Álgebra 1

Práctica 5: Sistemas de ecuaciones lineales de Congruencia y Teorema Chino del Resto

Patricia Jancsa
Viernes 2/6/2023

Ej. 1.

a) Determinar si existen y, en caso afirmativo, hallar todas las soluciones del sistema de congruencias

$$\begin{cases} x & \equiv 2 \ mod\ 4 \\ x & \equiv 13 \ mod\ 25 \end{cases}$$

¿Cuánto vale la mínima solución positiva?

Solución: $mcd(4:25) = 1$

$$\Longrightarrow \text{el sistema tiene infinitas soluciones en } \mathbb{Z}$$

$$\text{y una única solución módulo } 100 = 4 \cdot 25$$

¿Cómo se calculan?

$$\begin{cases} x & \equiv 2 \ mod\ 4 & \Longrightarrow & x = 4k + 2 : \ k \in \mathbb{Z} \\ x & \equiv 13 \ mod\ 25 & \Longrightarrow & x = 25m + 13 : \ m \in \mathbb{Z} \end{cases}$$

$$\Longrightarrow x \quad = 25m + 13 \quad \equiv m + 1 \quad \equiv 2 \mod 4$$

$$\Leftrightarrow m \quad \equiv 1 \; mod \; 4$$

$$\Leftrightarrow m = 4q + 1 : \; q \in \mathbb{Z}$$

Por lo tanto, $x = 25m + 13 = 25(4q + 1) + 13$

$$= 100q + 25 + 13$$

$$\Longrightarrow \; Soluciones \; = \{x = 100q + 38 : \; q \in \mathbb{Z}\} \checkmark$$

$\Longrightarrow$ La mínima solución positiva es $x_0 = 38$.

Comprobación

Reemplacemos en el sistema dado:

$$\begin{cases} x = 100q + 38 \equiv 38 \equiv 2 \ mod \ 4 \\ x = 100q + 38 \equiv 38 \equiv 13 \ mod \ 25 \checkmark \end{cases}$$

Ej. 1. b)

Hallar todas las soluciones del sistema de congruencias

$$\begin{cases} x & \equiv 118 \ mod\ 20 \\ x & \equiv 238 \ mod\ 50 \end{cases}$$

$Mcd(20:50) = 10 \neq 1 \Longrightarrow$ no garantiza soluciones en $\mathbb{Z}$

$$Calculemos: \ \boxed{20 = 2^2 \cdot 5, \ 50 = 2 \cdot 5^2}$$

C. Auxiliares

$$x \equiv 118 \ mod\ 20 \Leftrightarrow 20|(x-118)$$

$$\Leftrightarrow 4|(x-118) \ \wedge \ 5|(x-118)$$

$$\Leftrightarrow x \equiv 118 \ mod\ 4 \ \wedge \ x \equiv 118 \ mod\ 5$$

Del mismo modo,

$$x \equiv 238 \ mod \ 50 \Leftrightarrow 50|(x-238)$$

$$\Leftrightarrow 25|(x-238) \ \wedge \ 2|(x-238)$$

$$\Leftrightarrow x \equiv 238 \ mod \ 25 \ \wedge \ x \equiv 238 \ mod \ 2$$

Teorema Chino del Resto

$$\begin{cases} x \equiv 118 & \equiv 18 \; mod \; 20 \Leftrightarrow \begin{cases} x & \equiv 2 \; mod \; 4 \Longrightarrow x \equiv 0 \; mod \; 2 \\ x & \equiv 3 \; mod \; 5 \end{cases} \\ x \equiv 238 & \equiv 38 \; mod \; 50 \Leftrightarrow \begin{cases} x & \equiv 0 \; mod \; 2 \\ x & \equiv 13 \; mod \; 25 \Longrightarrow x \equiv 3 \; mod \; 5 \end{cases} \end{cases}$$

$\Longrightarrow$ las ecuaciones son compatibles y el sistema tiene soluciones en $\mathbb{Z}$

Además, el sistema es equivalente a

$$\begin{cases} x & \equiv 2 \; mod \; 4 \\ x & \equiv 13 \; mod \; 25 \end{cases}$$

cuyas soluciones son las del item a):

$$\Longrightarrow \; Soluciones \; = \{x = 100q + 38 : \; q \in \mathbb{Z}\} \checkmark$$

Ej. 2.

