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 es 13 y el resto de la división de $6a$ por 15 es 9.

12) i) Hallar los posibles restos de la división de a por 480

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

No puedo separar en UN PRIMO IGUAL

posibles conflictos pues $2 \mid 8$ y veo si $5 \equiv 1(2)$ y esto vale pues $5 \underset{(2)}{\equiv} 1(2)$. Entonces me quedo con $5(8)$

$$\iff \begin{cases} a \equiv 2(3) \\ a \equiv 3(5) \\ a \equiv 5(8) \end{cases}$$

Como 3, 5 y 8 son COPRIMOS DOS A DOS POR TCR $\exists$ solución y es única MOD 120.

Luego,

(S1) $40y_1 \equiv 2(3) \iff y_1 \equiv 2(3) \Rightarrow x_1 = 80$

(S2) $24y_2 \equiv 3(5) \iff 4y_2 \equiv 3(5) \iff -y_2 \equiv 3(5)$
$\iff y_2 \equiv -3(5)$
$\iff y_2 \equiv 2(5)$
$\Rightarrow x_2 = 48$

(S3) $15y_3 \equiv 5(8) \iff 7y_3 \equiv 5(8) \iff -y_3 \equiv 5(8)$
$\iff y_3 \equiv -5(8)$
$\iff y_3 \equiv 3(8)$
$\Rightarrow x_3 = 45$

Luego, a0 es solución part y es: $x_1+x_2+x_3 = 173$

Y, la solución debe ser menor a 120.

Por lo tanto $a \equiv 173(120) \iff a \equiv 53(120)$

Esto es MÓDULO 120 pero el enunciado pide 480.

$a = 120k + 53$

$a = 120(4 \cdot q + \boxed{r}) + 53$ → resto de 4.

$a = 480q + 120r + 53$

$0 \leq r < 4$

$r = 0,\ a = 480q + 53$

$r = 1,\ a = 480q + 173$

$r = 2,\ a = 480q + 293$

$r = 3,\ a = 480q + 413$

Luego, hay 4 posibles restos 53, 173, 293, 413

12) ii) Hallar el MENOR entero positivo tal que:

$(1:21) | 13$

$$\begin{cases} a \equiv 13(21) \\ 6a \equiv 9(15) \end{cases} \underset{(6:15)|9}{\iff} \begin{cases} a \equiv 13(21) \\ 2a \equiv 3(5) \end{cases} \underset{\cdot 3,\ 3 \perp 5}{\iff} \begin{cases} a \equiv 13(21) \\ a \equiv 4(5) \end{cases}$$

$(6:15)|9$

Como 21 y 5 son coprimos dos a dos, ∃ solución y es única

(S1) $5y_1 \equiv 13(21) \underset{\cdot 4,\ 4 \perp 21}{\iff} 20y_1 \equiv 52(21) \iff y_1 \equiv -52(21)$

$\iff y_1 \equiv 11(21) \Rightarrow x_1 = 55$

(S2) $21y_2 \equiv 4(5) \iff y_2 \equiv 4(5) \Rightarrow x_2 = 84$

Luego, $a \equiv 139 (105) \iff a \equiv 34 (105)$

Por lo tanto $a = 105k + 34$ ✓

Entonces el menor a que satisface es $\overbrace{34}^{k=0}$ ✓

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 en cajas de 12 unidades sobraban 4.
- Al poner las latas en 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?

$$12600 \leq m \leq 13000$$

$$63 = 3.7.3$$
$$12 = 2.2.3$$

$$\begin{cases} m \equiv 4 (12) \\ m \equiv 43 (63) \end{cases} \iff \begin{cases} m \equiv 4 (4) \\ m \equiv 4 (3) \\ m \equiv 43 (9) \\ m \equiv 43 (7) \end{cases} \iff$$

$$\begin{cases} m \equiv 0 (4) \\ m \equiv 1 (3) \\ m \equiv 7 (9) \\ m \equiv 1 (7) \end{cases}$$

$3 | 9, \ 7 \equiv 1 (3) \iff 1 \equiv 1 (3)$ ✓ $\Rightarrow m \equiv 7 (9)$

$$\Leftrightarrow \begin{cases} m \equiv 0(4) \\ m \equiv 7(9) \\ m \equiv 1(7) \end{cases}$$

Luego, como 4, 9 y 7 son coprimos dos a dos $\exists$ solución, es única y es MOD 252.

S_1 $\quad 63y_1 \equiv 0(4) \Leftrightarrow 3y_1 \equiv 0(4) \Leftrightarrow y_1 \equiv 0(4)$
$\Rightarrow x_1 = 0$

S_2 $\quad 28y_2 \equiv 7(9) \Leftrightarrow y_2 \equiv 7(9) \Rightarrow x_2 = 196$

S_3 $\quad 36y_3 \equiv 1(7) \Leftrightarrow y_3 \equiv 1(7) \Rightarrow x_3 = 36$

Luego, $m \equiv 232(252)$ PREGUNTAR ESTO.

Ahora, $m = 252k + 232$

Restar dividir de ambos lados.

sí.

DOBLE DES. AL MISMO TIEMPO. SI PASO IZQ TMB DER. LO MISMO

$$12600 \leq 252k + 232 \leq 13000$$

$$12368 \leq 252k \leq 12768$$

$$49.07 \leq k \leq 50.66$$

$$k \in \{49, 50\}$$

$k = 49 \rightarrow m = 12580$

$k = 50 \rightarrow m = 12832$

Entonces habría 12580 o 12832 latas.

VERIF: $12580 \equiv 232\ (252)$ ✓

$12832 \equiv 232\ (252)$ ✓

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

$a^2 \equiv 21\ (238)$ $\qquad$ $a \equiv\ ?\ (238)$

$238 = 2 \cdot 7 \cdot 17$

Necesito tener potencia para TCR.

$$\begin{cases} a^2 \equiv 21\ (2) \\ a^2 \equiv 21\ (7) \\ a^2 \equiv 21\ (17) \end{cases} \iff \begin{cases} a^2 \equiv 1\ (2) \\ a^2 \equiv 0\ (7) \\ a^2 \equiv 4\ (17) \end{cases}$$

→ NO.

(S1) $119 y_1 \equiv 1\ (2) \iff -y_1 \equiv 1\ (2) \iff y_1 \equiv 1\ (2)$

$\Rightarrow x_1 = 119$

(S2) $34 y_2 \equiv 0\ (7) \iff 6 y_2 \equiv 0\ (7) \iff -y_2 \equiv 0\ (7)$

$\Rightarrow x_2 = 0$

(S3) $14 y_3 \equiv 4\ (17) \overset{\cdot 6}{\iff} 84 y_3 \equiv 24\ (17) \iff -y_3 \equiv 7\ (17)$

$\iff y_3 \equiv 10\ (17)$

$\Rightarrow x_3 = 140$

Luego, $a^2 \equiv 259\ (238) \iff a^2 \equiv 21\ (238)$

* OJO. No puedo hacer TCR xq hay una potencia (a^2).

Hago posibles restos y resuelvo.
Si cada ecuación tiene 2 valores
de a que cumplen, tendré cada uno en
sistema distinto

* · $a^2 \equiv 1(2)$, tabla de restos mod 2.

a	$a^2 \equiv 1(2)$
0	$0 \equiv 1$ X
1	$1^2 \equiv 1$ X ✓

mod 2

$\Rightarrow a \equiv 1(2)$

· $a^2 \equiv 0(7)$ solo si $7 | a$.

