9) \end{cases}$ iii) $\begin{cases} a \equiv 1 \ (12) \\ a \equiv 7 \ (10) \\ a \equiv 4 \ (9) \end{cases}$

---

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

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

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

$$a \equiv 3 \ (10) \xleftrightarrow{\text{def}} a = 10k + 3 \overset{(7)}{\equiv}$$

Reemplazo ahora en $\bigstar^2$:

$$10k + 3 \equiv 2 \ (7) \Leftrightarrow 3k \equiv 6 \ (7) \xleftrightarrow{3 \perp 7} k \equiv 2 \ (7) \xleftrightarrow{\text{def}} k = 7j + 2$$

Reemplazo el valor de k en a:

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

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

$$70j + 23 \equiv 5 \ (9) \Leftrightarrow 7j \equiv 0 \ (9) \xleftrightarrow{7 \perp 9} j \equiv 0 \ (9) \xleftrightarrow{\text{def}} j = 9h$$

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

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

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

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

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

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

---

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

i) $\begin{cases} 3a \equiv 4\ (5) \\ 5a \equiv 4\ (6) \\ 6a \equiv 2\ (7) \end{cases}$ ii) $\begin{cases} 3a \equiv 1\ (10) \\ 5a \equiv 3\ (6) \\ 9a \equiv 1\ (14) \end{cases}$ iii) $\begin{cases} 15a \equiv 10\ (35) \\ 21a \equiv 15\ (8) \\ 18a \equiv 24\ (30) \end{cases}$

Ejercicio para practica resolución de sistemas de ecuaciones de congruencia. Acomodar, coprimizar, Teorema Chino del resto y resolver.

i) Este no tiene mucha rosca, no hay nada que coprimizar, los divisores son coprimos 2 a 2. Debería ser cuestión de simplificar el sistema y luego resolver despejando:

$$\begin{cases} 3a \equiv 4\ (5) \\ 5a \equiv 4\ (6) \\ 6a \equiv 2\ (7) \end{cases} \overset{!}{\Leftrightarrow} \begin{cases} a \equiv 3\ (5) \bigstar^1 \\ a \equiv 2\ (6) \bigstar^2 \\ a \equiv 5\ (7) \bigstar^3 \end{cases}$$

Todos los divisores son coprimos 2 a 2, así que por el THC debería poder encontrar una solución:

$$\bigstar^1 a = 5k + 3 \overset{\text{meto en } \bigstar^2}{\Longrightarrow} 5k + 3 \overset{(6)}{\equiv} -k + 3 \equiv 2\ (6) \Leftrightarrow k \equiv 1\ (6) \overset{\text{en } \bigstar^1}{\Longrightarrow} a = 5(6j + 1) + 3 = 30j + 8$$

Hasta el momento:

$$a = 30j + 8 \overset{\text{meto en } \bigstar^3}{\Longrightarrow} 30j + 8 \equiv 5\ (7) \Leftrightarrow j \equiv 2\ (7) \implies a = 30 \cdot (7h + 2) + 8 = 210h + 68$$

Por lo tanto la solución al sistema i):

$$\boxed{a \equiv 68\ (210)}$$

ii) Acá los divisores no son coprimos, habría que *quebrar* y estudiar la *compatibilidad* de las ecuaciones.

Primero simplifico un poco el sistema:

$$\begin{cases} 3a \equiv 1\ (10) \\ 5a \equiv 3\ (6) \\ 9a \equiv 1\ (14) \end{cases} \overset{!}{\Leftrightarrow} \begin{cases} a \equiv 7\ (10) \quad \rightsquigarrow \quad \begin{cases} a \equiv 1\ (2) \\ a \equiv 2\ (5) \end{cases} \\ a \equiv 3\ (6) \quad \rightsquigarrow \quad \begin{cases} a \equiv 1\ (2) \\ a \equiv 0\ (3) \end{cases} \\ a \equiv 11\ (14) \quad \rightsquigarrow \quad \begin{cases} a \equiv 1\ (2) \\ a \equiv 4\ (7) \end{cases} \end{cases}$$

La papa está en el divisor 2, pero como aparece con el mismo resto en todas las ecuaciones no tenemos problemas de *compatibilidad*.

$$\begin{cases} 3a \equiv 1\ (10) \\ 5a \equiv 3\ (6) \\ 9a \equiv 1\ (14) \end{cases} \overset{!}{\rightsquigarrow} \begin{cases} a \equiv 2\ (5) \bigstar^1 \\ a \equiv 0\ (3) \bigstar^2 \\ a \equiv 11\ (14) \bigstar^3 \end{cases}$$

Tengo todos los divisores coprimos. Resolver este último sistema me va a dar las soluciones del problema original.

Ahora hay que resolver:

$$\bigstar^1 a = 5k+2 \xrightarrow[\bigstar^2]{\text{meto en}} 5k+2 \overset{(3)}{\equiv} -k+2 \equiv 0\ (3) \Leftrightarrow k \equiv 2\ (3) \xrightarrow[\bigstar^1]{\text{en}} a = 5(3j+2)+2 = 15j+12$$

Hasta el momento:

$$a = 15j+12 \xrightarrow[\bigstar^3]{\text{meto en}} 15j+12 \equiv 11\ (14) \Leftrightarrow j \equiv 13\ (14) \implies a = 15\cdot(14h+13)+12 = 210h+207$$

Por lo tanto la solución al sistema ii):

$$\boxed{a \equiv 207\ (210)}$$

iii) Acá los divisores no son coprimos, parecido al anterior, pero no tanto.

Primero simplifico un poco el sistema, siempre coprimizo si se puede:

$$\begin{cases} 15a \equiv 10\ (35) \\ 21a \equiv 15\ (8) \\ 18a \equiv 24\ (30) \end{cases} \xrightarrow[\text{coprimizar}]{!!} \begin{cases} 3a \equiv 2\ (7) \\ 5a \equiv 7\ (8) \\ 3a \equiv 4\ (5) \end{cases} \Leftrightarrow \begin{cases} a \equiv 3\ (7) \bigstar^1 \\ a \equiv 3\ (8) \bigstar^2 \\ a \equiv 3\ (5) \bigstar^3 \end{cases}$$

Tengo todos los divisores coprimos. Resolver este último sistema me va a dar las soluciones del problema original.

Ahora hay que resolver:

$$\bigstar^1 a = 7k+3 \xrightarrow[\bigstar^2]{\text{meto en}} 7k+3 \equiv 3\ (8) \Leftrightarrow k \equiv 0\ (8) \xrightarrow[\bigstar^1]{\text{en}} a = 7(8j+0)+3 = 56j+3$$

Hasta el momento:

$$a = 56j+3 \xrightarrow[\bigstar^3]{\text{meto en}} 56j+3 \equiv 3\ (5) \Leftrightarrow j \equiv 0\ (5) \implies a = 56\cdot(5h+0)+3 = 280h+3$$

Por lo tanto la solución al sistema iii):

$$\boxed{a \equiv 3\ (280)}$$

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

12.

i) Sabiendo que los restos de la división de un entero a por 6, 10 y 8 son 5, 3 y 5 respectivamente, hallar los posibles restos de la división de a por 480.

ii) Hallar el menor entero positivo a tal que el resto de la división de a por 21 e 13 y el resto de la división de $6a$ por 15 es 9.

---

i) Nos dicen que:

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

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

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

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

La cosa quedaría así:

$$\begin{cases} a \equiv 5\ (6) \\ a \equiv 3\ (10) \\ a \equiv 5\ (8) \end{cases} \rightsquigarrow \begin{cases} a \equiv 2\ (3) \bigstar^1 \\ a \equiv 3\ (5) \bigstar^2 \\ a \equiv 5\ (8) \bigstar^3 \end{cases}$$

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

$$\bigstar^1 a = 3j + 2 \xrightarrow[\text{en } \bigstar^2!]{\text{reemplazo}} j \equiv 2\ (5) \overset{\text{def}}{\iff} j = 5k + 2$$

$$\xrightarrow[\text{en } a]{\text{reemplazo}} a = 3(5k+2) + 2 = 15k + 8 \xrightarrow[\text{en } \bigstar^3!]{\text{reemplazo}} k \equiv 3\ (8) \overset{\text{def}}{\iff} k = 8i + 3$$

$$\xrightarrow[\text{en } a]{\text{reemplazo}} a = 15(8i+3) + 8 = 120i + 53 \iff a \equiv 53\ (120)$$

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

$$a \equiv X\ (480)$$

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

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

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

ii) Hay que encontrar el menor entero positivo del sistema:

$$\begin{cases} a \equiv 13\ (21) \\ 6a \equiv 9\ (15) \end{cases}$$

No son coprimos los divisores y se puede coprimizar la segunda ecuación:

$$\begin{cases} a \equiv 13\ (21) \\ 6a \equiv 9\ (15) \end{cases} \xrightarrow[\text{coprimizo}]{!} \begin{cases} a \equiv 13\ (21) \\ 2a \equiv 3\ (5) \end{cases} \Leftrightarrow \begin{cases} a \equiv 13\ (21) \bigstar^1 \\ a \equiv 4\ (5) \bigstar^2 \end{cases}$$

Ahora hay que resolver:

$$\bigstar^1 a = 21k + 13 \xrightarrow[\bigstar^2]{\text{meto en}} 21k + 13 \equiv 4\ (5) \Leftrightarrow k \equiv 1\ (5) \xrightarrow[\bigstar^1]{\text{en}} a = 21(5j+1) + 13 = 105j + 34$$

Por lo tanto la solución al sistema:

$$a \equiv 34\ (105)$$

Nos piden el entero positivo más chico que cumpla eso:

$$\boxed{a = 34}$$

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

---

13. En un depósito se almacenan latas de gaseosa. El viernes por la noche, un empleado realizó un control de inventario y observó que:

- Al poner las latas de cajas de 12 unidades sobraban 4.
- Al poner las latas de cajas de 63 unidades sobraban 43.
- Había por lo menos 12.600 latas y no más de 13.000, pero no tomó nota de la cantidad eXacta.

¿Cuántas latas de gaseosa había en el depósito el viernes por la noche?

Ejercicio en el que hay que armar el sistemita de ecuaciones para poder resolver.

Voy a ponerle el poco original nombre $\underline{X}$ al total de latas. Del enunciado salen las condiciones:

$$\begin{cases} X \equiv 4 \ (12) \\ X \equiv 43 \ (63) \\ 12.600 \leq X \leq 13.000 \bigstar^{1} \end{cases}$$

Los divisores no son coprimos habrá que quebrar:

$$\begin{cases} X \equiv 4 \ (12) \rightsquigarrow \begin{cases} X \equiv 1 \ (3) \\ X \equiv 0 \ (4) \end{cases} \\ X \equiv 43 \ (63) \rightsquigarrow \begin{cases} X \equiv 1 \ (3) \\ X \equiv 1 \ (7) \end{cases} \end{cases}$$

El sistema es compatible. Me quedo con la equación que tiene el divisor potencia de 3 más grande. De no hacerlo obtendría soluciones de más.
Resuelvo el siguiente sistema:

$$\begin{cases} X \equiv 4 \ (12) \\ X \equiv 43 \ (63) \end{cases} \rightsquigarrow \begin{cases} X \equiv 0 \ (4) \\ X \equiv 43 \ (63) \end{cases}$$

Este sistema tiene divisores coprimos y por el TCHR puedo encontrar una solución:

$$X = 4k$$
$$4k \equiv 43 \ (63) \overset{!}{\Leftrightarrow} k \equiv 58 \ (63) \overset{\text{def}}{\Longleftrightarrow} k = 63j + 58$$
$$X = 4(63j + 58) = 252j + 232$$

Ahora hay que usar la condición $\bigstar^{1}$:

$$12.600 \leq 252j + 232 \leq 13.000 \Leftrightarrow 49.07\cdots \leq j \leq 50.\bar{6} \Leftrightarrow j = 50$$

Se puede concluir entonces que la cantidad de latas es:

$$\boxed{X = 252 \cdot 50 + 232 = 12832}$$

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

---

14. Hallar los posibles restos de dividir a un entero a por 238 sabiendo que $a^2 \equiv 21 \ (238)$.

$$a^2 \equiv 21\ (238) \rightsquigarrow \begin{cases} a^2 \equiv 1\ (2) \overset{!}{\Leftrightarrow} a \equiv 1\ (2) \\ a^2 \equiv 0\ (7) \overset{!}{\Leftrightarrow} a \equiv 0\ (7) \\ a^2 \equiv 4\ (17) \overset{\bigstar^1}{\Longleftrightarrow} \begin{cases} a \equiv 2\ (17) \\ \text{o} \\ a \equiv 15\ (17) \end{cases} \end{cases}$$

Donde $\bigstar^1$:

$r_{17}(a)$	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
$r_{17}(a^2)$	0	1	4	9	16	8	2	15	13	13	15	2	2	16	6	4	1

Y el resto es historia. Dos hermosos sistemas para resolver:

$$\begin{cases} a \equiv 1\ (2) \bigstar^2 \\ a \equiv 0\ (7) \bigstar^3 \\ a \equiv 2\ (17) \bigstar^4 \end{cases} \quad \text{y} \quad \begin{cases} a \equiv 1\ (2) \bigstar^2 \\ a \equiv 0\ (7) \bigstar^3 \\ a \equiv 15\ (17) \bigstar^5 \end{cases}$$

$$\bigstar^2 a \equiv 1\ (2) \overset{\text{def}}{\Longleftrightarrow} a = 2k+1 \xrightarrow[\text{en } \bigstar^3]{\text{meto}} 2k+1 \equiv 0\ (7) \Leftrightarrow k \equiv 3\ (7) \xrightarrow[\text{en } a]{\text{reemplazo}} a = 2(7h+3)+1 = 14h+7 \bigstar^6$$