Determinar si existen y, en caso afirmativo, hallar todas las soluciones de cada sistema de congruencias

$$a)\ \begin{aligned} x &\equiv 160\ mod\ 14 \\ x &\equiv 148\ mod\ 35 \end{aligned} \qquad b)\ \begin{aligned} n &\equiv 36\ mod\ 21 \\ n &\equiv 54\ mod\ 45 \\ n &\equiv 89\ mod\ 35 \end{aligned}$$

Solución: a) $mcd(14 : 35) = 7 \neq 1$

$\Longrightarrow$ no garantiza que exista alguna solución del sistema

$$14 = 2 \cdot 7, \quad 35 = 5 \cdot 7$$

$$\begin{cases} x \equiv 160 \quad \equiv 6 \; mod \; 14 \Leftrightarrow \begin{cases} x & \equiv 6 \; mod \; 7 \\ x & \equiv 0 \; mod \; 2 \end{cases} \\ x \equiv 148 \quad \equiv 8 \; mod \; 35 \Leftrightarrow \begin{cases} x & \equiv 3 \; mod \; 5 \\ x & \equiv 1 \; mod \; 7 \Longrightarrow x \not\equiv 6 \; mod \; 7 \end{cases} \end{cases}$$

$\Longrightarrow$ las ecuaciones son incompatibles y el sistema no tiene ninguna solución

Ej. 2. b)

$$\begin{cases} n & \equiv 36 \; mod \; 21 \\ n & \equiv 54 \; mod \; 45 \\ n & \equiv 89 \; mod \; 35 \end{cases}$$

Solución b) $21, \; 45, \; 35$ no son coprimos dos a dos
$\Longrightarrow$ T. Chino del Resto no garantiza que exista alguna solución del sistema

$$\begin{cases} x \equiv 36 \equiv 15 \; mod \; 21 & \Leftrightarrow \begin{cases} x & \equiv 1 \; mod \; 7 \\ x & \equiv 0 \; mod \; 3 \end{cases} \\ x \equiv 54 \equiv 9 \; mod \; 45 & \Leftrightarrow \begin{cases} x & \equiv 4 \; mod \; 5 \\ x & \equiv 0 \; mod \; 9 \Longrightarrow x \equiv 0 \; mod \; 3 \end{cases} \\ x \equiv 89 \equiv 19 \; mod \; 35 & \Leftrightarrow \begin{cases} x & \equiv 4 \; mod \; 5 \\ x & \equiv 5 \; mod \; 7 \Longrightarrow x \not\equiv 1 \; mod \; 7 \end{cases} \end{cases}$$

$\Longrightarrow$ las ecuaciones son incompatibles y el sistema no tiene ninguna solución

Ej. 3.

Se sabe que el resto de dividir a n por 18 es 2 y el resto de dividir a n por 20 es 6. Hallar los posibles restos de dividir a n por 360.

$$Datos: \begin{cases} n & \equiv 2 \; mod \; 18 \quad \Leftrightarrow \quad 18|(n-2) \\ n & \equiv 6 \; mod \; 20 \quad \Leftrightarrow \quad 20|(n-6) \end{cases}$$

$$\begin{cases} n \equiv 2 \quad mod\ 18 \Leftrightarrow \begin{cases} n & \equiv 2\ mod\ 2 \Longrightarrow n \equiv 0\ mod\ 2 \\ n & \equiv 2\ mod\ 9 \end{cases} \\ n \equiv 6 \quad mod\ 20 \Leftrightarrow \begin{cases} n & \equiv 6\ mod\ 4 \Longrightarrow n \equiv 2\ mod\ 4 \\ n & \equiv 6\ mod\ 5 \Longrightarrow n \equiv 1\ mod\ 5 \end{cases} \end{cases}$$

$\Longrightarrow$ las ecuaciones son compatibles
$\Longrightarrow$ el sistema tiene soluciones en $\mathbb{Z}$
y una única solución módulo $9 \cdot 5 \cdot 4 = 180$

entonces n debe cumplir

$$\begin{cases} n & \equiv 2\ mod\ 9 \\ n & \equiv 1\ mod\ 5 \\ n & \equiv 2\ mod\ 4 \end{cases}$$