$\boxed{a = 0}$ pues $0 \leq a < 6$

$\Leftrightarrow a \equiv 0(7)$ sii $a = 0$

· $a^2 \equiv 4(17)$ → Busco los $a^2 \equiv 4(17)$ → tengo 2 sistemas distintos.

2 a distintos

a	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
a^2	0	1	4	9	16	8	2	15	7	13	15	2	4	16	9	2	1

(17)

Luego, como $a^2 \equiv 4(17)$ si: $a \equiv 2(17)$ v $a \equiv 12(17)$

Así, ① $\begin{cases} a \equiv 0(7) \\ a \equiv 1(2) \end{cases}$ ② $\begin{cases} a \equiv 0(7) \\ a \equiv 1(2) \end{cases}$

$a \equiv 2(17)$

$S_1.\ 34y_1 \equiv 0(7) \Leftrightarrow y_1 \equiv 0(7) \Rightarrow x_1 = 0$

$S_2\ \ 119y_2 \equiv 1(2) \Leftrightarrow y_2 \equiv 1(2) \Rightarrow x_2 = 119$

$S_3.\ 14y_3 \equiv 2(17) \Leftrightarrow 7y_3 \equiv 1(17) \overset{\cdot 5}{\Leftrightarrow} y_3 \equiv 5(17)$

$\Rightarrow x_3 = 70$

Ent $x \equiv 189(238)$

$a \equiv 12(17)$

$S_1\ \ 34y_1 \equiv 0(7) \Rightarrow x_1 = 0$

$S_2\ \ 119y_2 \equiv 1(2) \Rightarrow x_2 = 119$

$S_3\ \ 14y_3 \equiv 12(17) \Leftrightarrow 7y_3 \equiv 6(17)$

$\overset{\cdot 5}{\Leftrightarrow} y_3 \equiv 13(17)$

$\Rightarrow x_3 = 182$

Ent, $x \equiv 63(238)$

Pequeño Teorema de Fermat

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

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

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

PTF: si p / a, ent $a^p \equiv a(p)$

si $p \nmid a$, ent $a^{p-1} \equiv 1(p)$

si $p \nmid a$ ent $a^n \equiv a^{r_{p-1}(n)}(p)$ ¿Cuando uso este? $\Rightarrow$ Es el mismo que el 2do.

i) $5^{22283} \equiv ?(11)$. Como 5 es primo y $11 \nmid 5$

ent aplico PTF.

$5^{10} \equiv 1(11)$ ent $22283 = 2228 \cdot 10 + 3$

Luego $(5^{10})^{2228} \cdot 5^3 \underset{(11)}{\overset{PTF}{\equiv}} 1^{2228} \cdot 5^3 \underset{(11)}{\equiv} 4(11)$

ii) $\underbrace{5 \cdot 7^{2451}}_{1} + \underbrace{3 \cdot 65^{2345}}_{2} - \underbrace{23 \cdot 8^{138}}_{3} \equiv ?(13)$

Reduzco x partes

2. $3 \cdot 0^{2345}$ $\Rightarrow$ Vale reducir pues $3 \cdot 65^1$ o $3 \cdot 65^2$ sigue siendo multiplo 65

3. $3 \cdot 8^{138}$

1. $5 \cdot \ldots\ 13 \nmid 7 \ldots\ 7^{12} \equiv 1(13) \ldots\ 2451 = 12 \cdot \ldots$

1. Ent, $13 \nmid 7$, $7 \equiv 1(13)$, $2451 = 12.204 + 3$

Luego, $5.(\underbrace{7^{12}}_{1 \text{ por PTF}})^{204} \cdot 7^3 = 5.1.7^3$

3. $13 \nmid 8$, $8^{12} \equiv 1(13)$, $136 = 12.11 + 6$

Luego, $3.(\underbrace{8^{12}}_{1 \text{ por PTF}})^{11} . 8^6 = 3.8^6$

MAS EFICIENTE.

Entonces, $5.7^3 + 0 + 3.8^6 \underset{(13)}{\equiv} 12 + 3.(8^3)^2 \underset{(13)}{\equiv} 12 + 3.5^2$

$\underset{(13)}{\equiv} 12 + 10 \underset{(13)}{\equiv} 9(13)$

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

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

i) 97 es PRIMO

$97 \nmid 2$, ent aplico PTF.

$2^{96} \equiv 1(97)$, $194 = 96.2 + 2$

Luego, $(\underbrace{2^{96}}_{1 \text{ por PTF}})^2 . 2^2 X \equiv 7(97)$

$\iff 4X \equiv 7(97)$

$\overset{\cdot 24}{\underset{24 \perp 97}{\iff}} 96X \equiv 168(97)$

$\iff -X \equiv 71(97)$

$\iff X \equiv 26(97)$

ii) $5^{86}x \equiv 3\,(89)$ $\quad a^{n} \equiv a^{r_{p-1}(n)}\,(p)$

89 es primo.

$89 \nmid 5$

* $5^{88} \equiv 1\,(89)$ mi exp $86 < 88$ no puedo usar.

$5^{86}x \equiv 5^{r_{88}(86)}x\,(89)$

$5 \cdot 18 \equiv 1\,(89)$

$x \equiv 3 \cdot 18^{86}\,(89)$

$86 \underset{(88)}{\equiv}$

PREGUNTAR $\Rightarrow$ lo hacen.

me dijo Sofi.

$5^{86} \cdot 5^{2}x \equiv 3 \cdot 5^{2}\,(89)$ $\quad (5^{2} \perp 89)$

* $5^{88}x \equiv 75\,(89) \Leftrightarrow x \equiv 75\,(89)$

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

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

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

i) $a^{27}-a^{3} \equiv ?(728)$

$728 = 2^{3} \cdot 7 \cdot 13$

Debo ver los casos en los que P divide y NO.

Casos $P|a$: Entonces P está dentro de a.

~~Caso 2^3:~~ $\cancel{a^{27}-a^{3} \underset{(2)}{\equiv} 0^{27}-0^{3} \equiv 0(2)}$

2^3 no es PRIMO.

Caso 7: $a^{27}-a^{3} \underset{(7)}{\equiv} 0(7)$

Caso 13: $a^{27}-a^{3} \underset{(13)}{\equiv} 0(13)$

Como sé que 728 DIVIDE VEO solo el caso 2^3 y no 2 y 2^2 porque yo sé que 2^3 divide.

Pero en este caso 2^3 NO es PRIMO, hago tablas de restos para el caso de 8.

Casos $P \nmid a$: Ej: $a=1, P=2$ $\quad 2 \nmid 1$ pero $2 | 1-1$

Caso 7:

$$a^6 \equiv 1(7)$$

$$27 = 6.4 + 3$$

$$\underbrace{(a^6)}_{PTF}{}^4 \cdot a^3 - a^3 \underset{(7)}{\equiv} a^3 - a^3 \equiv 0(7)$$

Caso 13:

$$a^{12} \equiv 1(13)$$

$$27 = 12.2 + 3$$

$$\underbrace{(a^{12})}_{1 \times PTF}{}^2 \cdot a^3 - a^3 \underset{(13)}{\equiv} 0(13)$$

Caso 2^3: Como 8 NO es primo hago tabla de restos.