Ese valor de $\bigstar^6$ lo uso en las otras dos ecuaciones:

$$\xrightarrow[\bigstar^4]{\text{meto en}} 14h+7 \equiv 2\ (17) \overset{\times 11}{\underset{11 \perp 17}{\Longleftrightarrow}} h \equiv 13\ (17) \xrightarrow[\text{en } a]{\text{reemplazo}} a = 14(17j+13)+7 = 238j+189$$

$$\xrightarrow[\bigstar^5]{\text{meto en}} 14h+7 \equiv 15\ (17) \overset{\times 11}{\underset{11 \perp 17}{\Longleftrightarrow}} h \equiv 3\ (17) \xrightarrow[\text{en } a]{\text{reemplazo}} a = 14(17j+3)+7 = 238j+49$$

Se termina el ejercicio. Los valores que cumplen lo pedido:

$$\boxed{a \equiv 189\ (238) \quad \text{y} \quad a \equiv 49\ (238)}$$

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

---

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

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

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

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

---

a) Escribo como ecuación de congruencia:

$$33^{1427} \equiv 3^{1427}\ (5)$$

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

$$33^{1427} \equiv 3^{1427}\ (5) \overset{\text{PTF}}{\Longleftrightarrow} 3^{1427} \equiv 3^3\ (5) \quad \text{y} \quad 3^3 = 27 \overset{(5)}{\equiv} 2$$

Por lo tanto:

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

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

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

Por lo tanto:

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

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

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

Nota que puede ser de interés:

Con la calculadora salen fácil los cálculos, pero está bueno poder calcularlos a mano masajeando las potencias, onda $8^6 = (8^2)^3 = 64^3 \overset{(13)}{\equiv} (-1)^3 = -1 \overset{(13)}{\equiv} 12$

Un par de cuentas y calcular congruencia y queda:

$$a \equiv 9 \ (13)$$

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

---

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

i) $2^{194}X \equiv 7 \ (97)$ ii) $5^{86}X \equiv 3 \ (89)$

---

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

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

La ecuación queda:

$$4^{97}X \equiv 7 \ (97) \overset{\overset{97 \nmid 4}{\text{PTF}}}{\iff} 4X \equiv 7 \ (97) \overset{\overset{24 \perp 97}{!!}}{\iff} X \equiv -168 \ (97) \Leftrightarrow X \equiv 26 \ (97)$$

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

$$5^{86}X \equiv 3 \ (89) \overset{\overset{89 \perp 5^2}{!}}{\iff} 5^{88}X \equiv 75 \ (89) \overset{\overset{89 \nmid 5}{}}{\iff} X \equiv 75 \ (89)$$

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

---

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

a) $728 \mid a^{27} - a^3$ b) $\frac{2a^7}{35} + \frac{a}{7} - \frac{a^3}{5} \in \mathbb{Z}$

---

a) Escribiendo la consigna como ecuación de congruencia:

$$728 \mid a^{27} - a^3 \overset{\text{def}}{\iff} a^{27} - a^3 \equiv 0 \ (728)$$

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

$$a^{27} - a^3 \equiv 0 \ (728) \leftrightsquigarrow \begin{cases} a^{27} - a^3 \equiv 0 \ (8) \bigstar^1 \\ a^{27} - a^3 \equiv 0 \ (7) \bigstar^2 \\ a^{27} - a^3 \equiv 0 \ (13) \bigstar^3 \end{cases}$$

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

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

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

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

Por lo que si $r_8(a)$ es impar, también mostramos que ★[1] es válida:

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

Ahora vienen casos más agradables (espero) con divisores primos que nos permiten usar el PTF.
Analizo ★[2]

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

Por lo que ★[2] se cumple para todo valor de a.
Analizo ★[3] muuuy parecido:

$$a^3 \cdot (a^{24} - 1) \equiv 0 \ (13) \Leftrightarrow \begin{cases} 0^3 \cdot (0^{24} - 1) \equiv 0 \ (13) & \text{si } 13 \mid a \\ \underset{!}{\overset{\text{PTF}}{\iff}} a^3 \cdot (a^0 - 1) \equiv 0 \ (13) \Leftrightarrow 0 \equiv 0 \ (13) & \text{si } 7 \nmid a \end{cases}$$

Por lo que ★[3] se cumple para todo valor de a.
Queda así demostrado que:

$$\begin{cases} a^{27} - a^3 \equiv 0 \ (8) \\ a^{27} - a^3 \equiv 0 \ (7) \\ a^{27} - a^3 \equiv 0 \ (13) \end{cases} \rightsquigarrow a^{27} - a^3 \equiv 0 \ (728) \overset{\text{def}}{\iff} 728 \mid a^{27} - a^3 \qquad \forall a \in \mathbb{Z}$$

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

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

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

$$2a^7 + 5a - 7a^3 \equiv 0 \ (35) \rightsquigarrow \begin{cases} 2a^7 + 5a - 7a^3 \equiv 0 \ (7) \text{★}[1] \\ 2a^7 + 5a - 7a^3 \equiv 0 \ (5) \text{★}[2] \end{cases}$$

Empiezo por ★[1]:

$$2a^7 + 5a - 7a^3 \equiv 0 \ (7) \Leftrightarrow 2a^7 + 5a \equiv 0 \ (7) \Leftrightarrow \begin{cases} \text{si } 7 \mid a \implies 0 \equiv 0 \ (7) \\ \text{si } 7 \nmid a \underset{!}{\overset{\text{PTF}}{\implies}} 7a \equiv 0 \ (7) \Leftrightarrow 0 \equiv 0 \ (7) \end{cases}$$

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

$$2a^7 + 5a - 7a^3 \equiv 0 \ (7) \qquad \forall a \in \mathbb{Z}$$

Ahora analizo ★[2]:

$$2a^7 + 5a - 7a^3 \equiv 0 \ (5) \Leftrightarrow 2a^7 - 2a^3 \equiv 0 \ (5) \Leftrightarrow \begin{cases} \text{si } 5 \mid a \implies 0 \equiv 0 \ (5) \\ \text{si } 5 \nmid a \underset{!}{\overset{\text{PTF}}{\implies}} 2a^3 - 2a^3 \equiv 0 \ (5) \Leftrightarrow 0 \equiv 0 \ (5) \end{cases}$$

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

$$2a^7 + 5a - 7a^3 \equiv 0\ (5) \qquad \forall a \in \mathbb{Z}$$

Se concluye entonces que la expresión:

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

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

---

18. Sea $a \in \mathbb{Z}$ coprimo con 561. Probar que $a^{560} \equiv 1\ (561)$

Partiendo de la hipótesis:

$$(a : 561) = 1 \iff (a : 3 \cdot 11 \cdot 17) = 1 \implies \begin{cases} (a:3) = 1 \\ (a:11) = 1 \\ (a:17) = 1 \end{cases}$$

Es decir que $a \nmid 3, 11, 17$. Además, como 3, 11 y 17 son primos, por PTF, tenemos que

$$\begin{cases} a^2 \equiv 1\ (3) \\ a^{10} \equiv 1\ (11) \\ a^{16} \equiv 1\ (17) \end{cases} \xRightarrow{a \perp 3,11,17} \begin{cases} (a^2)^{280} \equiv 1^{280}\ (3) \\ (a^{10})^{56} \equiv 1^{56}\ (11) \\ (a^{16})^{35} \equiv 1^{35}\ (17) \end{cases} \iff \begin{cases} a^{560} \equiv 1\ (3) \\ a^{560} \equiv 1\ (11) \\ a^{560} \equiv 1\ (17) \end{cases}$$

Por útimo, utilizando que 3, 11 y 17 son coprimos dos a dos y haciendo TCR, obtenemos

$$\begin{cases} a^{560} \equiv 1\ (3) \\ a^{560} \equiv 1\ (11) \\ a^{560} \equiv 1\ (17) \end{cases} \iff a^{560} \equiv 1\ (3 \cdot 11 \cdot 17) \iff \boxed{a^{560} \equiv 1\ (561)} \quad \checkmark$$

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

---

19. Resolver en $\mathbb{Z}$ los siguientes sistemas lineales de ecuaciones de congruencia:

i) $\begin{cases} 2^{2013}X \equiv 6\ (13) \\ 5^{2013}X \equiv 4\ (7) \\ 7^{2013}X \equiv 2\ (5) \end{cases}$

ii) $\begin{cases} 10^{49}X \equiv 17\ (39) \\ 5X \equiv 7\ (9) \end{cases}$

---

i) Todos divisores primos y coprimos dos a dos:

$$\begin{cases} 2^{2013}X \equiv 6\ (13) & \xRightarrow{\text{PTF}} & 2^9X \equiv 6\ (13) & \overset{!}{\Leftrightarrow} & X \equiv 9\ (13) \\ 5^{2013}X \equiv 4\ (7) & \xRightarrow{\text{PTF}} & 5^3X \equiv 4\ (7) & \overset{!}{\Leftrightarrow} & X \equiv 3\ (7) \\ 7^{2013}X \equiv 2\ (5) & \Leftrightarrow & 2X \equiv 2\ (5) & \overset{!}{\Leftrightarrow} & X \equiv 1\ (5) \end{cases}$$

Listo hay que resolver esa goma de sistema:

$$\begin{cases} X \equiv 9\ (13) \\ X \equiv 3\ (7) \\ X \equiv 1\ (5) \end{cases}$$

Ehm, paja resolverlo.

... hay que hacerlo!

Si querés mandá la solución → al grupo de Telegram, o mejor aún si querés subirlo en LaTeX→ una *pull request* al.

ii)

$$\begin{cases} 10^{49}X \equiv 17\ (39) \rightsquigarrow \begin{cases} 1^{49}X \equiv 2\ (3) \Leftrightarrow X \equiv 2\ (3) \\ 10^{49}X \equiv 4\ (13) \overset{\text{PTF}}{\iff} 10X \equiv 4\ (13) \underset{4\ \perp\ 13}{\overset{\times 4}{\iff}} X \equiv 3\ (13) \end{cases} \\ 5X \equiv 7\ (9) \Leftrightarrow X \equiv 5\ (9) \rightsquigarrow \{\ X \equiv 2\ (3) \end{cases}$$

El sistema es compatible. Tomo la ecuación que tiene el denominador con la mayor potencia de 3, si no obtendría más soluciones de las que tiene el sistema original.

El sistema a resolver:

$$\begin{cases} X \equiv 3\ (13) \\ X \equiv 5\ (9) \end{cases}$$

Ehm, paja resolverlo.

... hay que hacerlo!

Si querés mandá la solución → al grupo de Telegram, o mejor aún si querés subirlo en LaTeX→ una *pull request* al.

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

---

20. Hallar el resto de la división de:

i) $3 \cdot 7^{135} + 24^{78} + 11^{222}$ por 70

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

---

i) Hay que hallar:

$$r_{70}(3 \cdot 7^{135} + 24^{78} + 11^{222}) \overset{\text{def}}{\iff} 4 \cdot 7^{135} + 24^{78} + 11^{222} \equiv X\ (70)$$

Hay que quebrar eso:

$$3 \cdot 7^{135} + 24^{78} + 11^{222} \equiv X\ (70) \rightsquigarrow \begin{cases} 1 + 1 = 2 \equiv X\ (2) \Leftrightarrow 0 \equiv X\ (2) \\ 3 \cdot 2^{135} + (-1)^{78} + 1^{222} \equiv X\ (5) \overset{\text{PTF}}{\iff} 3 \cdot 2^3 + 2 \overset{(5)}{\equiv} 1 \equiv X\ (5) \\ 3^{78} + 4^{222} \equiv X\ (7) \overset{\text{PTF}}{\iff} 3^0 + 4^0 = 2 \equiv X\ (7) \end{cases}$$

Hay que resolver entonces el sistema:

$$\begin{cases} X \equiv 0\ (2) \bigstar^1 \\ X \equiv 1\ (5) \bigstar^2 \\ X \equiv 2\ (7) \bigstar^3 \end{cases}$$

De $\bigstar^1$:

$$X \equiv 0\ (2) \overset{\text{def}}{\iff} X = 2k \xrightarrow[\text{en } \bigstar^2]{\text{meto}} 2k \equiv 1\ (5) \underset{3\ \perp\ 5}{\overset{\times 3}{\iff}} k \equiv 3\ (5) \overset{\text{def}}{\iff} k = 5h + 3 \implies X = 10h + 6$$

$$\xrightarrow[\text{en } \bigstar^3]{\text{meto}} X = 10h + 6 \overset{(7)}{\equiv} 3h + 6 \equiv 2\ (7) \underset{2\ \perp\ 7}{\overset{\times 2}{\iff}} h \equiv 1\ (7) \overset{\text{def}}{\iff} 70j + 16$$

Por lo tanto el resto pedido:

$$\boxed{r_{70}(3 \cdot 7^{135} + 24^{78} + 11^{222}) = 16}$$

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

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

que será aún más simple si quiebro en la forma:

$$X \equiv \sum_{i=1}^{1759} i^{42} \ (56) \leftrightsquigarrow \begin{cases} X \equiv \sum\limits_{i=1}^{1759} i^{42} \ (7) \bigstar^1 \\ X \equiv \sum\limits_{i=1}^{1759} i^{42} \ (8) \bigstar^2 \end{cases}$$

Primero estudio $\bigstar^1$.
Acomodo la sumatoria, voy a abrirla y separar los términos *convenientemente*:

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

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

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

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

$$\sum_{i=1}^{1759} i^{42} \overset{(7)}{\equiv} 251 \cdot \left(1^{42} + 2^{42} + 3^{42} + 4^{42} + 5^{42} + 6^{42} + 0^{42}\right) + \left(1^{42} + 2^{42}\right)$$

$$\xleftrightarrow[\text{PTF en cada término}]{7 \text{ primo y } 7 \nmid i}$$

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

Encontramos entonces que $\bigstar^1$:

$$X \equiv 3 \ (7)$$

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

$$\sum_{i=1}^{1759} i^{42} \overset{(8)}{\equiv} 1^{42}+2^{42}+3^{42}+4^{42}+5^{42}+6^{42}+7^{42}+0^{42}+1^{42}+2^{42}+3^{42}+4^{42}+5^{42}+6^{42}+7^{42}+0^{42}+1^{42}+2^{42}+3^{42}+4^{42}+5^{42}\ldots$$

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

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

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

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

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

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

Encontramos entonces que ★²:

$$X \equiv 0 \ (8)$$

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

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

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

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

Dale las gracias y un poco de amor ♥ a los que contribuyeron! Gracias por tu aporte:
naD GarRaz Juan Iglesias

---

21. Hallar el resto de la división de 2^{2^n} por 13 para cada $n \in \mathbb{N}$.

Enunciado corto y al pie, eso vaticina *infierno*. Bueno, no, estoy exagerando un poco.

$$r_{13}(2^{2^n}) = X \overset{\text{def}}{\iff} 2^{2^n} \equiv X \ (13) \overset{\overset{(13:2)=1}{\text{PTF}}}{\iff} 2^{r_{12}(2^n)} \equiv X \ (13) \text{★}^1$$

La papa está en reconocer qué es esa expresión del exponente. *Let's estudiate it*:

$$r_{12}(2^n) \overset{\text{def}}{\iff} 2^n \equiv Y \ (12) \rightsquigarrow \text{★}^2 \begin{cases} 2^n \equiv Y \ (4) \overset{!!}{\iff} \begin{cases} \text{si } n = 1 & \implies & 2^1 = 2 \equiv Y \ (4) \\ \text{si } n \geq 2 & \implies & 2^n \overset{(4)}{\equiv} 2^{2m+m'} \overset{!}{=} 4^m \cdot 2^{m'} \overset{(4)}{\equiv} 0 \equiv Y \ (4) \end{cases} \\ 2^n \equiv Y \ (3) \overset{\overset{\text{PTF}}{3 \perp 2}}{\iff} 2^{r_2(n)} \equiv Y \ (3) \overset{!}{\iff} \begin{cases} \text{si } n \text{ par} & \implies & 2^0 = 1 \equiv Y \ (3) \\ & \text{o} & \\ \text{si } n \text{ impar} & \implies & 2^1 = 2 \equiv Y \ (3) \end{cases} \end{cases}$$

En donde pongo el exponente $2m + m'$ es una forma de descomponer un número mayor a 2 para mostrar que $4 \mid 2^{2m+m'}$ siempre. Podrías usar una tabla de restos también, *you are free to choose*.
Por lo tanto para el sistema de ★² saco 3 sistemas:

$$\text{Si } n = 1 \overset{\text{★}^3}{\implies} \begin{cases} Y \equiv 2 \ (4) \\ Y \equiv 2 \ (3) \end{cases}, \quad \text{si } n \equiv 0 \ (2) \overset{\text{★}^4}{\implies} \begin{cases} Y \equiv 0 \ (4) \\ Y \equiv 1 \ (3) \end{cases} \quad \text{y} \quad \text{si } n \equiv 1 \ (2) \overset{\text{★}^5}{\implies} \begin{cases} Y \equiv 0 \ (4) \\ Y \equiv 2 \ (3) \end{cases}$$

Para cada uno de esos casos quiero encontrar Y así puedo después volver al principio del ejercicio para calcular lo que piden. El sistema ★³ es para un solo valor de n, onda lo más fácil es poner $n = 1$ en ★¹ y fin, pero igual porque *soy un tipazo* lo resuelvo de forma mecánica por si no lo ves:

$$\overset{\text{★}^3}{\longrightarrow} Y = 4k + 2 \overset{\overset{\text{meto en}}{\text{mod } (3)}}{\longrightarrow} 4k + 2 \overset{(3)}{\equiv} k + 2 \equiv 2 \ (3) \Leftrightarrow k \equiv 0 \ (3) \overset{\text{def}}{\iff} k = 3j \overset{!!}{\implies} Y \equiv 2 \ (12)$$

Reemplazando ese resultado en ★¹:

$$\boxed{r_{13}(2^2) = 4 \quad \text{para } n = 1}$$

Como ya habrás notado, mucho más barato era ir a ★¹ y poner $n = 1$.

Ahora voy a resolver el sistema ★⁴:

$$\overset{\text{★}^4}{\longrightarrow} Y = 4k \overset{\overset{\text{meto en}}{\text{mod } (3)}}{\longrightarrow} 4k \overset{(3)}{\equiv} k \equiv 1 \ (3) \overset{\text{def}}{\iff} k = 3j + 1 \overset{!!}{\implies} Y \equiv 4 \ (12)$$

Reemplazando ese resultado en ★¹:

$$\boxed{r_{13}(2^4) = 3 \quad \text{para } n \equiv 0 \ (2)}$$

Por último voy a resolver el sistema $\bigstar^5$:

$$\xrightarrow{\bigstar^5} Y = 4k \xrightarrow[\text{mod } (3)]{\text{meto en}} 4k \overset{(3)}{\equiv} k \equiv 2\ (3) \iff k = 3j + 2 \overset{!!}{\Rightarrow} Y \equiv 8\ (12)$$

Reemplazando ese resultado en $\bigstar^1$:

$$\boxed{r_{13}(2^8) = r_{13}(2^4 \cdot 2^4) = 9 \quad \text{para } n \equiv 1\ (2)}$$

Concluyendo que si quiero calcular $r_{13}(2^{2^n}) \quad \forall n \in \mathbb{N}$:

$$\boxed{r_{13}(2^{2^n}) = \begin{cases} 4 & \text{si} \quad n = 1 \\ 3 & \text{si} \quad n \equiv 0\ (2) \\ 9 & \text{si} \quad n \equiv 1\ (2) \quad \text{y} \quad n \geq 2 \end{cases}}$$

Dale las gracias y un poco de amor ♥ a los que contribuyeron! Gracias por tu aporte:
naD GarRaz Olivia Portero

---

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

Acomodo un poco la ecuación que esta fea:

$$7X^{45} \equiv 1\ (46) \xleftrightarrow{13 \perp 46} 91X^{45} \equiv 13\ (46) \overset{!}{\iff} X^{45} \equiv 33\ (46)$$

La idea es quebrar para poder el PTF:

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

En el !!! acomodo X^{45} para poder usar el PTF y $X^{22} \equiv X^0\ (23)$
Se tiene hasta el momento:

$$7X^{45} \equiv 1\ (46) \rightsquigarrow \begin{cases} X \equiv 10\ (23) \\ X \equiv 1\ (2) \end{cases}$$

Sacar de acá, meter allá y coso:

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

Por lo tanto:

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

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

---

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

Escribiendo el enunciado en ecuaciones queda algo así:

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

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

$$\begin{cases} 5^{140} \equiv 0 \ (5^\alpha) \\ 5^\alpha \equiv 2 \ (9) \bigstar^1 \\ 5^\alpha \equiv 3 \ (11) \bigstar^2 \end{cases}$$

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

$$5^3 \equiv -1 \ (9) \underset{(\Leftarrow)\ 5^3 \perp 9}{\overset{!}{\Longleftrightarrow}} 5^6 \equiv 1 \ (9)$$

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

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

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

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

Concluyo que:

$$5^\alpha \equiv 2 \ (9) \Leftrightarrow \alpha \equiv 5 \ (6)$$

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

$$5^\alpha \equiv 3 \ (11) \underset{\text{PTF, con } \alpha = 10}{\overset{11 \nmid 5}{\Longrightarrow}} 5^{10} \overset{(!)}{\equiv} 5^{r_{10}(10)} \equiv 1 \ (11)$$

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

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

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

$$5^\alpha \equiv 3 \ (11) \Leftrightarrow \alpha \equiv 2 \ (5)$$

Los valores de α deben cumplir el sistema:

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

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

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

Finalmente los divisores porsitivos pedidos del enunciado son:

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

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

---

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

a) $2p \mid 38^{2p^2-p-1} + 3p + 171$ b) $3p \mid 5^{p-1} + 3^{p^2+2} + 833$

Voy a buscar primos p que cumplan lo pedido, usando PTF:

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

$$38^{2p^2-p-1} + 3p + 171 \equiv 0 \ (2p) \rightsquigarrow \begin{cases} p \equiv 1 \ (2) \bigstar^1 \\ 38^{2p^2-p-1} + 3p + 171 \equiv 0 \ (p) \bigstar^2 \end{cases}$$

Quiero que ocurra que:

$$38^{2p^2-p-1} + 3p + 171 \equiv 0 \ (p) \Leftrightarrow \begin{cases} \xLeftrightarrow[\implies p = 19]{\text{si } p \mid 38} 38^{2\cdot 19^2-19-1} + 3 \cdot 19 + 171 \overset{(19)}{\equiv} 0 \equiv 0 \ (19) \bigstar^3 \\ \xLeftrightarrow[p \nmid 38 \ !!]{\text{PTF}} 38^0 + 0 + 171 = \underbrace{172}_{2^2 \cdot 43} \equiv 0 \ (p) \bigstar^4 \end{cases}$$

Cálculo usado hacer el PTF con p genérico:

$$\begin{array}{rr|l} 2p^2 & -p-1 & p-1 \\ \cline{3-3} -2p^2+2p & & 2p+1 \\ \cline{1-1} \multicolumn{1}{r}{p-1} & & \\ \multicolumn{1}{r}{-p+1} & & \\ \cline{1-1} \multicolumn{1}{r}{0} & & \end{array}$$

Después de hacer todo eso, sacamos de $\bigstar^1$ que p es impar. De $\bigstar^3$ obtenemos que un posible valor sería:

$$\boxed{p = 19}$$

y luego del caso $p \nmid 38$ sale que debe ocurrir que $172 \overset{(p)}{\equiv} 0$, y dado que p tiene que ser impar, entonces queda que:

$$\boxed{p = 43}$$

.

b) Parecido al anterior. Voy a ver que pasa con $p = 3$ y con $p = 5$ así descarto esos valores y después le mando PTF:

$$p = 3 \implies 9 \mid 5^2 + 3^{11} + 833 \overset{\text{def}}{\iff} 7 + 0 + 5 \overset{(9)}{\equiv} 3 \not\equiv 0 \ (9)$$

La expresión no se divide por 9, entonces descarto $p = 3$. A ver con $p = 5$:

$$p = 5 \implies 3 \cdot 5 \mid 5^4 + 3^{27} + 833 \rightsquigarrow \begin{cases} 5^2 \cdot 5^2 + 3^{27} \cdot 3^3 + 833 \overset{(3)}{\equiv} 1 + 0 + 2 \equiv 0 \ (3) \\ 5^4 + (3^4)^6 \cdot 3^3 + 833 \overset{(5)}{\equiv} 0 + 2 + 3 \equiv 0 \ (5) \end{cases}$$

Con $p = 5$ funciona el sistema con divisores coprimos, así que $p = 5$ es un número primo que cumple el enunciado.

Para un primo p genérico con $p \neq 3$ y $p \neq 5$:

$$3p \mid 5^{p-1} + 3^{p^2+2} + 833 \rightsquigarrow \begin{cases} 5^{p-1} + 3^{p^2+2} + 833 \equiv 0 \ (p) \bigstar^1 \\ 5^{p-1} + 3^{p^2+2} + 833 \equiv 0 \ (3) \bigstar^2 \end{cases}$$

Laburo en ★[1] con PTF y

$$\begin{array}{r|l} p^2 \quad +2 & p-1 \\ \hline -p^2+p & p+1 \\ \hline p+2 & \\ -p+1 & \\ \hline 3 & \end{array} \qquad \text{y} \qquad \begin{array}{r|l} p-1 & p-1 \\ \hline -p+1 & 1 \\ \hline 0 & \end{array}$$

$$★[1] \Leftrightarrow 5^0+3^3+833=861=3\cdot 7\cdot 41 \equiv 0\ (p)$$

Como el $p=3$ está descartado a este punto tengo que pedir que $p\in\{7,41\}$ para que se cumpla la congruencia. Solo me falta chequear que ★[2] funciones bien para estos valores:

$$\Leftrightarrow \begin{cases} p=41 \overset{★[2]}{\iff} 5^{41-1}+3^{41^2+2}+833 \overset{(3)}{\equiv} 5^0+3^1+2\equiv 0\ (3) \\ p=7 \overset{★[2]}{\iff} 5^{7-1}+3^{7^2+2}+833 \overset{(3)}{\equiv} 5^0+3^1+2\equiv 0\ (3) \end{cases}$$

Concluyendo de esta manera que los números primos 7 y 41 también son soluciónes:

$$\boxed{p\in\{5,7,41\}}$$

Dale las gracias y un poco de amor ♥ a los que contribuyeron! Gracias por tu aporte:
naD GarRaz Tomás A.