Soluciones módulo $180 = 9 \cdot 5 \cdot 4$

$$
\begin{cases}
n \equiv 2 \; mod \; 9 & \Leftrightarrow n = 9k + 2 \\
n \equiv 1 \; mod \; 5 & \Leftrightarrow n = 9k + 2 \equiv 4k + 2 \equiv 1 \; mod \; 5 \\
 & \Leftrightarrow k \equiv 1 \Leftrightarrow k = 5m + 1 \\
 & \\
 & \Leftrightarrow n = 9(5m + 1) + 2 \\
 & \\
n \equiv 2 \; mod \; 4 & \Leftrightarrow n = 9 \cdot 5 \cdot m + 11 \equiv 2 \; mod \; 4 \\
 & \Leftrightarrow 1 \cdot 1 \cdot m + 11 \equiv m + 3 \equiv 2 \\
 & \Leftrightarrow m \equiv 3 \; mod \; 4 \\
 & \Leftrightarrow m = 4 \cdot q + 3 \\
 & \\
 & \Leftrightarrow n = 9 \cdot 5 \cdot (4 \cdot q + 3) + 11 \\
 & \Leftrightarrow n = 180 \cdot q + 146
\end{cases}
$$

$\Longrightarrow$ el resto de dividir a n por 180 es $\text{resto}(n)_{180} = 146$

¿Qué podemos decir del resto de dividir a x por 360?

$$360 = 2 \cdot 180$$

Ej. 3. b)

Calcular los posibles restos de dividir a n por 360

Solución:

$$n = 180 \cdot q + 146$$

Pero $360 = 2 \cdot 180$,

$$q = 2 \cdot d + r : r = 0, 1 \implies n = 180 \cdot (2 \cdot d + r) + 146$$
$$\implies n = 360 \cdot d + \underbrace{180r + 146}_{resto\ \ mod\ \ 360}$$

entonces los posibles restos mod 360 son

$$\implies \begin{cases} r = 0 \implies resto_{360}(n) = 146 \\ r = 1 \implies resto_{360}(n) = 180 + 146 = 326 \ \checkmark \end{cases}$$

Práctica 5: Pequeño Teorema de Fermat

Pequeño Teorema de Fermat

Sea p un primo positivo, entonces para todo $a \in \mathbb{Z}$,

$$a^p \equiv a \ mod \ p$$

Si $p \nmid a$

$$a^{p-1} \equiv 1 \ mod \ p$$

Ejemplo: $2^{12} \equiv 1 \ mod \ 13$
Comprobación: $2^{12} = (2^4)^3 = (16)^3 \equiv (3)^3 = 27 \equiv 1 \ mod \ 13$

Corolario del Pequeño Teorema

Corolario: Sea p un primo positivo, $a \in \mathbb{Z} : p \nmid a$;
$n \equiv r \ mod \ (p-1)$ entonces

$$a^n \equiv a^r \ mod \ p$$

En particular, $a^n \equiv a^r \ mod \ p$ para $r = r_{p-1}(n)$

Ejercicio 4. Calcular el resto de dividir a 2^{147} por 13:

$$p = 13 \ primo \nmid 2 \implies p - 1 = 12 \implies 2^{12} \equiv 1 \ mod \ 13$$

$$exponente \ 147 = 144 + 3 = (12)^2 + 3 \equiv \ mod \ 12$$

$$\implies 2^{147} \equiv \underbrace{(2^{12})}_{\equiv 1 mod \ 13}{}^{12} \cdot 2^3 \equiv 2^3 \equiv 8 \ mod \ 13$$

$$\implies r_{13}(2^{147}) = 8 \ \checkmark$$

Ejercicio 5.

Probar que $17|a^{4048} - a^{6^{13}}$ para todo $a \in \mathbb{Z}$.