MOD 8

a	0	1	2	3	4	5	6	7
$a^{27} - a^3$	0	0	0	0	0	0	0	0

Por lo tanto probamos que vale $\forall a \in \mathbb{Z}$

RECETA: si es PRIMO -> CASO DIVIDE, NO DIVIDE
: NO es PRIMO -> TABLA DE RESTOS.

ii)

a)

$$\frac{2a^7+5a-7a^3}{35} \iff 35 \mid 2a^7-5a-7a^3$$

$35=7.5$

Caso $p \mid a$:

Caso 5: $2.\underset{0}{a^7}+5\underset{0}{a}-7\underset{0}{a^3} \underset{(5)}{\equiv} 0\,(5)$

Caso 7: $2\underset{0}{a^7}+5\underset{0}{a}-7\underset{0}{a^3} \underset{(7)}{\equiv} 0\,(7)$

Caso $p \nmid a$:

Caso 5:

$a^4 \equiv 1\,(5)$

$7=4.1+3$

$2.(\underset{1 \text{ por PTF}}{a^4})^1.a^3+5a-7a^3 \underset{(5)}{\equiv} 2a^3+5a-7a^3$

$\iff -5a^3+5a \underset{(5)}{\equiv} 0\,(5)$

Caso 7:

$a^6 \equiv 1\,(7)$

$7=6.1+1$

$2(a^6)^1.a+5a-7a^3 \underset{(7)}{\equiv} 7a-7a^3$

1 por PTF

$\iff 0 (7)$

Por lo tanto probamos que 35 divide $\forall a \in \mathbb{Z}$

✓

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) $\begin{cases} 1.\ 2^{2013} X \equiv 6(13) \\ 2.\ 5^{2013} X \equiv 4(7) \\ 3.\ 2^{2013} X \equiv 2(5) \end{cases}$

1. 13 es primo y $13 \nmid 2$, por PTF $2^{12} \equiv 1(13)$

Así, $2013 = 12 \cdot 167 + 9$

Luego $2^{2013} = (\underbrace{2^{12}}_{1 \text{ por PTF}})^{167} \cdot 2^9 X \equiv 6(13) \iff 2^9 X \equiv 6(13)$

$\iff 5X \equiv 6(13)$

$\overset{\cdot 5}{\underset{5 \perp 13}{\iff}} -X \equiv 30(13)$

$\iff -X \equiv 4(13)$

$\iff X \equiv 9(13)$

2. 7 es primo y $7 \nmid 5$, por PTF $5^6 \equiv 1(7)$

$2013 = 6 \cdot 335 + 3$

$2013 = 6 \cdot 335 + 3$

Luego $5^{2013}x = (\underbrace{5^6}_{1 \text{ por PTF}})^{335} \cdot 5^3 x \equiv 4(7)$

$\iff 5^3 x \equiv 4(7) \iff 6x \equiv 4(7)$

$\iff -x \equiv 4(7)$

$\iff x \equiv 3(7)$

3. 5 es primo y $5 \nmid 2$, por PTF $2^4 \equiv 1(5)$

$2013 = 4 \cdot 503 + 1$

Luego $2^{2013}x = (\underbrace{2^4}_{\text{PTF}})^{503} \cdot 2x \equiv 2(5)$

$\iff 2x \equiv 2(5) \overset{/2}{\iff} x \equiv 1(5)$

Entonces,

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

Como 13, 7 y 5 son coprimos dos a dos por el TCR $\exists$ solución, es única y es módulo 455

(S1) $35y_1 \equiv 9(13) \iff 9y_1 \equiv 9(13) \overset{/9}{\iff} y_1 \equiv 1(13)$
$\Rightarrow x_1 = 35$

(S2) $65y_2 \equiv 3(7) \iff 2y_2 \equiv 3(7) \overset{\cdot 4}{\iff} y_2 \equiv 5(7)$
$\Rightarrow x_2 = 325$

(S3) $91y_3 \equiv 1(5) \iff y_3 \equiv 1(5) \Rightarrow x_3 = 91$

Luego $x \equiv 451(455)$ y como $451 < 455$ es la solución.

ii) $\begin{cases} 10^{49}x \equiv 17(39) \\ 5x \equiv 7(9) \end{cases}$ $39 = 3.13$

POSIBLE CONFLICTO

$\Longleftrightarrow \begin{cases} 10^{49}x \equiv 17(3) \\ 10^{49}x \equiv 17(13) \\ 5x \equiv 7(9) \end{cases} \Longleftrightarrow \begin{cases} \cancel{1^{49}}x \equiv 2(3) \\ 10^{49}x \equiv 4(13) \\ 3.\ 5x \equiv 7(9) \end{cases}$

3. $5x \equiv 7(9) \overset{\cdot 2}{\underset{2\perp 9}{\Longleftrightarrow}} x \equiv 14(9) \Longleftrightarrow x \equiv 5(9)$

$\Longleftrightarrow \begin{cases} {}^{*}x \equiv 2(3) \\ 10^{49}x \equiv 4(13) \\ x \equiv 5(9) \end{cases}$

$* \ 3 | 9, \ 5 \overset{?}{\equiv} 2(3) \Longleftrightarrow 2 \equiv 2(3)$ ✓

Entonces, $\begin{cases} 10^{49}x \equiv 4(13) \\ x \equiv 5(9) \end{cases}$

Como 13 es PRIMO y $13 \nmid 10$, por el PTF $10^{12} \equiv 1(13)$

$49 = 12.4 + 1$

Luego, $\left(10^{12}\right)^4 \cdot 10x \equiv 4(13) \iff 10x \equiv 4(13)$
$\underbrace{\left(10^{12}\right)}_{1 \text{ por PTF}}$

$\overset{/2}{\iff} 5x \equiv 2(13)$

$\overset{\cdot 5}{\iff} 25x \equiv 10(13)$

$\iff -x \equiv 10(13)$

$\iff x \equiv 3(13)$

Entonces el sistema queda

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

Ahora, como 13 y 9 son coprimos dos a dos $\exists$ solución ÚNICA y en MÓDULO 117

(S1) $9y_1 \equiv 3(13) \overset{\cdot 3,\ 3 \perp 13}{\iff} 27y_1 \equiv 9(13)$

$\iff y_1 \equiv 9(13)$

$\Rightarrow x_1 = 81$

(S2) $13y_2 \equiv 5(9) \iff 4y_2 \equiv 5(9)$

$\overset{\cdot 2,\ 2 \perp 9}{\iff} 8y_2 \equiv 10(9)$

$\iff -y_2 \equiv 10(9)$

$\iff y_2 \equiv 8(9)$

$\Rightarrow x_2 = 104.$

Entonces, $x \equiv 185(117)$ pero como $185 > 117$

$\Rightarrow x \equiv 68(117)$

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 $\longrightarrow 2^3 \cdot 7$: El 8 con TABLA DE RESTOS.

i) $\underbrace{3.7^{135}}_{1} + \underbrace{24^{78}}_{2} + \underbrace{11^{222}}_{3} \equiv ?\,(70)$

$70 = 7.10 = 7.5.2$

Ahora planteo un TCR cada uno con su MÓDULO, reduzco, PTF y luego hago solución.
La solución es un resto MOD 70

$$\begin{cases} 3.7^{135} + 24^{78} + 11^{222} \overset{?}{\equiv} x\,(7) & 1 \\ 3.7^{135} + 24^{78} + 11^{222} \overset{?}{\equiv} x\,(5) & 2 \\ 3.7^{135} + 24^{78} + 11^{222} \overset{?}{\equiv} x\,(2) & 3 \end{cases}$$

1. $3.7^{135} + 24^{78} + 11^{222} \underset{(7)}{\equiv} 3^{78} + 4^{222}\ (7)$

Como 7 es primo y $7 \nmid 3$ ni $7 \nmid 4$ uso PTF.