---

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

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

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

Vamos a buscar info sobre a. De ★[1] tenemos que:

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

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

Ahora estudio ★[2] para distintos valores de a. Vamos a poder usar PTF? NO, porque 4 no es primo chequea la teoría acá:

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

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

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

Misma historia con ★[3], y si estás despierto todavía, finalmente vamos a poder usar el PTF, porque 11 es un número primo (teoria acá):

$$a^{760}+11a+10 \equiv a^{760}-1\equiv 0\ (11) \Leftrightarrow \begin{cases} \text{si } 11 \mid a \implies -1\equiv 0\ (11) \\ \text{si } 11 \nmid a \overset{\text{PTF}}{\underset{!}{\implies}} a^{r_{10}(760)}-1=0\equiv 0\ (4) \end{cases}$$

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

$$11 \mid a \overset{\text{def}}{\iff} a \equiv 0 \ (11)$$

Con estos resultados puedo formar 2 sistemas:

$$\bigstar^4 \begin{cases} a \equiv 0 \ (4) \\ a \equiv 0 \ (11) \end{cases} \quad \text{y} \quad \bigstar^5 \begin{cases} a \equiv 1 \ (4) \\ a \equiv 0 \ (11) \end{cases}$$

Por TCH los sistemas tienen solución, porque los divisores son coprimos 2 a 2.
El sistema $\bigstar^4$ sale fácil $\boxed{a \equiv 0 \ (44)}$
El sistema $\bigstar^5$:

$$a \equiv 1 \ (4) \overset{\text{def}}{\iff} a = 4k + 1$$
$$4k + 1 \equiv 0 \ (11) \overset{\substack{11 \perp 3 \\ !!}}{\iff} k \equiv 8 \ (11) \overset{\text{def}}{\iff} k = 11j + 8$$
$$a = 4(11j + 8) + 1 = 44j + 33$$
$$\boxed{a \equiv 33 \ (44)}$$

Los posibles restos que nos pedían son 0 y 33.

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

---

26. Escribir las tablas de suma y producto en $\mathbb{Z}/m\mathbb{Z}$ para $m = 5$ y 8. Alguno de estos anillos es un cuerpo?

$$\mathbb{Z}/5\mathbb{Z}$$

$+$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{0}$	$\bar{1}$
$\bar{3}$	$\bar{3}$	$\bar{4}$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{4}$	$\bar{4}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$

$\times$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{2}$	$\bar{0}$	$\bar{2}$	$\bar{4}$	$\bar{1}$	$\bar{3}$
$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{1}$	$\bar{4}$	$\bar{2}$
$\bar{4}$	$\bar{0}$	$\bar{4}$	$\bar{3}$	$\bar{2}$	$\bar{1}$

$$\mathbb{Z}/8\mathbb{Z}$$

$+$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$	$\bar{7}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$	$\bar{7}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$	$\bar{7}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$	$\bar{7}$	$\bar{0}$	$\bar{1}$
$\bar{3}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$	$\bar{7}$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{4}$	$\bar{4}$	$\bar{5}$	$\bar{6}$	$\bar{7}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{5}$	$\bar{5}$	$\bar{6}$	$\bar{7}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{6}$	$\bar{6}$	$\bar{7}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$
$\bar{7}$	$\bar{7}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$

$\times$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$	$\bar{7}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$	$\bar{6}$	$\bar{7}$
$\bar{2}$	$\bar{0}$	$\bar{2}$	$\bar{4}$	$\bar{6}$	$\bar{0}$	$\bar{2}$	$\bar{4}$	$\bar{6}$
$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{6}$	$\bar{1}$	$\bar{4}$	$\bar{7}$	$\bar{2}$	$\bar{5}$
$\bar{4}$	$\bar{0}$	$\bar{4}$	$\bar{0}$	$\bar{4}$	$\bar{0}$	$\bar{4}$	$\bar{0}$	$\bar{4}$
$\bar{5}$	$\bar{0}$	$\bar{5}$	$\bar{2}$	$\bar{7}$	$\bar{4}$	$\bar{1}$	$\bar{6}$	$\bar{3}$
$\bar{6}$	$\bar{0}$	$\bar{6}$	$\bar{4}$	$\bar{2}$	$\bar{0}$	$\bar{6}$	$\bar{4}$	$\bar{2}$
$\bar{7}$	$\bar{0}$	$\bar{7}$	$\bar{6}$	$\bar{5}$	$\bar{4}$	$\bar{3}$	$\bar{2}$	$\bar{1}$

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

27. Un elemento $\bar{a} \in \mathbb{Z}/m\mathbb{Z}$ es un cuadrado (en $\mathbb{Z}/m\mathbb{Z}$) si existe $\bar{b} \in \mathbb{Z}/m\mathbb{Z}$ tal que $\bar{a}^2 = \bar{b}^2$ en $\mathbb{Z}/m\mathbb{Z}$

i) Calcular los cuadrados en $\mathbb{Z}/m\mathbb{Z}$ para $m = 2, 3, 4, 9, 11$. Cuantos hay en cada caso?

ii) Sea $p \in \mathbb{N}$ primo. Probar que, en $\mathbb{Z}/p\mathbb{Z}$, si $\bar{a}^2 = \bar{b}^2$, entonces $\bar{a} = \bar{b}$ ó $\bar{a} = -\bar{b}$. Deducir que si p es impar, entonces hay exactamente $\frac{p-1}{2}$ cuadrados no nulos en $\mathbb{Z}/p\mathbb{Z}$

---

i)

$(m=2)$	$(m=3)$	$(m=4)$	$(m=9)$	$(m=11)$
$\bar{0}^2 = \bar{0}$	$\bar{0}^2 = \bar{0}$	$\bar{0}^2 = \bar{0}$	$\bar{0}^2 = \bar{0}$	$\bar{0}^2 = \bar{0}$
$\bar{1}^2 = \bar{1}$	$\bar{1}^2 = \bar{1}$	$\bar{1}^2 = \bar{1}$	$\bar{1}^2 = \bar{1}$	$\bar{1}^2 = \bar{1}$
	$\bar{2}^2 = \bar{1}$	$\bar{2}^2 = \bar{0}$	$\bar{2}^2 = \bar{4}$	$\bar{2}^2 = \bar{4}$
		$\bar{3}^2 = \bar{1}$	$\bar{3}^2 = \bar{0}$	$\bar{3}^2 = \bar{9}$
			$\bar{4}^2 = \bar{7}$	$\bar{4}^2 = \bar{5}$
			$\bar{5}^2 = \bar{7}$	$\bar{5}^2 = \bar{3}$
			$\bar{6}^2 = \bar{0}$	$\bar{6}^2 = \bar{3}$
			$\bar{7}^2 = \bar{4}$	$\bar{7}^2 = \bar{5}$
			$\bar{8}^2 = \bar{1}$	$\bar{8}^2 = \bar{9}$
				$\bar{9}^2 = \bar{4}$
				$\bar{10}^2 = \bar{1}$
cantidad: 2	cantidad: 2	cantidad: 2	cantidad: 4	cantidad: 6

Notar que contamos al $\bar{0}$ como un cuadrado pues en el enunciado no especifica si tienen que ser cuadrados no nulos o no.

ii)

$$\bar{a}^2 = \bar{b}^2 \Leftrightarrow \bar{a}^2 - \bar{b}^2 = 0 \Leftrightarrow (\bar{a}+\bar{b})\cdot(\bar{a}-\bar{b}) = 0 \overset{\bigstar^1}{\Leftrightarrow} \bar{a}+\bar{b} = 0 \text{ ó } \bar{a}-\bar{b} = 0$$
$$\bar{a}+\bar{b} = 0 \Leftrightarrow \bar{a} = -\bar{b}$$
$$\bar{a}-\bar{b} = 0 \Leftrightarrow \bar{a} = \bar{b}$$

$\bigstar^1$ Ojo aca, este paso lo podemos hacer porque $\mathbb{Z}/p\mathbb{Z}$ es un dominio integro, es decir ($ab = 0 \implies a = 0$ ó $b = 0$), pero en general no es valido para $\mathbb{Z}/m\mathbb{Z}$, m compuesto.

Ahora vamos a deducir que en $\mathbb{Z}/p\mathbb{Z}$ hay $\frac{p-1}{2}$ cuadrados no nulos, aca ya tenemos la primera pista, como nos piden cuadrados no nulos, sacamos de la lista al 0, por lo tanto de p elementos que teniamos para elegir (del 0 a $p-1$), ahora tenemos $p-1$ elementos disponibles, ahora veamos, una conclusion de lo que demostramos mas arriba es que cada cuadrado tiene dos raices ($\bar{x}^2 = \bar{y}^2 \implies \bar{x} = \pm\bar{y}$). (Notar la similitud con $x^2 = y^2$ en el cuerpo de los numeros reales). Luego de los $p-1$ elementos vamos a tener que solo la mitad son distintos, pues un cuadrado se puede conseguir con dos numeros diferentes (por ejemplo $\bar{2}^2 = \bar{5}^2$ en $\mathbb{Z}/7\mathbb{Z}$). Entonces nos queda que la cantidad de cuadrados no nulos es $\boxed{\frac{p-1}{2}}$

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

28.

i) Probar que $\{\bar{2}^n : n \in \mathbb{N}\} = \mathbb{Z}/11\mathbb{Z} - \{\bar{0}\}$

ii) Hallar $\bar{a} \in \mathbb{Z}/7\mathbb{Z}$ tal que $\{\bar{a}^n : n \in \mathbb{N}\} = \mathbb{Z}/7\mathbb{Z} - \{\bar{0}\}$

---

i) Bueno, en definitiva lo que queremos es que elevando 2 a potencias podamos construir todo $\mathbb{Z}/11\,\mathbb{Z}$, estamos elevando 2 a potencias, y luego tomando modulo 11, es decir, en algun momento se van a repetir (Ppio del palomar). Vamos a ver casos individuales que es la manera mas facil de probarlo porque 11 no es un numero grande.

$$\begin{aligned}\bar{2}^1 &= \bar{2}\\ \bar{2}^2 &= \bar{4}\\ \bar{2}^3 &= \bar{8}\\ \bar{2}^4 &= \bar{5}\\ \bar{2}^5 &= \bar{10}\\ \bar{2}^6 &= \bar{9}\\ \bar{2}^7 &= \bar{7}\\ \bar{2}^8 &= \bar{3}\\ \bar{2}^9 &= \bar{6}\\ \bar{2}^{10} &= \bar{1}\\ \bar{2}^{11} &= \bar{2}\end{aligned}$$

Vemos que a partir de $\bar{2}^{11}$ se va a volver a repetir todo el ciclo de vuelta. Obtuvimos todos los elementos de $\mathbb{Z}/11\,\mathbb{Z}$, sin incluir el 0 (igual esto no podria haber pasado pues $11 \nmid 2^k \ \ \forall k \in \mathbb{N}$).

ii) ... hay que hacerlo!

Si querés mandá la solución → al grupo de Telegram, o mejor aún si querés subirlo en LaTeX→ una *pull request* al.

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

---

29. Sea p un primo. Probar que en $\mathbb{Z}/p\,\mathbb{Z}$ vale que $(\bar{a}+\bar{b})^p = \bar{a}^p + \bar{b}^p, \ \ \forall \bar{a}, \bar{b} \in \mathbb{Z}/p\,\mathbb{Z}$ (sug: ver Ej. 25 Practica 4). Vale lo mismo en $\mathbb{Z}/m\,\mathbb{Z}$ si m no es primo?

Expandimos con Newton la expresion:

$$(\bar{a}+\bar{b})^p = \sum_{k=0}^{p} \binom{p}{k} \bar{a}^k \cdot \bar{b}^{p-k} = \tag{1}$$

$$= \bar{a}^p + \sum_{k=1}^{p-1} \binom{p}{k} \bar{a}^k \cdot \bar{b}^{p-k} + \bar{b}^p \tag{2}$$

En el ejercicio 25 de la practica 4 se probó que $p \mid \binom{p}{k}, 0 < k < p$, por lo tanto:

$$\sum_{k=1}^{p-1} \binom{p}{k} \bar{a}^k \cdot \bar{b}^{p-k} = \bar{0}$$

Entonces

$$\bar{a}^p + \sum_{k=1}^{p-1} \binom{p}{k} \bar{a}^k \cdot \bar{b}^{p-k} + \bar{b}^p = \bar{a}^p + \bar{b}^p$$

Como se queria probar. Ahora veamos si lo mismo se cumple para $\mathbb{Z}/m\,\mathbb{Z}, m$ compuesto. Con un contraejemplo basta para desmotrar que no se cumple. Consideremos $\mathbb{Z}/6\,\mathbb{Z}$, elijamos $a = \bar{2}$, $b = \bar{4}$.

$$(\bar{2}+\bar{4})^6 = \bar{0} \text{ pero } \bar{2}^6 + \bar{4}^6 = \bar{4} + \bar{4} = \bar{2} \neq \bar{0}$$

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

30. El objetivo de este ejercicio es probar que si $n \in \mathbb{N}$ es distinto de 1, entonces

$$(n-1)! \equiv -1 \pmod{n} \iff n \text{ es primo .}$$

i) Verificar que $3! \not\equiv -1$ (4) y probar que si $n \geq 5$ es compuesto, entonces $(n-1)! \equiv 0 \pmod{n}$. Qué implicacion se prueba con esto?

ii) Sea p un primo positivo. Se recuerda que $\mathbb{Z}/p\mathbb{Z}$ es un cuerpo. Probar que $\bar{a} = \bar{a}^{-1}$ en $\mathbb{Z}/p\mathbb{Z}$ si y solo si $\bar{a} = \pm\bar{1}$. Deducir que $(p-1)! \equiv -1$ (p).

(Este test de primalidad debe su nombre al matematico inglés John Wilson, 1741-1793, pero era conocido mucho antes por los árabes, y fue de hecho probado por primera vez por el matematico italiano Joseph-Louis Lagrange en 1771).

Empecemos por el item i), primero de todo $3! = 6 \equiv 2$ (4) que es distinto de -1, ahora vamos a probar que si n es compuesto y mayor o igual a 5 entonces $(n-1)! \equiv 0 \pmod{n}$.