Solución: $p = 17$ primo positivo, si $17|a \Longrightarrow 17|a^{4048} - a^{6^{13}}$

Si $17 \nmid a$ entonces

$$n \equiv r \ mod\ 16 \Longrightarrow a^n \equiv a^r \ mod\ 17$$

$$4048 = 16 \cdot 253 \equiv 0 \ mod\ 16 \Longrightarrow a^{4048} \equiv a^0 \equiv 1 \ mod\ 17$$

Análogamente,

$$6^{13} = 2^{13} \cdot 3^{13} = 2^{4^3} \cdot 2 \cdot 3^{13} = 16^3 \cdot 2 \cdot 3^{13} \equiv 0 \ mod\ 16$$

$$\Longrightarrow a^{6^{13}} \equiv a^0 \equiv 1 \ mod\ 17$$

$$\Longrightarrow a^{4048} - a^{6^{13}} \equiv 1 - 1 \equiv 0 \ mod\ 17, \ para\ todo\ a \in \mathbb{Z}$$

Ejercicio 6. a.

Calcular el resto de dividir por 11 a $N = 49^{3894}$.

Solución: $49 \equiv 5 \ mod\ 11$

$$\Longrightarrow N = 49^{3894} \equiv 5^{3894} \ mod\ 11$$

Calculemos el resto mod 10 del exponente:

$$3894 \equiv 4 \ mod\ 10$$

entonces

$$N = 49^{3894} \equiv 5^{3894} \equiv a^n \equiv a^r = 5^{r_{10}(3894)} \equiv 5^4 \ mod\ 11$$

$$\equiv 25^2 \equiv 3^2 \equiv 9 \ mod\ 11$$

Por lo tanto, el resto de $N = 49^{3894} \mod 11$ es $r_{11}(N) = 9$

Ejercicio 6. b.

Calcular el resto de dividir por 11 a $m^E = 57^{37^{3001}}$

Solución: Calculemos el exponente $r = r_{10}(37^{3001})$

$$exponente\ E \equiv r \equiv 37^{3001} \equiv 7^{3001}\ mod\ 10$$

$$\equiv (-3)^{3000} \cdot (-3) \equiv 9^{1500} \cdot (-3)\ mod\ 10$$

$$\equiv (-1)^{1500} \cdot (-3) \equiv -3 \equiv 7\ mod\ 10$$

Además, $57 \equiv 2\ mod\ 11$

$$\Longrightarrow m^E = 57^{37^{3001}} \equiv 2^{37^{3001}} \equiv 2^{r_{10}(37^{3001})} \equiv 2^7\ mod\ 11$$

$$\equiv 2^5 \cdot 2^2 \equiv 32 \cdot 4 \equiv (-1) \cdot 4 \equiv 7\ mod\ 11 \Longrightarrow el\ resto\ es\ r_{11}(m^E) = 7 \checkmark$$

Ejercicio 7.

Hallar todas las soluciones $n \in \mathbb{N}$ de $2^n \equiv 1 \ mod \ 23$.
¿Es cierto que la ecuación tiene una única solución módulo 22?

- $a^{p-1} \equiv 1 \ mod \ p \quad \forall (a:p) = 1, \ a \in \mathbb{Z}, \ p \ primo$

$a = 2, \ p = 23$ primo $\nmid 2$

$$\Longrightarrow 2^{p-1} = 2^{22} \equiv 1 \ mod \ 23 \Longrightarrow 2^{22k} \equiv 1 \ mod \ 23 \ \forall \ k \in \mathbb{N}$$

¡Pero este exponente no necesariamente es el más chico con esta propiedad!
¿Cómo nos aseguramos de no perder soluciones?
Podría haber $1 \leq d < 22 : \ 2^d \equiv 1 \ mod \ 23$

$$Si\ d \text{ mínimo: } 2^d \equiv 1\ mod\ 23 \Longrightarrow d|22$$

$$\Longrightarrow d \in \mathcal{D}(22) = \{1, 2, 11, 22\}$$

n	2^n	$2^n\ mod\ 23$	$2^n\ mod\ 23$	
1	2^1	2	$\equiv 2$	$mod\ 23$
2	2^2	4	$\equiv 4$	$mod\ 23$
4	2^4	$4^2 = 16$	$\equiv -7$	$mod\ 23$
6	2^6	$2^4 \cdot 2^2 \equiv (-7)4$	$\equiv -28 \equiv -5$	$mod\ 23$
8	2^8	$2^6 \cdot 2^2 \equiv (-5)4$	$\equiv -20 \equiv 3$	$mod\ 23$
11	2^{11}	$2^8 \cdot 2^3 \underbrace{\equiv 3 \cdot 8}_{\equiv 24}$	$\equiv 1$	$mod\ 23$

$$2^n \equiv 1\ mod\ 23 \Longleftrightarrow n = 11 \cdot k : \quad k \in \mathbb{N}$$