$3^{6} \equiv 1(7) \quad \wedge \quad 4^{6} \equiv 1(7)$

Luego, $78 = 6.13 \qquad 222 = 6.37$

Ent. $3^{78} + 4^{222} \underset{(7)}{\equiv} (3^{6})^{13+0} + (4^{6})^{37+0} \overset{PTF}{\underset{(7)}{\equiv}} (\underbrace{3^{6}}_{\text{1 por PTF}})^{13} . 3^{0} + (\underbrace{4^{6}}_{\text{1 por PTF}})^{37} . 4^{0}$

$\underset{(7)}{\equiv} 1 + 1 \underset{(7)}{\equiv} \boxed{2(7)}$

2. $3 \cdot 7^{135} + 24^{78} + 11^{222} \underset{(5)}{\equiv} 3 \cdot 2^{135} + (-1)^{78} + 1^{222} \underset{(5)}{\equiv} 3 \cdot 2^{135} + 1 + 1$

Luego, Como 5 es primo y $5 \nmid 2$ aplico PTF.

$2^4 \equiv 1(5)$

Ent, $135 = 4 \cdot 33 + 3$

Por lo tanto, $3 \cdot (\underbrace{2^4}_{1 \text{ por PTF}})^{33} \cdot 2^3 + 2 \underset{(5)}{\overset{\text{PTF}}{\equiv}} \underbrace{3 \cdot \overset{3}{8}}_{9(5)=4} + 2 \underset{(5)}{\equiv} \boxed{1(5)}$

3. $\underbrace{3}_{1} \cdot \underbrace{7}_{(-1)}^{135} + \underbrace{24}_{0}^{78} + \underbrace{11}_{1}^{222} \underset{(2)}{\equiv} -1 + 1 \underset{(2)}{\equiv} \boxed{0(2)}$

Luego,

$$\begin{cases} \overset{\times}{3 \cdot 7^{135} + 24^{78} + 11^{222}} \equiv 2(7) \\ \overset{\times}{3 \cdot 7^{135} + 24^{78} + 11^{222}} \equiv 1(5) \\ \overset{\times}{3 \cdot 7^{135} + 24^{78} + 11^{222}} \equiv 0(2) \end{cases}$$

S_1 $10y_1 \equiv 2(7) \iff 3y_1 \equiv 2(7) \overset{\cdot 2}{\iff} -y_1 \equiv 4(7)$

$\iff y_1 \equiv 3(7)$

$\implies x_1 = 30$

S_2 $14y_2 \equiv 1(5) \iff -y_2 \equiv 1(5) \iff y_2 \equiv 4(5)$

$\implies x_2 = 56$

(S_3) $35 y_3 \equiv 0(2) \iff y_3 \equiv 0(2) \Rightarrow x_3 = 0$

Luego, $S = \{x \in \mathbb{Z} : x \equiv 86 \ (70)\}$
$= \{x \in \mathbb{Z} : x \equiv 16 \ (70)\}$

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

ii) $56 = 2^3 \cdot 7$

Veo la suma de restos de cada mod, ie para los dos MOD y luego sistema de ecuaciones

• Caso 2^3: $i^{42} \equiv ? \ (8)$

Tabla de restos MOD 8

i	0	1	2	3	4	5	6	7
i^{42}	0	1	$(2^3)^{14} = 0$	$(3^2)^{21} = 1$	$(4^2)^{21} = 0$	$(5^2)^{21} = 1$	$(6^3)^{14} = 0$	$(7^2)^{21} = 1$

MOD 8

$i^{42} \equiv 0(8)$ sii i es PAR.

$i^{42} \equiv 1(8)$ sii i es IMPAR

Luego, de 1759 tenemos $\left(\frac{1759}{2}\right)$ pares e impares

PREC

879 pares y 880 impares, osea, el resto de la suma MOD 8 es 880, $\Rightarrow$ $880 \ (8) = 0$

$\hookrightarrow \sum_{i=1}^{1759} i^{42} \ (8) = 0$

• Caso 7: 7 es PRIMO

$i^{42} \equiv ?(7)$

Caso $7 \mid i$: $0 \equiv 0(7)$

Caso $7 \nmid i$: Por el PTF $i^6 \equiv 1(7)$

$42 = 7.6 + 0$

Ent. $(i^7)^6 . i^0 \underset{(7)}{\equiv} 1(7)$

Luego, si $7 \nmid i$ el resto es 1.

Osea, los $7K$ no suman.

Tenemos 1759 números, ¿Cuántos múltiplos de 7 hay?

$\#MULT 7: \frac{1759}{7} = 251$, PREGUNTAR Q PASA CUANDO DA CON DECIMAL

Ent., $\#TOTAL - \#MULT 7 = 1508 \Rightarrow 1508 \bmod 7 = 3$

¿El resto no sería 0+3?? no. Ya es 0 mod 8 y 3 mod 7. Lo necesito mod 56.

$$\sum_{i=1}^{1759} i^{42} (7) = 3$$

CUBAWIKI PLANTEA:

Luego, tengo dos restos posibles para un número

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

Como 8 y 7 coprimos dos a dos $\exists$ solución y es mod 56

(S1) $7y_1 \equiv 0(8) \Rightarrow x_1 = 0$

(S2) $8y_2 \equiv 3(7) \Leftrightarrow y_2 \equiv 3(7) \Rightarrow x_2 = 24$

$X \equiv 24 \, (56)$

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

$r_{13}(2^{2^n})$ ¿Qué valores puede tomar n?

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

$7x^{45} \equiv 1\ (46)$

$46 = 2 \cdot 23$

PRIMER VISTAZO

$\begin{cases} 7x^{45} \equiv 1\ (2) \\ 7x^{45} \equiv 1\ (23) \end{cases} \Rightarrow$

El tema está en que ya no sé qué valor le toma x. Puede que $x \mid 23$ o $x \nmid 23$.

Necesito bajar el Exp.
Necesito usar FERMAT de alguna manera.

· Si $x \nmid 23$ y 23 es PRIMO así $x = 23k$

si $x \perp 23$ puede tomar cualquier valor MENOS 23 y sus múltiplos.

$$\Updownarrow$$

$$\begin{cases} x^{45} \equiv 1(2) \\ 7x^{45} \equiv 1(23) \end{cases} \iff \begin{cases} x^{45} \equiv 1(2) \\ 70x^{45} \equiv 10(23) \end{cases} \iff \begin{cases} x^{45} \equiv 1(2) & 1. \\ x^{45} \equiv 10(23) \end{cases}$$

$\cdot 10$

$10 \perp 23$

TABLA DE RESTOS MOD 2.

1.

x	0	$\boxed{1}$
x^{45}	0	$\boxed{1}$

MOD 2

Vale si $x \equiv 1(2)$.

Luego, $\begin{cases} x \equiv 1(2) \\ x^{45} \equiv 10(23) \end{cases}$

Caso $23 \nmid x$ y como 23 es PRIMO x es 23 o MULTIPLO DE 23 osea $23 | x$.

Luego $0^{45} \equiv 10(23)$ ¡ABS!

Caso $23 \perp x$ $(23 \nmid x)$

PTF

$$x^{22} \equiv 1(23)$$

$$45 = 22 . 2 + 1$$

Entonces, $x^{45} \underset{(23)}{\equiv} (x^{22})^2 . x \overset{PTF}{\underset{(23)}{\equiv}} x \equiv 10(23)$

Luego x está entre 0 y 22.

Luego, $\begin{cases} x \equiv 1(2) \\ x \equiv 10(23) \end{cases}$ Como $2 \perp 23$, $\exists$ solución, es única y es MOD 46.