Bien, como n es compuesto significa que se puede escribir como factor de dos numeros, que si a su vez son compuestos se pueden escribir como factores de mas numeros, en definitiva, $n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_n^{\alpha_n}$, todos estos factores son menores que n por lo tanto esta garantizado que van a aparecer en algun momento al expandir $(n-1)!$, lo que significa que $n \mid (n-1)!$, que es equivalente a decir $(n-1)! \equiv 0 \pmod{n}$.
Con este recurso podemos probar la implicacion hacia la derecha, nuestra hipotesis seria que $(n-1)! \equiv -1 \pmod{n}$, luego asumimos que n es compuesto, llegamos a una contradiccion por el argumento de arriba, por lo tanto n es primo

Ahora con el item ii) vamos a proabr la vuelta, que es un poco mas complicado. Sea p un primo, nos piden probar que

$$\bar{a} = \bar{a}^{-1} \Leftrightarrow \bar{a} = \pm\bar{1} \text{ en } \mathbb{Z}/p\mathbb{Z}$$

Bueno vamos a transformar a palabras lo que quiere decir esto, primero que nada como p es primo, sabemos que $\mathbb{Z}/p\mathbb{Z}$ es un cuerpo, lo que quiere decir que cada elemento tiene un inverso, es decir:

$$\forall \bar{a} \in (\mathbb{Z}/p\mathbb{Z})\, \exists\, \bar{a}^{-1} \text{ tal que } \bar{a} \cdot \bar{a}^{-1} = \bar{1}$$

Entonces, $\bar{a} = \bar{a}^{-1}$ significa un elemento que es igual a su inverso, bueno ahora vamos a probar el claim original.
$\rightarrow$)

$$\bar{a} \cdot \bar{a}^{-1} = \bar{a} \cdot \bar{a} = \bar{a}^2 = \bar{1}$$
$$\bar{a}^2 - \bar{1} = \bar{0} \Leftrightarrow (\bar{a}+1) \cdot (\bar{a}-1) = \bar{0}$$
$$\bar{a} = \pm\bar{1}$$

$\leftarrow$) Este es mas facil, notemos que $\pm\bar{1}$ al cuadrado es 1, luego tanto $\bar{1}$ como $\bar{-1}$ son sus propios inversos.
Finalmente estamos listos para probar la implicacion hacia la izquierda del teorema, tenemos que n es primo, luego consideramos todos los elementos en el grupo multiplicativo de $\mathbb{Z}/n\mathbb{Z}$, cuyos elementos son $\{1, 2, \ldots, (n-1)\}$, sabemos que cada elemento tiene un inverso multiplicativo, y tambien sabemos que hay solo dos elementos que son su propio inverso, 1 y $n-1$ (Notar que $n-1 \equiv -1$ (n)), luego $(n-1)! = 1 \cdot 2 \cdots (n-1) = 1 \cdot (n-1) \cdot$(pares de inversos).
Acá esta la clave, como sabemos que cada elemento tiene su inverso, y ya separamos aquellos que son su propio inverso, todos los elementos que quedan van a venir de a pares de inversos, que multiplicados dan 1, por lo tanto $1 \cdot 2 \cdots n - 1 = 1 \cdot (n-1) \cdot$ (pares de inversos) $= 1 \cdot (n-1) \cdot 1 = n - 1 \equiv -1$ (n), como se queria probar.

Ejercicios de parciales:

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

Como $105 = 3 \cdot 5 \cdot 7$ quiero que ocurra:

$$\begin{cases} a^{1081} + 3a + 17 \equiv 0 \ (5) \\ a^{1081} + 3a + 17 \equiv 0 \ (7) \\ a^{1081} + 3a + 17 \not\equiv 0 \ (3) \end{cases} \overset{!}{\Leftrightarrow} \begin{cases} a^{1081} + 3a + 2 \equiv 0 \ (5) \bigstar^1 \\ a^{1081} + 3a + 3 \equiv 0 \ (7) \bigstar^2 \\ a^{1081} + 2 \not\equiv 0 \ (3) \bigstar^3. \end{cases}$$

De esa forma me aseguro que el MCD sea 35. Ahora empiezo a estudiar $\bigstar^1$:

$$a^{1081} + 3a + 2 \equiv 0 \ (5) \Leftrightarrow \begin{cases} \xrightarrow[a \equiv 0 \ (5)]{\text{caso si}} & 2 \equiv 0 \ (5) \xRightarrow[\text{que}]{\text{concluyo}} a \not\equiv 0 \ (5) \\ & \text{o} \\ \xrightarrow[\text{y } a \not\equiv 0 \ (5)]{\text{PTF: 5 es primo}} & a + 3a + 2 \equiv 0 \ (5) \Leftrightarrow a \equiv 2 \ (5) \end{cases}$$

Hasta el momento tengo que para que se cumpla lo pedido:

$$a \equiv 2 \ (5) \bigstar^4$$

Busco más condiciones en $\bigstar^2$:

$$a^{1081} + 3a + 1 \equiv 0 \ (7) \Leftrightarrow \begin{cases} \xrightarrow[a \equiv 0 \ (7)]{\text{caso si}} & 1 \equiv 0 \ (7) \xRightarrow[\text{que}]{\text{concluyo}} a \not\equiv 0 \ (7) \\ & \text{o} \\ \xrightarrow[\text{y } a \not\equiv 0 \ (7)]{\text{PTF: 7 es primo}} & 4a + 3 \equiv 0 \ (7) \Leftrightarrow a \equiv 1 \ (7) \end{cases} .$$

Se concluye de este último resultado que a también puede tomar los valores:

$$a \equiv 1 \ (7) \bigstar^5$$

Por último falta estudiar los valores de a en $\bigstar^3$:

$$a^{1081} + 2 \not\equiv 0 \ (3) \Leftrightarrow \begin{cases} \xrightarrow[a \equiv 0 \ (3)]{\text{caso si}} & 2 \not\equiv 0 \ (3) \xRightarrow[\text{que}]{\text{concluyo}} a \equiv 0 \ (3) \bigstar^6 \\ & \text{o} \\ \xrightarrow[\text{y } a \not\equiv 0 \ (3)]{\text{PTF: 3 es primo}} & a + 2 \not\equiv 0 \ (3) \Leftrightarrow a \not\equiv 1 \ (3) \xRightarrow[\text{que } !!]{\text{concluyo}} a \equiv 2 \ (3) \bigstar^6. \end{cases}$$

En el !! estoy en la rama donde $a \not\equiv 0 \ (3)$ y si $a \equiv 1 \ (3)$ no se cumpliría $\bigstar^3$, por eso el único valor que sale de esa rama es $a \equiv 2 \ (3)$.
Se concluye de este último resultado que a también puede tomar los valores:

$$a \equiv 0 \ (3) \quad \text{o} \quad a \equiv 2 \ (3)$$

El resultado del estudio de $\bigstar^1, \bigstar^2$ y $\bigstar^3$, dio los resultados de $\bigstar^4, \bigstar^5, \bigstar^6$ con los cuales se puede formar los 2 sistemas:

$$\begin{cases} a \equiv 2 \ (5) \\ a \equiv 1 \ (7) \\ a \equiv 0 \ (3) \end{cases} \xrightarrow[\text{TCH}]{\text{divisores coprimos}} \boxed{a \equiv 57 \ (105)} \quad \text{y} \quad \begin{cases} a \equiv 2 \ (5) \\ a \equiv 1 \ (7) \\ a \equiv 2 \ (3) \end{cases} \xrightarrow[\text{TCH}]{\text{divisores coprimos}} \boxed{a \equiv 92 \ (105)}$$

El conjunto de posibles a:

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

Solo falta calcular el $r_{70}(a)$ para estos valores de a. Calcular el resto es ver la congruencia 70, $r_{70}(a)$:

$$\begin{cases} a \overset{(70)}{\equiv} 35k_1 + 57 \overset{\text{def}}{\iff} \boxed{a \equiv 57\ (70)} \\ a \overset{(70)}{\equiv} 35k_2 + 22 \overset{\text{def}}{\iff} \boxed{a \equiv 22\ (70)} \end{cases}$$

Los restos pedidos de dividir a por 70:

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

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

---

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

Como $135 = 3^3 \cdot 5$, los posibles valores sin tener en cuenta la restricción que puede tomar el MCD serían:

$$\bigstar^1 \text{MCD} \in \{1, 3, 5, 9, 15, 27, 45, 135\}$$

.

Por otro lado tengo que:

$$15 = 3 \cdot 5 \quad \text{y} \quad (a^{197} - 26 : 15) = 1,$$

lo cual se cumple para:

$$\bigstar^2 \begin{cases} a^{197} - 26 \not\equiv 0\ (5) \Leftrightarrow a^{197} \not\equiv 1\ (5) \\ a^{197} - 26 \not\equiv 0\ (3) \Leftrightarrow a^{197} \not\equiv 2\ (3) \end{cases}$$

$$a^{197} \not\equiv 1\ (5) \overset{\substack{5 \text{ es} \\ \text{primo}}}{\iff} \begin{cases} \overset{a \not\equiv 0\ (5)}{\underset{\text{PTF}}{\iff}} a \not\equiv 1\ (5) \\ \overset{a \equiv 0\ (5)}{\iff} 0 \not\equiv 1\ (5) \end{cases}$$

$$a^{197} \not\equiv 2\ (3) \overset{\substack{3 \text{ es} \\ \text{primo}}}{\iff} \begin{cases} \overset{a \not\equiv 0\ (3)}{\underset{\text{PTF}}{\iff}} a \not\equiv 2\ (3) \\ \overset{a \equiv 0\ (3)}{\iff} 0 \not\equiv 2\ (3) \end{cases}$$

Por lo tanto tengo que los valores permitido de a para calcular los MCD son:

$$a^{197} \not\equiv 1\ (5) \Leftrightarrow a \not\equiv 1\ (5) \begin{cases} a \equiv 0\ (5) \\ a \equiv 2\ (5) \\ a \equiv 3\ (5) \\ a \equiv 4\ (5) \end{cases}$$

$$a^{197} \not\equiv 2\ (3) \Leftrightarrow a \not\equiv 2\ (3) \begin{cases} a \equiv 0\ (3) \\ a \equiv 1\ (3) \end{cases}$$

Divisibilidad por 3. ¿Es la expresión $a^{97} - 36$ divisible por 3 para alguno de los valores de a permitidos?:

$$a^{97} - 36 \equiv 0\ (3) \Leftrightarrow a^{97} \equiv 0\ (3) \overset{\substack{3 \text{ es} \\ \text{primo}}}{\iff} \begin{cases} \overset{a \not\equiv 0\ (3)}{\underset{\text{PTF}}{\iff}} a \equiv 0\ (3) \quad \text{incompatible con} \quad a \not\equiv 0\ (3) \\ \overset{a \equiv 0\ (3)}{\iff} 0 \equiv 0\ (3) \quad \text{compatible con} \quad a \equiv 0\ (3) \quad \text{y} \quad \left\{ \begin{array}{l} a \equiv 0\ (3) \\ a \equiv 0\ (5) \end{array} \right\} \end{cases}$$

Se concluye que la expresión $a^{97} - 36$ es divisible por 3 para alguno de los valores de a permitidos.

Divisibilidad por 5. ¿Es la expresión $a^{97}-36$ divisible por 5 para alguno de los valores de a permitidos?:

$$a^{97}-36\equiv 0\ (5)\Leftrightarrow a^{97}\equiv 1\ (5)\overset{\text{5 es primo}}{\Longleftrightarrow}\begin{cases}\overset{a\not\equiv 0\ (5)}{\underset{\text{PTF}}{\Longleftrightarrow}} a\equiv 1\ (5) & \text{incompatible con } a\not\equiv 1\ (5)\\ \overset{a\equiv 0\ (5)}{\Longleftrightarrow} 0\equiv 1\ (5) & \text{incompatible}\end{cases}$$

Se concluye que la expresión $a^{97}-36$ no es divisible por 5 para los valores de a permitidos. Esto reduce la cantidad de *posibles* MCD a:

$$\text{MCD}\in\{1,3,9,27\}$$

Divisibilidad por 9.
Teniendo en cuenta que los posibles MCD, son todos potencias de 3 y que $a\equiv 0\ (3)$ *¿Es la expresión $a^{97}-36$ divisible por 9 para alguno de los valores de a permitidos?*:

$$a^{97}-36\equiv 0\ (9)\overset{\underset{\Rightarrow a=3k}{a\equiv 0\ (3)}}{\Longleftrightarrow}(3k)^{97}\overset{!!}{=}3\cdot\underbrace{(3^2)^{48}}_{\downarrow 9}\cdot k^{97}\equiv 0\ (9)\Leftrightarrow 0\equiv 0\ (9)$$

Se concluye que la expresión $a^{97}-36$ es divisible por 9 para los a que cumplen $a\equiv 0\ (3)$. De esa manera destronando al 3 como posible MCD.

Divisibilidad por 27.
Teniendo en cuenta que hasta el momento que el 9 es el MCD. *¿Es la expresión $a^{97}-36$ divisible por 27 para alguno de los valores de a permitidos?*:

$$a^{97}-36\equiv 0\ (27)\Leftrightarrow a^{97}\equiv 9\ (27)\Leftrightarrow\begin{cases}\overset{a\equiv 0\ (3)}{\Longleftrightarrow} 0\equiv 9\ (27) & \text{noup!}\\ \overset{a\equiv 1\ (3)}{\Longleftrightarrow} 1\equiv 9\ (27) & \text{noup!}\end{cases}$$

Se concluye que la expresión $a^{97}-36$ no es divisible por 27 para ninguno de los valores de a permitidos.