En particular, la ecuación $2^n \equiv 1\ mod\ 23$ tiene exactamente dos soluciones módulo 22, que son $n_1 = 11$ y $n_2 = 22$ ✓

Atención Teorema de Fermat

Lema: Sea $a \in \mathbb{Z}$ y $p > 0$ primo tal que $(a : p) = 1$.
1) Sea $1 \leq d \leq p - 1$ el mínimo tal que $a^d \equiv 1 \; mod \; p$

$$\implies d|(p-1)$$

2) Sea $1 \leq \tilde{d}$ tal que $a^{\tilde{d}} \equiv 1 \; mod \; p$

$$\implies d|\tilde{d}$$

Demostración 1) : Dividamos a $p - 1$ por d: escribamos

$$p - 1 = d \cdot q + r : \; 0 \leq r < d$$

$\implies$ veamos que $r = 0$

$$Fermat \implies 1 \equiv a^{p-1} \; mod \; p \equiv (a^d)^q \cdot a^r \equiv a^r \; mod \; p$$

absurdo si $r > 0$ pues d era el mínimo con la propiedad

$$a^d \equiv 1 \; mod \; p$$

Dem 2) Sea $1 \leq \tilde{d}$ tal que $a^{\tilde{d}} \equiv 1 \ mod \ p$. Queremos probar que

$$d | \tilde{d}$$

Como antes, dividamos a $\tilde{d}$ por d y veamos que $r = 0$:

$$\tilde{d} = d \cdot m + r : \ 0 \leq r < d$$

$$\Longrightarrow 1 \equiv a^{\tilde{d}} \equiv (a^d)^m \cdot a^r \ \equiv a^r \ mod \ p$$

absurdo si $r > 0$ pues $r < d$ pero d era el mínimo con la propiedad

$$a^d \equiv 1 \ mod \ p$$

$$\Longrightarrow \text{ debe ser } r = 0 \Longrightarrow d | \tilde{d}$$

Concluímos que todos los exponentes $\tilde{d}$ con la propiedad

$$a^{\tilde{d}} \equiv 1 \ mod \ p$$

son múltiplos de un mínimo d divisor de $p - 1$ ✓

Atención Teorema de Fermat

Ejercicio 8.

Hallar todas las soluciones de:
a) $5^{\ell} \equiv 1 \ mod \ 11$; b) $5^{k+3} \equiv 4^{13} \ mod \ 11$

$$a) \ Fermat: \quad 5^{10} \equiv 1 \ mod \ 11$$

$$entonces \text{ si existe } 1 \leq \ell \leq 10: \ 5^{\ell} \equiv 1 \ mod \ 11 \ \Rightarrow \ell | 10$$

$$\bullet \ 5^2 = 25 \equiv 3 \not\equiv 1 \ mod \ 11$$

$$\bullet \ 5^5 = 5^2 \cdot 5^2 \cdot 5 \equiv 3 \cdot 3 \cdot 5 \equiv 45 \equiv 1 \ mod \ 11$$

Por lo tanto, todas las soluciones son

$$Soluciones = \{\ell \equiv 0 \ mod \ 5\} = \{\ell = 5q : q \in \mathbb{Z}\}$$

b) Reescribamos la ecuación mod 11: $5^{k+3} \equiv 4^{13} \equiv \underbrace{4^{10}}_{\equiv 1 \ mod \ 11} \cdot 4^3$

$$\equiv 4^3 \equiv \underbrace{4^2}_{\equiv 5 mod \ 11} \cdot 4 \equiv 5 \cdot 4 \equiv 20 \equiv 9 \ mod \ 11$$