(S1) $23y_1 \equiv 1(2) \iff y_1 \equiv 1(2) \Rightarrow x_1 = 23$

(S2) $2y_2 \equiv 10(23) \overset{/2}{\iff} y_2 \equiv 5(23) \Rightarrow x_2 = 10$

$x \equiv 33(46)$ y como $33 < 46$, es un resto válido

VERIF: $\begin{cases} 33 \equiv 1(2) \\ 33 \equiv 10(23) \end{cases}$

Preg si está bien razonado. ✓

x $\quad 5^{140} = 5^{\alpha}$ $\quad$ Hola Juli

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

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

i) $2p \mid 38^{2p^2-p-1} + 3p + 171$ $\qquad$ ii) $3p \mid 5^{p-1} + 3^{p^2+2} + 833$

23| PRIMER VISTAZO: $25^{70} = 25 \cdot 25 \cdot 25 \ldots$

Divisor: Es de la forma $ak+r$

$\text{Div}_+(25^{70}) \,/\, \begin{cases} x \equiv 2(9) \\ x \equiv 3(11) \end{cases}$

$25^{70} = (5^2)^{70}$ Luego, $5^{140}, 5^m \quad 0 \leq m \leq 140$

$$\begin{cases} 5^m \equiv \underline{2}(9) \\ 5^m \equiv 3(11) \end{cases}$$

Caso 9: Tabla de restos pues 9 no es PRIMO.

m	0	1	2	3	4	$\boxed{5}$	6	7	$\overbrace{8}^{5^4 \cdot 5^4}$	MOD 9
5^m	1	5	7	8	4	$\boxed{2}$	1	5	7	vuelven a repetirse luego de $m \equiv 6(9)$

Luego, $5^m \equiv 2(9) \iff m \equiv 5(9)$

Caso 11: Como 11 es PRIMO y $11 \nmid 5$ por el PTF.

$5^{10} \equiv 1(11)$ $\quad 10 \to 10q+r \Rightarrow 0 \le r < 10$ mod 10

$0 \le r \le 9$

Luego, $5^m \equiv 3(11) \iff 5^{10k+\overline{r_{10}(m)}} \equiv 3(11) \overset{PTF}{\iff} 5^{r_{10}(m)} \equiv 3(11)$

$\underbrace{\qquad}_{\equiv 3(11)}$

$r=0$ no, $r=1$ no, $r=2$ sí, $r=3$ no, $r=4$ no,

$m = 10k+r$

$r=7$ sí. $r=8$ no.

Luego, $5^m \equiv 3(11)$ $\quad m \equiv 2(10)$ $\vee$ $m \equiv 7(10)$ $\quad m = 10k+2$

$m = 10q+2$

VERIF: $5^{10q+2} \equiv 3(11)$

* Es módulo 10 pues es $5^{10k+r_{10}(m)}$

$m \equiv 2(10) = 10k+2$ en 5^{10k+2}

1. $\quad m \equiv 5(9)$

2: $\quad m \equiv 5(9)$

$\begin{cases} m \equiv 2(10) \end{cases}$, $\begin{cases} m \equiv 7(10) \end{cases}$

Por el TCR, como 9 y 10 coprimos dos a dos $\exists$ solución y es mod 90.

1. (S1) $10y_1 \equiv 5(9) \iff y_1 \equiv 5(9) \Rightarrow x_1 = 50$

(S2) $9y_2 \equiv 2(10) \iff -y_2 \equiv 2(10) \iff y_2 \equiv 8(10)$

$\Rightarrow x_2 = 72$

2. (S1) $10y_1 \equiv 5(9) \iff y_1 \equiv 5(9) \Rightarrow x_1 = 50$

(S2) $9y_2 \equiv 7(10) \iff -y_2 \equiv 7(10) \iff y_2 \equiv 3(10)$

$\Rightarrow x_2 = 27.$

Ent, las soluciones posibles son:

$x \equiv 122(90) \iff x \equiv 32(90)$

$x \equiv 77(90)$

¿Cómo verifico si son divisores?

Libro Teresa

- Determinar todos los $a \in \mathbb{Z}$ tales que

$$a \equiv 1 \pmod 4 \quad \text{y} \quad (11\,a + 3\cdot 2^{150} : 3\,a - 2^{151}) = 31.$$

Veamos primero cuáles son los posibles valores del mcd para ver las condiciones que necesitamos. Sea d un divisor común. Entonces:

$$\begin{cases} d \mid 11\,a + 3\cdot 2^{150} \\ d \mid 3\,a - 2^{151} \end{cases} \Longrightarrow \begin{cases} d \mid 33\,a + 9\cdot 2^{150} \\ d \mid 33\,a - 11\cdot 2^{151} \end{cases} \Longrightarrow d \mid 31\cdot 2^{150}.$$

$$\begin{cases} d \mid 11\,a + 3\cdot 2^{150} \\ d \mid 3\,a - 2^{151} \end{cases} \Longrightarrow \begin{cases} d \mid 22\,a + 3\cdot 2^{151} \\ d \mid 9\,a - 3\cdot 2^{151} \end{cases} \Longrightarrow d \mid 31\,a. \quad \text{OK}$$

Ahora bien,

$$d \mid 31\, 2^{150} \;\text{ y }\; d \mid 31\cdot a \iff d \mid (31\, 2^{150} : 31\, a) = \underline{31}\,(2^{150} : a) = 31$$

pues $a \equiv 1 \pmod 4$ implica que a es impar, por lo tanto coprimo con 2^{150}. OK

OK → ¿x7 1? ¿ya no tengo que asegurarlo al 31?

Por lo tanto, el mcd puede ser 1 o 31. Para que sea 31 nos tenemos que asegurar que $31 \mid 11\,a + 3\cdot 2^{150}$ y que $31 \mid 3\,a - 2^{151}$. Pero por el PTF, al ser 31 primo que no divide a 2, se tiene:

$\forall\, d/31.$ Los divisores de 31 son 1 y 31.

$$\begin{aligned} 31 \mid 11\,a + 3\cdot 2^{150} &\iff 11\,a + 3\cdot 2^{150} \equiv 0 \pmod{31} \\ &\underset{\text{PTF}}{\iff} 11\,a + 3\cdot 2^{r_{30}(150)} \equiv 0 \pmod{31} \\ &\iff 11\,a + 3 \equiv 0 \pmod{31} \\ &\iff a \equiv 11 \pmod{31}. \end{aligned}$$

Hay que verificar entonces si $a \equiv 11 \pmod{31}$ implica $31 \mid 3\,a - 2^{151}$:

$$a \equiv 11 \pmod{31} \underset{\text{PTF}}{\Longrightarrow} 3\,a - 2^{151} \equiv 3\cdot 11 - 2^{r_{30}(151)} \equiv 33 - 2 \equiv 0 \pmod{31}.$$

- Determinar todos los $a \in \mathbb{Z}$ tales que

$$a \equiv 1 \pmod 4 \quad \text{y} \quad (11\,a + 3 \cdot 2^{150} : 3\,a - 2^{151}) = 31.$$

$$\begin{aligned}
31 \mid 11\,a + 3 \cdot 2^{150} &\iff 11\,a + 3 \cdot 2^{150} \equiv 0 \pmod{31} \\
&\underset{\text{PTF}}{\iff} 11\,a + 3 \cdot 2^{r_{30}(150)} \equiv 0 \pmod{31} \\
&\iff 11\,a + 3 \equiv 0 \pmod{31} \\
&\iff a \equiv 11 \pmod{31}.
\end{aligned}$$

Hay que verificar entonces si $a \equiv 11 \pmod{31}$ implica $31 \mid 3\,a - 2^{151}$:

$$a \equiv 11 \pmod{31} \underset{\text{PTF}}{\Longrightarrow} 3\,a - 2^{151} \equiv 3 \cdot 11 - 2^{r_{30}(151)} \equiv 33 - 2 \equiv 0 \pmod{31}.$$

Se concluye el ejercicio con el TCR:

$$\begin{cases} a \equiv 1 \pmod 4 \\ a \equiv 11 \pmod{31} \end{cases} \iff a \equiv 73 \pmod{124}.$$

Se concluye que $r_{390}(3 \quad) = 321$.