Hasta el momento obtuvimos que $\{9\}$ es el único MCD posible.
Falta analizar el caso del MCD $=1$:
Encuentro que si:

$$\underbrace{a=4}_{\text{a ojímetro}}\implies 4^{97}-36\equiv 0\ (3)\Leftrightarrow 1\equiv 0\ (3)$$

Entonces $a=4$ es un valor de a para el cual el MCD no es divisible por 3, por lo que tampoco por 9:

$$(4^{97}-36:135)=1.$$

De esta formar $a=4$ es un valor permitido por la restricción $a\equiv 4\ (5)$ y $a\equiv 1\ (3)$. Concluyendo así que el 1 es otro posible valor para el MCD.

Conclusión, posibles valores:

$$\boxed{\text{MCD}\in\{1,9\}}$$

Esto fue la fatality de sub-zero para el sega megadrive, espero que les haya gustado, chau!

Dale las gracias y un poco de amor ♥ a los que contribuyeron! Gracias por tu aporte:
naD GarRaz Ale Teran

---

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

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

Expresar las soluciones mediante una única ecuación.

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

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

Estudio la divisibilidad 7:
Si

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

Analizo esa expresión en los casos cuando $7 \mid n$ y cuando $7 \nmid n$ o lo que es lo mismo cuando $n \equiv 0\ (7)$ y cuando $n \not\equiv 0\ (7)$:

$$n^{433} \equiv 0\ (7) \Leftrightarrow \begin{cases} \xrightarrow{n \equiv 0\ (7)} 0 \equiv 0\ (7) \implies \boxed{n \equiv 0\ (7)} & \checkmark \bigstar^1 \\ \xrightarrow[n \not\equiv 0\ (7)]{\text{PTF, 7 es primo}} n \equiv 0\ (7) \to \text{incompatible} & \end{cases}$$

Conclusión divisibilidad 7:

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

Estudio la divisibilidad $7^2 = 49$:
Si,

$$7^2 \nmid n^{433}+7n+91 \overset{\text{def}}{\iff} n^{433}+7n+91 \not\equiv 0\ (49) \iff n^{433}+7n+42 \not\equiv 0\ (49),$$

de $\bigstar^1$ tengo que $n \equiv 0\ (7) \overset{\text{def}}{\iff} n = 7k$, por lo tanto:

$$(7k)^{433}+7\cdot 7k+42 \not\equiv 0\ (49) \Leftrightarrow 7\cdot(49)^{216}\cdot k^{433}+49k+42 \not\equiv 0\ (49) \Leftrightarrow 42 \not\equiv 0\ (49)$$

Conclusión divisibilidad 49:

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

Estudio la divisibilidad 19:
Si

$$19 \mid n^{433}+7n+91 \iff n^{433}+7n+91 \equiv 0\ (19) \iff n^{433}+7n+15 \equiv 0\ (19)$$

Analizo esa expresión en los casos cuando $19 \mid n$ y cuando $19 \nmid n$ o lo que es lo mismo cuando $n \equiv 0\ (19)$ y cuando $n \not\equiv 0\ (19)$:

$$n^{433}+7n+15 \equiv 0\ (19) \Leftrightarrow \begin{cases} \xrightarrow{n \equiv 0\ (19)} 15 \equiv 0\ (19) \to \text{ningún } n & \\ \xrightarrow[n \not\equiv 0\ (19)]{\text{PTF, 19 es primo}} 8n \equiv 4\ (19) \xrightarrow[7 \perp 19]{(\Leftarrow)} 56n \equiv 28\ (19) \Leftrightarrow \boxed{n \equiv 10\ (19)} & \checkmark \bigstar^2 \end{cases}$$

Conclusión divisibilidad 19:

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

$$\begin{cases} \bigstar^1 n \equiv 0\ (7) \\ \bigstar^2 n \equiv 10\ (19) \end{cases} \xrightarrow[\text{por T chino R}]{7 \perp 19 \text{ hay solución}} \begin{cases} \xrightarrow[\text{en } \bigstar^1]{\bigstar^2} n = 19k+10 \overset{(7)}{\equiv} 5k+3 \overset{(7)}{\equiv} 0 \Leftrightarrow k \equiv 5\ (7) & \checkmark \end{cases}$$

Finalmente:

$$n = 19\cdot(7q+5)+10 \Leftrightarrow \boxed{n \equiv 105\ (133)}$$

Dale las gracias y un poco de amor ♥ a los que contribuyeron! Gracias por tu aporte:
Nad Garraz Dani Tadd

---

4. Determinar para cada $n \in \mathbb{N}$ el resto de dividir a 8^{3^n-2} por 20.

Quiero encontrar $r_{20}(8^{3^n-2})$ entonces analizo congruencia:

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

Laburo con $\bigstar^1$, 5 es primo y $5 \nmid 3$, puedo usar PTF:

$$8^{3^n-2} \equiv 3^{3^n-2} \equiv 3^{r_4(3^n-2)} \ (5)$$

A ver esta última expresión:

$$X = r_4(3^n-2) \overset{\text{def}}{\iff} X \equiv 3^n - 2 \ (4) \Leftrightarrow X \equiv (-1)^n + 2 \ (4) \overset{!}{\iff} \begin{cases} X \equiv 3 \ (4) & \text{si } n \text{ par} \\ X \equiv 1 \ (4) & \text{si } n \text{ impar} \end{cases}$$

Volviendo a $\bigstar^1$ con los resultados calculados de X:

$$\bigstar^3 \begin{cases} 8^{3^n-2} \equiv 0 \ (4) & \forall n \in \mathbb{N} \\ 8^{3^n-2} \equiv 2 \ (5) & \forall n \in \mathbb{N} \text{ par} \end{cases} \quad \text{y} \quad \bigstar^4 \begin{cases} 8^{3^n-2} \equiv 0 \ (4) & \forall n \in \mathbb{N} \\ 8^{3^n-2} \equiv 3 \ (5) & \forall n \in \mathbb{N} \text{ impar} \end{cases}$$

Lo que resta por hacer es resolver los sistemas. Empiezo por el sistema con n par $\bigstar^3$:

$$n \equiv 0 \ (2) \implies \begin{cases} 8^{3^n-2} \equiv 0 \ (4) \overset{\text{def}}{\iff} 8^{3^n-2} = 4j \overset{\text{reemplazo}}{\iff} 4j \equiv 2 \ (5) \Leftrightarrow j \equiv 3 \ (5) \overset{\text{def}}{\iff} j = 5k+3 \\ \implies 8^{3^n-2} = 4(5k+3) \overset{\text{def}}{\iff} \boxed{8^{3^n-2} \equiv 12 \ (20) \Leftrightarrow n \equiv 0 \ (2)}. \end{cases}$$

Con n impar $\bigstar^4$:

$$n \equiv 1 \ (2) \implies \begin{cases} 8^{3^n-2} \equiv 0 \ (4) \overset{\text{def}}{\iff} 8^{3^n-2} = 4j \overset{\text{reemplazo}}{\iff} 4j \equiv 3 \ (5) \Leftrightarrow j \equiv 2 \ (5) \overset{\text{def}}{\iff} j = 5k+2 \\ \implies 8^{3^n-2} = 4(5k+2) \Leftrightarrow \boxed{8^{3^n-2} \equiv 8 \ (20) \Leftrightarrow n \equiv 1 \ (2)}. \end{cases}$$

Se concluye que:

$$\boxed{r_{20}(8^{3^n-2}) = 12 \ \forall n \in \mathbb{N} \text{ par} \quad \text{y} \quad r_{20}(8^{3^n-2}) = 8 \ \forall n \in \mathbb{N} \text{ impar}}$$

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

---

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.

Masajeando un poco el enunciado:

$$(n^{109} + 37 : 13 \cdot 2^2) = 13 \cdot 2 \quad \text{y} \quad (n^{63} - 21 : 13 \cdot 3) = 13 \cdot 3$$

¿Qué información obtenemos de los MCD?:
Para que $(n^{109} + 37 : 52) = 26$ debe ocurrir que:

$$\bigstar^1 \begin{cases} 13 \mid n^{109} + 37 \overset{\text{def}}{\iff} n^{109} \equiv 2 \ (13) \overset{\substack{13 \text{ primo} \\ 13 \nmid n}}{\iff} n^1 \equiv 2 \ (13) \\ 2 \mid n^{109} + 37 \overset{\text{def}}{\iff} n^{109} \equiv 1 \ (2) \overset{!!}{\iff} n \equiv 1 \ (2) \\ 4 \nmid n^{109} + 37 \overset{\text{def}}{\iff} n^{109} \not\equiv 3 \ (4) \overset{\bigstar^3}{\iff} \begin{cases} n^{109} \equiv 0 \ (4) \\ \text{o} \\ \boxed{n^{109} \equiv 1 \ (4)} \overset{\substack{!!! \\ n \perp 4}}{\iff} n \equiv 1 \ (4) \\ \text{o} \\ n^{109} \equiv 2 \ (4) \end{cases} \end{cases}$$

En !! pienso en la paridad que tiene que tener n. Dado que n^{109} tiene que ser impar, concluyo que n es impar. Como n debe ser impar en ★3, y me dicen que $n^{109} \not\equiv 3\ (4)$, solo puede ocurrir que $n^{109} \equiv 1\ (4)$.
Si eso último te parece medio fantasma, podés encarar ★3, quizás más mecánicamente, armando 3 sistemas, uno para cada condición del divisor 4. De esa forma vas a eliminar *incompatibilidades* y vas a terminar llegando al único sistema posible (me contó un pajarito).

Para que $(n^{63} - 21 : 39) = 39$ debe ocurrir que:

$$\text{★}^2 \begin{cases} 13 \mid n^{63} - 21 \overset{\text{def}}{\iff} n^{63} \equiv 8\ (13) \overset{13 \text{ primo}}{\underset{13 \nmid n}{\iff}} n^3 \equiv 2^3\ (13) \overset{\text{Tabula Rasta}}{\underset{!}{\iff}} \begin{cases} n \equiv 2\ (13) \\ \text{o} \\ n \equiv 5\ (13) \\ \text{o} \\ n \equiv 6\ (13) \end{cases} \\ 3 \mid n^{63} - 21 \overset{\text{def}}{\iff} n^{63} \equiv 0\ (3) \overset{!}{\iff} n \equiv 0\ (3) \end{cases}$$

Junto info que salió de los MCD. Quedan 3 sistemas de ★1 y ★2, descartando los valores de módulo 13 que son incompatibles con ★1:

$$\begin{cases} n \equiv 2\ (13) \\ n \equiv 1\ (2) \\ n \equiv 1\ (4) \rightsquigarrow \begin{cases} n \equiv 1\ (2) \\ n \equiv 1\ (2) \end{cases} \end{cases} \quad \text{y} \quad \begin{cases} n \equiv 2\ (13) \\ n \equiv 0\ (3) \end{cases}$$

Juntando la info para que sea compatible. Me quedo con $n \equiv 1\ (4)$ para no agregar soluciones de más:

$$\begin{cases} n \equiv 2\ (13) \\ n \equiv 1\ (4) \\ n \equiv 0\ (3) \end{cases}$$

Los divisores son coprimos dos a dos, es decir que por TCHR tenemos solución. La cual queda si no hago cagadas en las cuentas:

$$n \equiv 93\ (156)$$

Por lo tanto el resto que nos pedían es:

$$\boxed{r_{156}(n) = 93}$$

Dale las gracias y un poco de amor ♥ a los que contribuyeron! Gracias por tu aporte:
naD GarRaz Vera R. Francisco Sureda

---

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

Arrancamos con un descontracturante masajeo del enunciado:

$$12^{2^n} \equiv 5^{2^n}\ (7)$$

Busco entonces:

$$r_7(12^{2^n}) = r_7(5^{2^n})$$

Ataco con PTF, 7 es primo y $7 \nmid 5$:

$$r_7(5^{2^n}) = X \overset{\text{def}}{\iff} X \equiv 5^{2^n}\ (7) \overset{\text{PTF}}{\iff} X \equiv 5^{r_6(2^n)}\ (7) \text{★}^1$$

Estudio $r_6(2^n)$:

$$r_6(2^n) = Y \overset{\text{def}}{\iff} 2^n \equiv Y\ (6) \overset{!}{\rightsquigarrow} \begin{cases} 2^n \equiv Y\ (3) \overset{!!}{\iff} \begin{cases} Y \equiv 2\ (3) & \text{si } n \text{ impar} \\ Y \equiv 1\ (3) & \text{si } n \text{ par} \end{cases} \\ 2^n \overset{(2)}{\equiv} 0 \equiv Y\ (2) \end{cases}$$

En !! pensalo como $2^{2k+1} = 4^k \cdot 2 \overset{(3)}{\equiv} 2$. Es así que quedan dos sistemas:

$$\text{para } n \text{ impar } \begin{cases} Y \equiv 2 \ (3) \\ Y \equiv 0 \ (2) \end{cases} \overset{\text{TCR}}{\iff} Y \equiv 2 \ (6) \qquad \text{y} \qquad \text{para } n \text{ par } \begin{cases} Y \equiv 1 \ (3) \\ Y \equiv 0 \ (2) \end{cases} \overset{\text{TCR}}{\iff} Y \equiv 4 \ (6)$$

Volviendo a ★1 sé que los posibles valores que puede tomar el exponente $Y = r_6(2^n)$ son 2 o 4. Es decir que:

$$\begin{cases} X \equiv 5^2 \overset{(7)}{\equiv} 4 \ (7) & \text{si } n \text{ impar} \\ X \equiv 5^4 \overset{(7)}{\equiv} 2 \ (7) & \text{si } n \text{ par} \end{cases}$$

Finalmente:

$$\boxed{r_7(12^{2^n}) = \begin{cases} 2 & \text{si } n \text{ par} \\ 4 & \text{si } n \text{ impar} \end{cases}}$$

Dale las gracias y un poco de amor ♥ a los que contribuyeron! Gracias por tu aporte:
- naD GarRaz
- Nico Alegre
- Dani Tadd
- Ramiro E.