$$a) \implies 5^\ell \equiv 1 \ mod \ 11 \iff \ell \equiv 0 \ mod \ 5$$

$$\Rightarrow 5^{k+3} \equiv 9 \ mod \ 11 \Leftrightarrow 5^{k+4} \equiv 5 \cdot 5^{k+3} \equiv 5 \cdot 9 \equiv 1 \ mod \ 11$$

$$\Leftrightarrow \underbrace{k+4}_{=\ell} \equiv 0 \ mod \ 5 \Leftrightarrow k \equiv 1 \ mod \ 5$$

$$\implies Soluciones = \{k \in \mathbb{N} : k \equiv 1 \ mod \ 5\}$$

$$\implies Soluciones = \{k \in \mathbb{N} : k = 5 \cdot q + 1 : \ q \in \mathbb{N} \cup \{0\}\} \checkmark$$

Ejercicio 9.

a) Encontrar todos los $n \in \mathbb{N}$ tales que $372 \cdot 7^n \equiv -35 \ mod \ 37$.
b) Resolver la ecuación $39 \cdot 7^{72} \cdot X \equiv 5 \ mod \ 37$

Solución a) $\underbrace{372}_{=370+2} \cdot 7^n \equiv 2 \cdot 7^n \equiv -35 \equiv 2 \ mod \ 37$

$$\Leftrightarrow 2 \cdot 7^n \equiv 2 \ mod \ 37 \Leftrightarrow \underbrace{(-18)2}_{\equiv 1} \cdot 7^n \equiv \underbrace{(-18)2}_{\equiv 1} \ mod \ 37$$

$$\Leftrightarrow 7^n \equiv 1 \ mod \ 37$$

$p = 37$ primo positivo, $37 \nmid 7$

$$\text{Pequeño Teo Fermat} \implies 7^{36} \equiv 1 \ mod \ 37$$

$$7^n \equiv 7^{r_{36}(n)} \ mod \ 37 \implies 7^{36 \cdot k} \equiv 1 \ mod \ 37$$

Pero podría haber $1 \leq d < 36 : \ 7^d \equiv 1 \ mod \ 37$

$$Si \ 1 \leq d \leq p - 1 \text{ es el mínimo tal que } a^d \equiv 1 \ mod \ p \implies d | 36$$

Restos de 7^d mod 37 para $d|36$

n	7^n	7^n *mod 37*	7^n *mod 37*	
1	7^1	7	$\equiv 7$	*mod* 37
2	7^2	49	$\equiv 12$	*mod* 37
3	7^3	$7 \cdot 12$	$\equiv 10$	*mod* 37
4	7^4	$7 \cdot 10$	$\equiv -4$	*mod* 37
6	7^6	$7^4 \cdot 7^2 \equiv (-4) \cdot 12$	$\equiv -48 \equiv -11$	*mod* 37
9	7^9	$7^4 \cdot 7^4 \cdot 7$	$\equiv \underbrace{(-4)(-4) \cdot 7}_{37 \cdot 3 + 1} \equiv 1$	*mod* 37

Por lo tanto, el exponente más chico es 9:

$$7^n \equiv 1 \ mod\ 37 \iff n \equiv 0 \ mod\ 9$$

$$\implies Soluciones = \{n = 9 \cdot k : \quad k \in \mathbb{Z}\}$$

b) Resolver la ecuación $39 \cdot 7^{72} \cdot X \equiv 5 \; mod \; 37$:
Sabemos por Fermat: $p = 37$ primo: $(37:7) = 1$,

$$72 \equiv 0 \; mod \; 36 = p - 1 \Longrightarrow 7^{72} \equiv 1 \; mod \; p = 37$$

$$\Longrightarrow \underbrace{39 \cdot 7^{72}}_{\equiv 2 \; mod \; 37} \cdot X \equiv 2 \cdot X \equiv 5 \; mod \; 37$$

$$\Leftrightarrow 2 \cdot X \equiv 5 \; mod \; 37$$

$$\Leftrightarrow X \equiv \underbrace{(-18) \cdot 2}_{\equiv 1 \; mod \; 37} \cdot X \equiv (-18) \cdot 5 \equiv -90 \equiv 21 \; mod \; 37$$

pues $90 + 21 = 111 = 3 \cdot 37$

$$\Longrightarrow \; Soluciones = \{X = 37 \cdot q + 21 : \; q \in \mathbb{Z}\} \checkmark$$

Ejercicio 10.