- Determinar todos los $a \in \mathbb{Z}$ tales que $(12\,a^{41} - a^{31} - a : 55) = 11$:

Como $55 = 5 \cdot 11$, para $b \in \mathbb{Z}$ cualquiera, el valor de $(b : 55)$ puede ser en principio 1, 5, 11 o 55. Por lo tanto, se observa que

$$(b : 55) = 11 \iff 11 \mid b \text{ y } 5 \nmid b.$$ => Decisión acá OK

↳ $12a^{41} \ldots$

Determinamos entonces para qué valores de $a \in \mathbb{Z}$, $11 \mid 12\,a^{41} - a^{31} - a$ y $5 \nmid 12\,a^{41} - a^{31} - a$:

  - Para el 11:

$$11 \mid 12\,a^{41} - a^{31} - a = a\,(12\,a^{40} - a^{30} - 1) \underset{11 \text{ primo}}{\iff} 11 \mid a \text{ o } 11 \mid 12\,a^{40} - a^{30} - 1.$$

-> xq miro el caso q no divide si 11 debe dividir?

Pero si $11 \nmid a$, por el PTF, $a^n \equiv a^{r_{10}(n)} \pmod{11}$. Luego en ese caso,

si: $11 \nmid a$ ent. =)

↳ xq $11 \mid$ toda la EXP pero puede no dividir a "a"

↳ xq si $11 \nmid a$ significa que a no tiene al 11 dentro pero eso no significa que 11 NO divida a toda la EXP.

Ej: $a = 23$, $11 \nmid a$; $a = 22$, $11 \mid a$.

$$12\,a^{40} - a^{30} - 1 \equiv 1\,a^0 - a^0 - 1 \equiv -1 \pmod{11} \Longrightarrow 11 \nmid a^{40} - a^{30} - 1.$$

=> $11 \nmid b$

Por lo tanto

$$11 \mid 12\,a^{41} - a^{31} - a \iff 11 \mid a.$$

$11 \mid b \iff 11 \mid a$

  - Para el 5:

$$5 \mid 12\,a^{41} - a^{31} - a = a\,(12\,a^{40} - a^{30} - 1) \underset{5 \text{ primo}}{\iff} 5 \mid a \text{ o } 5 \mid 12\,a^{40} - a^{30} - 1.$$

Pero si $5 \nmid a$, entonces, por el PTF, $12\,a^{40} - a^{30} - 1 \equiv 2\,a^0 - a^2 - 1 \equiv 1 - a^2 \pmod 5$. Mirando las posibles congruencias de $a^2 \pmod 5$, se tiene

$$1 - a^2 \equiv 0 \pmod 5 \iff a^2 \equiv 1 \pmod 5 \iff a \equiv 1 \text{ o } 4 \pmod 5.$$

Por lo tanto

$$\begin{aligned}
5 \mid 12\,a^{41} - a^{31} - a &\iff a \equiv 0 \text{ o } 1 \text{ o } 4 \pmod 5, \\
5 \nmid 12\,a^{41} - a^{31} - a &\iff a \equiv 2 \text{ ó } 3 \pmod 5.
\end{aligned}$$?? no entiendo

Como necesito que el MCD sea 11, busca los casos que 5 divida y los EXCLUYE. O sea agarro todos menos los que dividen. Como $a \equiv 0, 1, o\ 4$ DIVIDEN y necesito q no divida agarro $a \equiv 2$ y $a \equiv 3$

199/281

Se concluye aplicando el TCR:

1) $11 \mid 12a^{41} - a^{31} - a$ $\wedge$ 2) $5 \nmid 12a^{41} - a^{31} - a$

1) Caso $11 \mid a$: $0^{41} - 0^{31} - 0 \underset{(11)}{\equiv} 0 \mid 11 \mid$ ¿Por que hay que separar en $11 \mid a$ y $11 \nmid a$?

Caso $11 \nmid a$: Como 11 es PRIMO, ∧ $P \nmid a$ ... por el PTF nole que $a^{10}\equiv 1(11)$

Luego, $41 = 4\cdot 10+1$, $31 = 3\cdot 10+1$

$$(a^4)^{10}\cdot a^1 - (a^3)^{10}\cdot a^1 - a \underset{(11)}{\overset{PTF}{\equiv}} -a\,(11)$$

Y si $11\nmid a$ entonces $11\nmid -a \Rightarrow a^{41}-a^{31}-a\not\equiv 0(11)$

Luego, $11 \mid 12a^{41}-a^{31}-a$ sii $11\mid a$.

2) Caso $5\mid a$: $2a^{41}-a^{31}-a\equiv 0(5)$

Caso $5\nmid a$: Como 5 es primo y $5\nmid a$ por el PTF sé que

$$a^4\equiv 1(5)$$

Luego, $41=4\cdot 10+1$ $\quad 31=4\cdot 7+3$

Entonces $2(a^4)^{10}\cdot a-(a^4)^7\cdot a^3 - a \underset{(5)}{\overset{PTF}{\equiv}} 2a-a^3-a \underset{(5)}{\equiv} -a^3+a\,(5)$

Estoy en el caso $5\nmid a$

$$5\mid a-a^3 \iff 5\mid a(1-a^2) \overset{5\nmid a}{\iff} 5\mid(1-a^2)$$

$$\overset{5\text{ es primo}}{\iff} 5\mid(1-a)(1+a) \iff 5\mid(1-a) \vee 5\mid(1+a)$$

Luego, $1-a\equiv 0(5) \quad \vee \quad 1+a\equiv 0(5)$

$$\Updownarrow$$

$a\equiv 1(5) \quad \vee \quad a\equiv 4(5)$

Finalmente

$5 \mid 12a^{41} - a^{31} - a \iff a \equiv 0(5) \vee a \equiv 1(5) \vee a \equiv 4(5)$

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

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

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

24) 2 es primo y p tmb

Caso $p = 2$

$4 \mid 38^{\;\;} + 3(2) + 171$

Vemos a qué es congruente

$$38^5 + 6 + 171 \underset{(4)}{\equiv} 2^5 + 2 + 3 \underset{(4)}{\equiv} 1 \, (4)$$

Luego, $P=2$ no nos sirve.

Caso $P \neq 2$

Como $P \neq 2$ veo que al ser primos distintos $ab \mid c \Rightarrow a \mid c \wedge b \mid c$ a, b primos distintos

Caso $2 \mid 38^{2P^2-P-1} + 3P + 171$

Veo congruencia

$$38^{2P^2-P-1} + 3P + 171 \underset{(2)}{\equiv} P + 1 \, (2)$$

Como todos los primos son impares excepto el 2, pero $P \neq 2$ entonces $P \equiv 1 (2)$.

Luego, $p+1 = 0(2)$ y entonces tenemos que

$\exists$ 2 divisible si $p \neq 2$ $\forall p \neq 2$.

Caso $p \mid 38^{2p^2-p-1} + 3p + 171$

Caso $p \mid 38 \iff p \mid 2.19$

ya sé que $p \neq 2$ entonces sólo vale si es 19.