---

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

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

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

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

Arrancando:

$$3^{p^2+3} \equiv -84 \ (p)$$

Estudio los dos casos. Uno cuando $p \nmid 3$ y $p \mid 3$:

Caso $p \nmid 3$ entonces puedo usar el PTF para simplificar un poco:

$$3^{p^2+3} \equiv 3^{r_{(p-1)}(p^2+3)} \ (p) \overset{★1}{\iff} 3^{p^2+3} \equiv 81 \ (p)$$

Calculo ese resto con división de polinomios ★1:

$$\begin{array}{rr|l} p^2 & +3 & p-1 \\ \cline{3-3} -p^2+p & & p+1 \\ \cline{1-1} p+3 & & \\ -p+1 & & \\ \cline{1-1} 4 & & \end{array}$$

El problema ahora queda así:

$$3^{p^2+3} \overset{(p)}{\equiv} 81 \equiv -84 \ (p) \overset{!}{\iff} \underbrace{165}_{5\cdot 3\cdot 11} \equiv 0 \ (p) \overset{\substack{!! \\ p \nmid 3}}{\iff} \begin{cases} p = 5 \\ \text{o} \\ p = 11 \end{cases}$$

Caso $p \mid 3$. Pero como p es primo, entonces $p = 3$:

$$3^{p^2+3} \equiv -84 \ (3) \Leftrightarrow 0 \equiv -84 \ (3) \Leftrightarrow p = 3$$

Tengo entonces 3 *posibles* valores para p:

$$p \in \{3, 5, 11\}\,.$$

Ahora viene el problema de ver si estos 3 valores verifican la segunda condición del enunciado:

$$(7 \cdot p + 8)^{2024} \equiv 4 \ (p)$$

Caso $p = 3$:

$$(7 \cdot 3 + 8)^{2024} \equiv 4 \ (3) \overset{\text{PTF}}{\underset{!!!}{\iff}} 2^0 \equiv 4 \ (3) \Leftrightarrow 1 \equiv 1 \ (3)$$

De donde se rescata que cuando $\boxed{p = 3,}$ está todo bien ☺.

Caso $p = 5$:

$$(7 \cdot 5 + 8)^{2024} \equiv 4 \ (5) \overset{\text{PTF}}{\underset{!!!}{\iff}} 3^0 \equiv 4 \ (5) \iff 1 \equiv 4 \ (5)$$

De donde se rescata que cuando $p = 5$, está todo mal 😨.

Caso $p = 11$:

$$(7 \cdot 11 + 8)^{2024} \equiv 4 \ (11) \overset{\text{PTF}}{\underset{!!!}{\iff}} 8^4 \equiv 4 \ (11) \Leftrightarrow 4096 \equiv 4 \ (11) \iff 4 \equiv 4 \ (11)$$

De donde se rescata que cuando $\boxed{p = 11,}$ está todo bien también ☺.
Por lo tanto los valores de p que cumplen lo pedido son:

$$\boxed{p = 3 \quad \text{y} \quad p = 11}$$

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

---

8. Un coleccionista de obras de arte compró un lote compuesto por pinturas y dibujos. Cada pintura le costó 649 dólares y cada dibujo 132 dólares. Cuando el coleccionista llega a su casa no recuerda si gastó 9779 o 9780 dólares. Deducir cuánto le costó el lote y cuántas pinturas y dibujos compró.

Del enunciado se deduce que el coleccionista no sabe si gastó:

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

Dos ecuaciones diofánticas que no pueden estar bien a la vez, porque el tipo gastó o 9779 o bien 9780, seguramente alguna no tenga solución. *Let's see:*

El $(\underbrace{649}_{11\cdot 59} : \underbrace{132}_{2^2\cdot 3\cdot 11}) = 11$ tiene que dividir al número independiente. En este caso $11 \nmid 9780$ y $11 \mid 9779$, así que gastó un total de 9779 dólares.

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

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

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

$$\begin{cases} 59 = 4 \cdot 12 + 11 \\ 12 = 1 \cdot 11 + 1 \end{cases} \rightarrow 1 = 12 - 1 \cdot \underbrace{11}_{59-4\cdot 12} = (-1) \cdot 59 + 5 \cdot 12.$$

Por lo que se obtiene que:

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

La solución del homogéneo sale fácil. Sumo las soluciones y obtengo la solución general:

$$(P,D)_k = k\cdot(12,-59) + (-889,4445) \quad \text{con } k\in\mathbb{Z}\,.$$

Observación totalmente innecesaria, pero está buena: Esa ecuación es una recta común y corriente. Si quiero puedo ahora encontrar algún punto más bonito, para expresarla distinto, por ejemplo si $k = 75 \implies (P,D)_{\text{part}} = (11,20)$, 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 ★[1] :

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

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

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

---

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*:

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

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

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

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

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

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

Ahora logramos tener el sistema con los divisores coprimos 2 a 2. Por teorema chino del resto este sistema va a tener una solución particular x_0 con $0 \leq x_0 < 3 \cdot 8 \cdot 25 = 600$:

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

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

---

10. Hallar todos los $a \in \mathbb{Z}$ tales que $(855 : a^{126} + 15) = 5$

Como $855 = 5 \cdot 3^2 \cdot 19$, hay que pedir que:

$$a^{126} + 15 \equiv 0 \ (5) \bigstar^1$$
$$a^{126} + 15 \not\equiv 0 \ (3) \bigstar^2$$
$$a^{126} + 15 \not\equiv 0 \ (19) \bigstar^3$$

Resulta que $\bigstar^1$ vale para:

$$a \equiv 0 \ (5)$$

$\bigstar^2$ vale para:

$$a \equiv 1 \ (3) \quad \text{o} \quad a \equiv 2 \ (3)$$

y por último $\bigstar^3$ vale para:

$$\forall a \in \mathbb{Z}$$

lo cual es bueno porque los siguientes sistemas quedan más fáciles.

Resolver los sistemas *que ya tienen divisores coprimos* nos da la solución:

$$\bigstar^4 \begin{cases} a \equiv 0 \ (5) \\ a \equiv 1 \ (3) \end{cases} \quad \text{y} \quad \bigstar^5 \begin{cases} a \equiv 0 \ (5) \\ a \equiv 2 \ (3) \end{cases}$$

nos devuelve los posibles valores que puede tomar a para que se cumpla lo pedido:

$$\bigstar^4 a \equiv 10 \ (15) \quad \text{o} \quad \bigstar^5 a \equiv 5 \ (15)$$

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

---

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

$$p \mid 15^{2p-2} + 7^{p+3} + 174$$

Teniendo en cuenta que $174 = 3 \cdot 2 \cdot 29$

$$p \mid 15^{2p-2} + 7^{p+3} + 3 \cdot 2 \cdot 29 \quad \Leftrightarrow \quad 15^{2p-2} + 7^{p+3} + 3 \cdot 2 \cdot 29 \equiv 0 \ (p)$$

Viendo esa expresión tengo ciertos p primos de interés:

$$p \in \{2, 3, 5, 7, 29\}$$

Hago PTF con p genérico que no divide a ninguno de ese conjunto para ver que sale:
Caso $p \notin \{2, 3, 5, 7, 29\}$:

$$15^{2p-2} + 7^{p+3} + 3 \cdot 2 \cdot 29 \equiv 0 \ (p) \overset{\text{PTF}}{\underset{!!}{\Longleftrightarrow}} 15^0 + 7^4 + 174 \equiv 0 \ (p) \Leftrightarrow 2576 \equiv 0 \ (p) \Leftrightarrow 2^4 \cdot 7 \cdot 23 \equiv 0 \ (p)$$

Por si no lo agarraste, en !! usé:

$$\begin{array}{r|l} 2p-2 & p-1 \\ \hline -2p+2 & 2 \\ \hline 0 & \end{array} \quad \text{y} \quad \begin{array}{r|l} p+3 & p-1 \\ \hline -p+1 & 1 \\ \hline 4 & \end{array}$$

De acá saco que el 23 también puede ser solución.
Arranco a analizar con cada uno de los $p \in \{2, 3, 5, 7, 23, 29\}$ en particular:

- *Caso* $p = 29$:

$$15^{56} + 7^{32} \equiv 0 \ (29) \overset{\text{PTF}}{\Longleftrightarrow} 15^0 + 7^4 \equiv 0 \ (29) \Leftrightarrow 7^4 \equiv 0 \ (29) \Leftrightarrow 23 \equiv 0 \ (29)$$

  $p = 29$ no cumple.
- *Caso* $p = 23$:

$$15^{44} + 7^{26} + 174 \equiv 0 \ (23) \overset{\text{PTF}}{\Longleftrightarrow} 15^0 + 7^4 + 13 \equiv 0 \ (23) \Leftrightarrow 0 \equiv 0 \ (23)$$

  $p = 23$ *cumple*.
- *Caso* $p = 7$:

$$1^{12} + 174 \equiv 0 \ (7) \Leftrightarrow 7 \equiv 0 \ (7) \Leftrightarrow 0 \equiv 0 \ (7) \quad \checkmark$$

  $p = 7$ *cumple*.
- *Caso* $p = 5$:

$$2^8 + 4 \equiv 0 \ (5) \Leftrightarrow 5 \equiv 0 \ (5) \Leftrightarrow 0 \equiv 0 \ (5) \quad \checkmark$$

  $p = 5$ *cumple*.
- *Caso* $p = 3$:

$$1^6 \equiv 0 \ (3) \Leftrightarrow 1 \equiv 0 \ (3)$$

  $p = 3$ no cumple.
- *Caso* $p = 2$:

$$1^0 + 1^5 \equiv 0 \ (2) \Leftrightarrow 0 \equiv 0 \ (2) \quad \checkmark$$

  $p = 2$ *cumple*.

Hay 4 números *primos* que cumplen lo pedido.

El resultado sería:

$$p \in \{2, 5, 7, 23\}$$

Dale las gracias y un poco de amor ♥ a los que contribuyeron! Gracias por tu aporte:
naD GarRaz Dani Tadd

---

12. Determinar todos los primos $p \in \mathbb{N}$ que satisfacen que:

$$5p \mid 6^{p-1} + 10^{p^2} + 119$$

Si $5p \mid 6^{p-1} + 10^{p^2} + 119$ entonces:

$$p \mid 6^{p-1} + 10^{p^2} + 119$$

y ahí puedo sacar info sobre p:

$$p \mid 6^{p-1} + 10^{p^2} + 119 \overset{\text{def}}{\underset{!}{\iff}} 6^{p-1} + 10^{p^2} + 119 \equiv 0 \ (p)$$

Las factorizaciones en primos de los números del ejercicio:

$$(2 \cdot 3)^{p-1} + (2 \cdot 5)^{p^2} + 17 \cdot 7 \equiv 0 \ (p) \ ★^1$$

Si $p = 2$ en $★^1$:

$$0 + 0 + 1 \equiv 0 \ (2)$$

$p = 2$, no sirve $★^2$.

Si $p = 3$ en $★^1$:

$$0 + 1 + 2 \equiv 0 \ (3)$$

$\boxed{p = 3}$, sí sirve. $★^3$

Si $p = 5$ en $★^1$:

$$1 + 0 - 1 \equiv 0 \ (5)$$

$\boxed{p = 5}$, sí sirve. $★^4$

Si $p = 17$ en $★^1$:

$$6^0 + 10^1 \equiv 0 \ (17)$$

$p = 17$, no sirve. $★^5$

Hago el caso con p genérico $★^1$:

$$6^{p-1} + 10^{p^2} + 119 \equiv 0 \ (p) \overset{\text{PTF}}{\iff} 6^0 + 10^1 + 119 \equiv 0 \ (p) \Leftrightarrow 130 \equiv 0 \ (p) \Leftrightarrow 2 \cdot 5 \cdot 13 \equiv 0 \ (p)$$

Encuentro de esta forma que el $\boxed{p = 13}$, sí sirve. $★^6$

De $★^2$, $★^3$, $★^4$, $★^5$ y $★^6$ sé que el 2 y el 17 no sirven pero 3, 5 y 13 sí.