Calcular el resto de dividir por 104 al entero

$$N = \sum_{n=1}^{2000} n^{60}$$

Solución: $104 = 2^3 \cdot 13$ entonces

$$r_{104}(N) \textit{ depende de los restos } r_{13}(N) \quad y \quad r_8(N)$$

Módulo 13:

• Si $13 | n \Longrightarrow n^{60} \equiv 0 \; mod \; 13$

•$Si\ 13 \nmid n,\ 60 \equiv 0 \; mod \; 12 \; (PTFermat) \Longrightarrow n^{60} \equiv n^0 \equiv 1 \; mod \; 13$

$2000 = 153 \cdot 13 + 11 \Longrightarrow$ en la suma se tienen

$$\begin{cases} \bullet \quad \#\{1 \leq n \leq 2000 : 13|n\} = \underbrace{\left[\frac{2000}{13}\right]}_{\textit{parte entera del cociente}} = 153 \\ \\ \bullet \quad \#\{1 \leq n \leq 2000 : 13 \nmid n\} = 2000 - 153 = 1847 \end{cases}$$

entonces módulo 13

$$N = \sum_{n=1}^{2000} n^{60} = \sum_{13|n} n^{60} + \sum_{13\nmid n} n^{60}$$

$$\equiv \sum_{13|n} 0 + \sum_{13\nmid n} 1$$

$$\equiv 1847 = 13 \times 142 + 1 \equiv 1 \ mod \ 13$$

Módulo 8:

- Si $2|n \Longrightarrow n = 2k : k \in \mathbb{Z} \Longrightarrow n^{60} = (2^3)^{20}k^{60} \equiv 0 \; mod \; 8$

- *Si* $2 \nmid n \Longrightarrow n \equiv 1 \vee 3 \vee 5 \vee 7 \; mod \; 8$

n	n^2	n^2	$n^2 \; mod \; 8$	$n^{60} \; mod \; 8$
1	1	1	$\equiv 1$	$\equiv 1 \quad mod \; 8$
3	3^2	9	$\equiv 1$	$\equiv 1 \quad mod \; 8$
5	5^2	25	$\equiv 1$	$\equiv 1 \quad mod \; 8$
7	7^2	49	$\equiv 1$	$\equiv 1 \quad mod \; 8$

$$\Longrightarrow n^2 \equiv 1 \; mod \; 8 \Longrightarrow n^{60} \equiv 1 \; mod \; 8$$

Módulo 8

En la suma se tienen 1000 naturales pares y 1000 impares, pues

$$\begin{cases} \bullet \quad \#\{1 \leq n \leq 2|n\} = \dfrac{2000}{2} = 1000 \\ \bullet \quad \#\{1 \leq n \leq 2000 : 2 \nmid n\} = 2000 - 1000 = 1000 \end{cases}$$

entonces módulo 8

$$N = \sum_{n=1}^{2000} n^{60} = \sum_{2|n} n^{60} + \sum_{2\nmid n} n^{60} \equiv \sum_{2|n} 0 + \sum_{2\nmid n} 1$$

$$\equiv 1000 = 250 \times 8 \equiv 0 \; mod \; 8$$

$$\Longrightarrow \begin{cases} N \equiv 1 \; mod \; 13 \\ N \equiv 0 \; mod \; 8 \end{cases}$$

N módulo 13×8: Teo Chino del Resto

$$\begin{cases} N & \equiv 1 \ mod \ 13 \\ N & \equiv 0 \ mod \ 8 \end{cases}$$

$$\Longrightarrow N = 13m + 1 \equiv 5m + 1 \equiv 0 \ mod \ 8$$

$$\Longleftrightarrow 5m \equiv -1 \ mod \ 8 \Longleftrightarrow m \equiv 25m \equiv -5 \Longleftrightarrow m \equiv 3 \ mod \ 8$$

Por lo tanto,

$$N = 13m + 1 = 13(8q + 3) + 1 = 104q + 13 \cdot 3 + 1 = 104q + 40$$

$\Longrightarrow N$ tiene resto 40 en la division por 104 ✓