Caso $p = 19$

$$38^{2p^2-p-1} + 3p + 171 \underset{(19)}{\equiv} 171 \underset{(19)}{\equiv} 0(19)$$

$p = 19$ es solución

Caso $p \nmid 38$ Como p es primo y $p \nmid 38$ aplico el PTF

$$38^{p-1} \equiv 1(p)$$

$$2p^2 - p - 1 = p-1 \cdot q + r$$

$$2p^2 - p - 1 \quad \underline{\lfloor p-1}$$

$$\begin{array}{r} -\;2p^2 - 2p \qquad 2p+1 \\ \hline p - 1 \\ -\quad p - 1 \\ \hline 0 \end{array}$$

$$2p^2 - p - 1 = (p-1)(2p+1) + 0$$

si me pide módulo p debería QUEDAR UN NRO.

$$\left(38^{p-1}\right)^{2p+1} \cdot 38^{0} + 3p + 171 \underset{(p)}{\overset{p \neq 2}{\equiv}} 3\underbrace{p}_{0} + 172 \equiv 172\,(p)$$

Ahora necesito un p tal que $172 \equiv 0\,(p)$

$$172 = 2 \cdot 2 \cdot 43$$

$$2 \cdot 2 \cdot 43 \equiv 0\,(p)$$

y como $p \neq 2$ el único debe ser 43.

Entonces las soluciones son 19 y 43.

ii) Como 3 es PRIMO y P puede ser 3 también tengo un caso aparte pues 3.3 no sería primo

Caso $P = 3$

$$9 \mid 5^2 + 3^{3^2+2} + 833$$

Veo Congruencia

$$25 + 3^{17} + 833 \underset{(9)}{\equiv} 7 + 0 + 5 \underset{(9)}{\equiv} 3 \, (9)$$

Luego $P = 3$ NO DIVIDE.

P DEBE SER DISTINTO DE 3 para que $3P$ divida

Como $P \neq 3$

$$3P \mid 5^{P-1} + 3^{P^2+2} + 833$$

Como $P \neq 3$ y 3 y P son primos distintos

$$3 \mid 5^{P-1} + 3^{P^2+2} + 833 \wedge \underline{P \mid 5^{P-1} + 3^{P^2+2} + 833}$$

Caso 3:

Veo congruencia si divide:

$$5^{P-1} + 3^{P^2+2} + 833 \underset{(3)}{\equiv} 2^{P-1} \equiv (-1)^{P-1} + 2 \, (3)$$

Luego, como $P \neq 3$, y todos los primos excepto el 2 son impares

- $(-1)^{p-1}$ siempre es POSITIVO si $P \neq 2$.

- $(-1)^{p-1}$ es NEGATIVO si $P = 2$.

Luego,

- si $P \neq 2$, $1+2 \equiv 0 (3)$
- si $P = 2$, $-1+2 \equiv 1 (3)$

Por lo tanto 3 divide si P NO es 2 ni 3.

*1

3 DIVIDE si $P \neq 2$ o $P \neq 3$.

Caso $P | 5^{P-1} + 3^{P^2+2} + 833$

si $P | 5 \wedge P | 3$ P no es primo ¿?

Caso $P | 5 \Rightarrow P = 5$

$$5^4 + 3^{27} + 833 \underset{(5)}{\equiv} (3^2)^{13+1} + 3 \underset{(5)}{\equiv} 3^2 + 3 \equiv 2 (5)$$

Luego, $P=5$ no divide.

Caso $P | 3 \Rightarrow P = 3$

$$5^2 + 3^{3^2+2} + 833 \underset{(3)}{\equiv} 1 + 2 \equiv 0(3)$$

Luego $p = 3$ DIVIDE ?? ¿Llegué ABS? 3 divide si $p \neq 3$.
Acá $p = 3$, entonces ¿divide?

Caso $p \nmid 5^{p-1} + 3^{p^2+2} + 833$

Como p es primo y $p \nmid 5$ y $p \nmid 3$ aplico el PTF

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

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

$[\, p-1 = (p-1).1 + 0$

$[\, p^2+2 = (p-1).(p+1) + 3$

Entonces, $(5^{p-1})^{1} . 5^{0} + (3^{p-1})^{(p+1)} . 3^{3} + 833 \underset{(p)}{\equiv} 861 (p)$

*1

$861 = 3.7.41$ pero 3 no vale pues si $p = 3$ no divide.

Caso $p = 7$

$$5^{7-1} + 3^{7^2+2} + 833 \underset{(7)}{\equiv} 5^6 + (3^3)^{17} + 833 \underset{(7)}{\equiv} 1 + (-1)^{17} + 0 \equiv 0(7)$$

Luego $p = 7$ divide.

Caso $p = 41$

$$5^{41-1} + 3^{41^2+2} + 833 \underset{(41)}{\equiv} \quad ?$$

PREGUNTAR. ME MAREE MUCHO.

$3p = 9$.

¿Si $3p \mid x$ sii $p \neq 3$, $3 \mid x$ puede pasar que $p \mid x$ siendo $p = 3$? Pregunta xq llegué a eso pero si $3 \mid x$ y $p \mid x$ siendo $p = 3$ no sería el caso $9 \mid x$?

Puede haber 1, 2, 3... necesito fórmula/ TCR/

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

$88 = 2^3 . 11$

si el MCD es $2 \Rightarrow 2^2, 2^3$ y 11 no dividen a

$a^{760}+11a+10$. Busco los casos donde dividan para excluirlos.

Caso $11 | a$

$$a^{760}+11a+10 \underset{(11)}{\equiv} 10(11)$$ Luego, $11 \nmid a$. ✓

$\hookrightarrow a \equiv 10(11)$ mediante

Caso $11 \nmid a$

Como 11 es PRIMO, por el PTF

$a^{10} \equiv 1(11)$ luego $760 = 10 \cdot 76 + 0$

$$(a^{10})^{76} \cdot a^{0} + 11a + 10 \overset{PTF}{\underset{(11)}{\equiv}} 11 + 11a \underset{(11)}{\equiv} 0(11)$$

¡ABS! ?

Caso $2 | a$:

$$a^{760}+11a+10 \underset{(2)}{\equiv} 0(2)$$ Luego 2 divide ✓

Caso $2 \nmid a$: (a no tiene el 2 en su factor PRIMOS)

Por el PTF $a \equiv 1(2)$

$760 = 1 \cdot 760 + 0$

$2 \nmid a$ luego como 2 es PRIMO a es IMPAR.

$$(a^{1})^{760} \cdot a^{0} + 11a + 10 \overset{PTF}{\underset{(2)}{\equiv}} 1 + a \underset{(2)}{\equiv} 0(2)$$

Luego 2 divide $\forall a$. a PAR o a IMPAR.

Caso $2^2 \mid a^{760} + 11a + 10$

Como 4 no es primo, tabla de restos

a	$a^{760} + 11a + 10$ MOD 4
0	2
1	2
2	$(2^2)^{380} + (-1)a + 2 = 0$
3	$(3^2)^{380} + (-1)a + 2 = 1 - 3 + 2 = 0$

Luego, 2^2 divide sii $a \equiv 2(4)$, $a \equiv 3(4)$

Ent., a mi me sirven los casos $a \equiv 0(4)$ y $a \equiv 1(4)$ pues necesito que 2^2 no divida.

Entonces si $a \equiv 0(4)$ ∧ $a \equiv 1(4)$ no divide 2^3 + imp.