Todo muy lindo, ahora quiero ver si para $p = 3$:

$$5 \cdot 3 \mid 6^{p-1} + 10^{p^2} + 119 \overset{\text{def}}{\iff} 6^2 + 10^9 + 14 \equiv 0 \ (15) \overset{!!!}{\iff} 6 + 10 + 14 \equiv 0 \ (15) \quad \checkmark$$

En !!! cálculo fue el de $10^9 \equiv 10\ (15)$: $\quad X \equiv 10^9\ (15) \rightsquigarrow \begin{cases} X \equiv 0\ (5) \\ X \equiv 1\ (3) \end{cases} \overset{\text{TCH}}{\iff} X \equiv 10\ (15)$

Ahora para $p = 5$:

$$5 \cdot 5 \mid 6^{p-1} + 10^{p^2} + 119 \overset{\text{def}}{\iff} 6^4 + 10^{25} + 19 \equiv 0\ (25) \overset{!}{\iff} 21 + 0 + 19 \equiv 15 \not\equiv 0\ (25)$$

Para $p = 13$:

$$5 \cdot 13 \mid 6^{12} + 10^{169} + 119 \Leftrightarrow 6^{12} + 10^{169} + 54 \equiv 0\ (65) \overset{!!!}{\iff} 1 + 10 + 54 \equiv 0\ (65)$$

En !!! como se hizo antes el cálculo fue el de $10^{169} \equiv 10\ (65)$:

$$X \equiv 10^{169}\ (65) \rightsquigarrow \begin{cases} X \equiv 0\ (5) \\ X \equiv 10^{169}\ (13) \overset{\text{PTF}}{\iff} X \equiv 10\ (13) \end{cases} \overset{\text{TCH}}{\iff} X \equiv 10\ (65)$$

Se concluye de esta forma que los únicos p primos que cumplen que $5p \mid 6^{p-1} + 10^{p^2} + 119$ son:

$$\boxed{p \in \{3, 13\}}$$

Dale las gracias y un poco de amor ♥ a los que contribuyeron! Gracias por tu aporte:
naD GarRaz Nacho Dani Tadd

---

13. Hallar todos los $a \in \mathbb{Z}$ tales que el resto de la división de $15a^{831}$ por 77 es 6.

Teniendo en cuenta que:

$$831 = 3 \cdot 277$$

Queremos ver para cuál valor de a:

$$15a^{831} \equiv 6\ (77)$$

Para poder usar PTF, necesitamos que el divisor sea un número primo:

$$15a^{831} \equiv 6\ (77) \rightsquigarrow \begin{cases} a^{831} \equiv 6\ (7) \bigstar^1 \\ 4a^{831} \equiv 6\ (11) \bigstar^2 \end{cases}$$

Estudio $\bigstar^1$*:*

$$a^{831} \equiv 6\ (7) \Leftrightarrow \begin{cases} \overset{a \equiv 0\ (7)}{\iff} 0 \equiv 6\ (7) \\ \underset{\text{PTF}}{\overset{a \not\equiv 0\ (7)}{\iff}} a^3 \equiv 6\ (7) \underset{\bigstar^3}{\overset{!!}{\iff}} \begin{cases} a \equiv 3\ (7) \\ a \equiv 5\ (7) \\ a \equiv 6\ (7) \end{cases} \end{cases}$$

donde en !! hacés una hermosa tabla de restos.

Estudio $\bigstar^2$*:*

$$4a^{831} \equiv 6\ (11) \Leftrightarrow \begin{cases} \overset{a \equiv 0\ (11)}{\iff} 0 \equiv 6\ (11) \\ \underset{\text{PTF}}{\overset{a \not\equiv 0\ (11)}{\iff}} 4a^1 \equiv 6\ (11) \overset{3 \perp 11}{\iff} a \equiv 7\ (11) \end{cases}$$

Con los resultados encontrados quedan 3 sistemas, uno por cada ecuación en $\bigstar^3$:

$$\begin{cases} a \equiv 7\ (11) \\ a \equiv 3\ (7) \end{cases}, \quad \begin{cases} a \equiv 7\ (11) \\ a \equiv 5\ (7) \end{cases} \text{ y } \begin{cases} a \equiv 7\ (11) \\ a \equiv 6\ (7) \end{cases}$$

Tengo solución por TCH, dado que los divisores son coprimos en todos los sistemas:

Desarrollo el sistema con $a \overset{(7)}{\equiv} 6$, y los otros, *pajilla*:

$$a \equiv 7\ (11) \overset{\text{def}}{\iff} a = 11 \cdot k + 7$$

$$\xrightarrow{\text{reemplazo}}$$

$$11 \cdot k + 7 \equiv 6\ (7) \Leftrightarrow 4 \cdot k \equiv 6\ (7) \overset{\substack{2 \perp 7 \\ !}}{\iff} k \equiv 5\ (7) \overset{\text{def}}{\iff} k = 7 \cdot q + 5$$

$$\xrightarrow[\text{en } a]{\text{reemplazo}}$$

$$a = 11 \cdot (7 \cdot q + 5) + 7 = 77 \cdot q + 62 \overset{\text{def}}{\iff} \boxed{a \equiv 62\ (77)}$$

Las soluciones de los otros sistemas:

$$a \overset{(7)}{\equiv} 3 \quad \to \quad \boxed{a \equiv 73\ (77)}$$
$$a \overset{(7)}{\equiv} 5 \quad \to \quad \boxed{a \equiv 40\ (77)}$$

Dale las gracias y un poco de amor ♥ a los que contribuyeron! Gracias por tu aporte:
Nad Garraz Dani Tadd

---

14. [final 30/07/2024] Determinar todos los primos positivos p que satisfacen:

$$2p \mid 13^{p^2+p} + 3 \cdot 2^p + 295^{p-1}.$$

Arranco acomodando el enunciado:

$$2p \mid 13^{p^2+p} + 3 \cdot 2^p + 295^{p-1} \overset{\text{def}}{\iff} 13^{p^2+p} + 3 \cdot 2^p + 295^{p-1} \equiv 0\ (2p)$$

Quiero ver para cuales valores de p esa ecuación de congruencia es verdadera. Laburo el sistema equivalente, quebrando:

Hay que observar que el sistema quebrado funciona bien por el *teorema chino del resto*. En particular cuando $p = 2$ también funciona (¡Mostralo, sino estás haciendo cagadas!):

$$2p \mid a \implies p \mid a \ \wedge\ 2 \mid a$$

peeeeero, la vuelta no vale en general para $p = 2$.

$$13^{p^2+p} + 3 \cdot 2^p + 295^{p-1} \equiv 0\ (2p) \rightsquigarrow \begin{cases} 1 + 3 \cdot 26p + 295^{p-1} \overset{\substack{(2) \\ !}}{\equiv} 0 \equiv 0\ (2) \\ 13^{p^2+p} + 3 \cdot 2^p + 295^{p-1} \equiv 0\ (p) \bigstar^1 \end{cases}$$

Hay que estudiar $\bigstar^1$ para distintos valores de p. Se va a usar fuerte el *pequeño teorema de Fermat* click click. Factorizando $295 = 5 \cdot 59$ para un $p \notin \{2, 5, 13, 59\}$ así uso PTF:

$$\bigstar^1 \overset{\text{PTF}}{\iff} \bigstar^2 \begin{cases} 2^{p^2+p} \equiv 2\ (p) \\ 13^{p^2+p} \equiv 13^2\ (p) \\ 295^{p-1} \equiv 1\ (p) \end{cases}$$

Donde usé:

$$\begin{array}{r|l} p^2 + p & p-1 \\ \cline{2-2} -\,p^2 + p & p+2 \\ \cline{1-1} 2p & \\ -\,2p + 2 & \\ \cline{1-1} 2 & \end{array} \quad \text{y} \quad \begin{array}{r|l} p-1 & p-1 \\ \cline{2-2} -\,p+1 & 1 \\ \cline{1-1} 0 & \end{array}$$

Metiendo toda la info calculada en $\bigstar^2$ en $\bigstar^1$:

$$13^2 + 3 \cdot 2 + 1 \overset{!}{=} 2^4 \cdot 11 \equiv 0\ (p) \iff p \in \{2, 11\}$$

Muchas cuentas. Pará respirá e interpretá. ¿Qué son estos valores encontrados? ¿Listo? ¿Terminó el ejercicio?

Las cuentas hechas habían arrancado con cierta restricción en p, tengo que laburar los valores que propuse que p no podía tomar para usar el PTF. Por lo tanto ahora voy a ver que pasa ★[1] con los valores de $p \in \{2, 5, 13, 59\}$:

$p = 2$:

$$13^{2^2+2} + 3 \cdot 2^2 + 295^{2-1} \equiv 0 \ (2)$$

$p = 5$:

$$13^{5^2+5} + 3 \cdot 2^5 + 295^{5-1} \equiv 0 \ (5)$$

$p = 13$:

$$13^{13^2+13} + 3 \cdot 2^{13} + 295^{13-1} \ \equiv \ 7 \not\equiv 0 \ (13)$$ 💀

$p = 59$:

$$13^{59^2+59} + 3 \cdot 2^{59} + 295^{59-1} \overset{!!}{\equiv} 54 \not\equiv 0 \ (59)$$ 💀

Los p que cumplen que: $2p \mid 13^{p^2+p} + 3 \cdot 2^p + 295^{p-1}$ son:

$$\boxed{p \in \{2, 5, 11\}}$$

Dale las gracias y un poco de amor ❤ a los que contribuyeron! Gracias por tu aporte:
Tizi S. F. naD GarRaz

---

15. [integrador 16/12/2025] Calcular el resto de dividir por 11 al producto de todos los divisores positivos de $23 \cdot 5^{32}$.

Por suerte el número $23 \cdot 5^{32}$ ya es un producto de primos por lo que es fácil escribir todos los divisores positivos:

$$\begin{cases} 23^{\alpha} & \text{con} \quad 0 \leq \alpha \leq 1 \\ 5^{\beta} & \text{con} \quad 0 \leq \beta \leq 32 \end{cases}$$

Si bien no se pidió hay un total de $(1+1) \cdot (32+1) = 66$ divisores.
El producto de todos los divisores va a ser algo así:

$$23^0 5^0 \cdot 23^0 5^1 \cdots 23^0 5^{31} \cdot 23^0 5^{32} \cdot 23^1 5^0 \cdot 23^1 5^1 \cdots 23^1 5^{31} \cdot 23^1 5^{32} \overset{!!}{=} 23^{32} \cdot 5^{1056}$$

En el !! es solo multiplicar potencias, nada súper raro, bueh, usé la suma de *Gauss*.
Calculo el resto haciendo un par de cuentas y usando *PTF*. 11 es primo y $11 \nmid 5$:

$$23^{32} \cdot 5^{1056} \equiv 1^{32} \cdot 5^{r_{10}(1056)} \ (11) \iff \boxed{23^{32} \cdot 5^{1056} \equiv 5 \ (11)}$$

Por lo tanto:

$$\boxed{r_{11}\big(\textit{el producto de los divisores de } 23 \cdot 5^{32}\big) = 5}$$

---

16. [recuperatorio 21/03/2025]
Encuentre todos los divisores de 3^{200} que tengan resto 82 en la división por 119.

Tiene pinta de que voy a usar PTF. Con $119 = 7 \cdot 17$.
Los divisores de 3^{200} son números de la pinta:

$$\pm 3^{\alpha} \text{ con } \alpha \in [0, 200]$$

Trato a los valores de positivos y negativos por separado:

$$3^\alpha \equiv 82\ (119) \overset{\bigstar^1}{\rightsquigarrow} \begin{cases} 3^\alpha \equiv 5\ (7) & \overset{\text{PTF}}{\underset{\text{7 primo}}{\Longleftrightarrow}} & 3^{r_6(\alpha)} \equiv 5\ (7) \\ 3^\alpha \equiv 14\ (17) & \overset{\text{PTF}}{\underset{\text{17 primo}}{\Longleftrightarrow}} & 3^{r_{16}(\alpha)} \equiv 14\ (17) \end{cases}$$

$$-3^\alpha \equiv 82\ (119) \Leftrightarrow 3^\alpha \equiv 37\ (119) \overset{\bigstar^2}{\rightsquigarrow} \begin{cases} 3^\alpha \equiv 2\ (7) & \overset{\text{PTF}}{\underset{\text{7 primo}}{\Longleftrightarrow}} & 3^{r_6(\alpha)} \equiv 2\ (7) \\ 3^\alpha \equiv 3\ (17) & \overset{\text{PTF}}{\underset{\text{17 primo}}{\Longleftrightarrow}} & 3^{r_{16}(\alpha)} \equiv 3\ (17) \end{cases}$$

Uso tablas de restos para resolver:

$r_6(\alpha)$	0	1	2	3	4	5
$r_7(3^{r_6(\alpha)})$	1	3	2	6	4	5

$r_{16}(\alpha)$	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
$r_{17}(3^{r_{16}(\alpha)})$	1	3	9	10	13	5	15	11	16	14	8	7	4	12	2	6

(¿Cómo harías esto más elegante sin toda esa tabla fea? Mandame un mesaje con esa idea así lo cambiamos, que no me gusta como quedó.)

Para poder satisfacer la ecuaciones de congruencias necesito que:

$$\overset{\text{para}}{\underset{\bigstar^1}{\longrightarrow}} \begin{cases} \alpha \equiv 5\ (6) \rightsquigarrow \begin{cases} \alpha \equiv 2\ (3) \\ \alpha \equiv 1\ (2) \end{cases} \\ \alpha \equiv 9\ (16) \rightsquigarrow \{\ \alpha \equiv 1\ (2) \end{cases}$$

$$\overset{\text{para}}{\underset{\bigstar^2}{\longrightarrow}} \begin{cases} \alpha \equiv 2\ (6) \rightsquigarrow \begin{cases} \alpha \equiv 2\ (3) \\ \alpha \equiv 0\ (2) \end{cases} \\ \alpha \equiv 1\ (16) \rightsquigarrow \{\ \alpha \equiv 1\ (2) \end{cases}$$ 💀

Tengo un sistema compatible solo para $\bigstar^1$, lo que quiere decir que ningún *divisor negativo* de 3^{200} satisface lo que se pide. Resuelvo para encontrar valores de α que cumplan $\bigstar^1$:

$$\begin{cases} \alpha \equiv 2\ (3) \\ \alpha \equiv 9\ (16) \end{cases}$$

Por los divisores con coprimos, por TCH habemos solución, la cual no quiero desarrollar todo el procedimiento porque *pajilla*, pero es $\alpha \equiv 41\ (48)$.

Los divisores de 3^{200} que cumplen que $r_{119}(3^{200}) = 82$:

$$\boxed{\{3^{41};\ 3^{89};\ 3^{137};\ 3^{185}\}}$$