Ent. 1. $\begin{cases} a \equiv 0(4) \\ a \equiv 10(11) \end{cases}$ y 2. $\begin{cases} a \equiv 1(4) \\ a \equiv 10(11) \end{cases}$

(Como $4 \perp 11$ dos a dos)

Por el TCR, $\exists$ solución y es módulo 44.

1. (S_1) $11y \equiv 0(4) \iff -y_1 \equiv 0(4) \implies x_1 = 0$

$.3, 3 \perp 11$

(S_2) $4y_2 \equiv 10(11) \iff y_2 \equiv 30(11) \iff y_2 \equiv 8(11)$
$\implies x_2 = 32.$

Ent, $a \equiv 32(44)$

2. (S1) $11y_1 \equiv 1(4) \iff -y_1 \equiv 1(4) \iff y_1 \equiv 3(4)$

$\Rightarrow x_1 = 33$

$\cdot 3, \; 3 \perp 11$

(S2) $4y_2 \equiv 10(11) \iff y_2 \equiv 30(11) \iff y_2 \equiv 8(11)$

$\Rightarrow x_2 = 32$

Ent $a \equiv 65(44) \iff a \equiv 21(44)$ ✓ ✓

PREG no está bien razonado y el tema del ¡ABS! llegué a $0(11)$ cuando $11 \nmid a$.

Rehago las de PRÁCTICA:

1) Hallar el resto de dividir

$X = 4 . 7^{2311} + 3 . 114^{1571} - 2 . 5^{43}$ por 35

Tengo que ver $4 . 7^{2311} + 3 . 114^{1571} - 2 . 5^{43} \equiv ?(35)$

35 = 7.5 por lo tanto el resto final sale de un TCR xq primero busco MOD 7, luego MOD 5 y luego junto.

Caso 7:

$$3 \cdot 2^{1571} + 5^{44} \equiv ?\ (7).$$

Como 7 es PRIMO y $7 \nmid 2$, por el PTF

$$2^6 \equiv 1\ (7) \Rightarrow 1571 = 6 \cdot 261 + 5$$

Como 7 es PRIMO y $7 \nmid 5$, por el PTF

$$5^6 \equiv 1\ (7) \Rightarrow 44 = 6 \cdot 7 + 2$$

Ent, $3\left(2^6\right)^{261} \cdot 2^5 + \left(5^6\right)^7 \cdot 5^2 \underset{(7)}{\equiv} 3 \cdot 32 + 5^2 \underset{(7)}{\equiv} 2\ (7)$

Caso 5:

$$(-1) \cdot 2^{2311} + \overbrace{3 \cdot (-1)^{1571}}^{-3} + 0 \underset{(5)}{\equiv} (-1) \cdot \left(2^4\right)^{577} \cdot 2^3 - 3 \equiv 4\ (5)$$

$5 \nmid 2$, $2^4 \equiv 1\ (5)$

$$2311 = 4 \cdot 577 + 3$$

Luego, necesito el resto MOD 56.

$\begin{cases} x \equiv 2(7) \\ x \equiv 4(5) \end{cases}$ Por el TCR, como $7 \perp 5$ y tomamos y en módulo 35.

(S_1) $5y_1 \equiv 2(7) \overset{\cdot 3,\ 3|7}{\iff} y_1 \equiv 6(7) \Rightarrow x_1 = 30$

(S_2) $7y_2 \equiv 4(5) \iff 2y_2 \equiv 4(5) \overset{\cdot 3,\ 3|5}{\iff} y_2 \equiv 2(5)$

$\Rightarrow x_2 = 14$

Así, $x \equiv 44(35) \iff x \equiv 9(35)$

2) Hallar todos los primos $p > 0$ tq $p \mid 2^p + 5$

Si $p \mid 2^p + 5 \Rightarrow 2^p + 5 \equiv 0(p)$

¿Qué valores de p hacen eso?

$p \mid 2^p$ OJO xq p podría ser 2.

Por el PTF, $a^p \equiv a(p)$ con p PRIMO

Luego $2^p \equiv 2(p)$ así $2 + 5 \equiv 0(p)$ luego para que el resto sea 0 debe suceder que $p = 7$.

3) Hallar el resto de dividir

$S = \sum_{k=1}^{3240} k^{120}$ por $\overset{\text{PRIMO}}{\widehat{11}}$

Como 11 es primo, la solución será MOD 11 y no uso TCR.

Como 11 es primo separo en 2 casos, para ver como repite el ciclo.

Caso $11 \mid K$: $K^{120} \underset{(11)}{\equiv} 0(11)$ => si K es múltiplo de 11 resto 0.

Caso $11 \nmid K$: por el PTF. $K^{10} \equiv 1(11)$

$$120 = 10.12 + 0$$

ent $(K^{10})^{12} . K^{0} \underset{(11)}{\overset{PTF}{\equiv}} 1(11)$ => si K NO es múltiplo de 11 resto 1

Luego, ¿Cuántos múltiplos de 11 hay en la sumatoria?

$\#MULT\,11 = 3240/11 = 294.$ → 294 NROS que MOD 11 dan 0.

Ent, $\#TOTAL - \#MULT\,11 = 3240 - 294 = 2946$

Ent, como hay 2946 nros con resto 1, ent

$$2946 \underset{(11)}{\equiv} 9(11)$$

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

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

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

ii)

Caso $P = 3$

$$9 \mid 5^{2} + 3^{11} + 833$$

$$5^{2} + 3^{11} + 833 \overset{?}{\underset{(9)}{\equiv}} 3 + 0 \underset{(9)}{\equiv} 3\ (9)$$

Luego, si $P=3$, No divide.

Caso $P \neq 3$

$$3P \mid 5^{P-1} + 3^{P^2+2} + 833$$

Por $ab \mid c$ y $a \perp b \Rightarrow a \mid c \wedge b \mid c$

1) $3 \mid 5^{P-1} + \underline{3^{P^2+2}} + 833$

y 2) $P \mid 5^{P-1} + 3^{P^2+2} + 833$

1) $5^{\;\cdots} + 3^{p^2+2} + 833 \underset{(3)}{\equiv} 2^{\;\cdots} + 2 \; (3)$

P NO puede ser 3.

Si P ES PAR, NO DIVIDE

Si P ES IMPAR, DIVIDE
PRIMO

Luego 3 DIVIDE sii es PRIMO IMPAR

2) $5^{p-1} + 3^{p^2+2} + 833 \underset{(p)}{\overset{?}{\equiv}}$

$$\underbrace{5^{p-1}} + 3^{p^2+2} + 833 \equiv 0 \quad (p)$$

$p \neq 5 \qquad \underbrace{1 + 3^3 + 833} = 861$
$= 3 \cdot 7 \cdot 41$

$p \neq 3 \qquad 3^{p^2+2} = 3^{\cancel{(p+1)(p-1)}+3}$

$$p^2+2 = \cancel{p(p-1)+p+2}$$

$$\cancel{p^2-p}$$

$$(p+1)(p-2)+3$$

$$p^2-1$$

$3 \cdot 7 \cdot 41 \equiv 0$

$5, 3, 7, 41$

$2^4 \equiv 2^{2^{2^n}}$ for 13

$2^{12} \equiv 1 \mod 13$

$2^{2^n} = \cancel{4} \mod 12$

$\equiv x \mod 4$

$1 \quad \cancel{2^n} \equiv \cancel{2} \mod 3$

$(-2)^{2^n} =$ $\qquad x \equiv 4 \ (12)$

$2 \quad \underline{4} \quad 7 \quad 10$

$7 \mid a$

$ax + by = c \qquad 3 \mid b$

$(m + k$