CONGRUENCIAS II

Por Mai Vila y Sebastián de la Torre

ÍNDICE

¿QUÉ SIGNIFICA “SER CONGRUENTE”?

Se dice que dos números a y b son <u>congruentes módulo n</u> si sus restos al dividirlos entre n son iguales.

$$1 \div 4 = 0 \cdot 4 + \mathbf{1}$$
$$9 \div 4 = 2 \cdot 4 + \mathbf{1}$$

$(9 - 1) = 8$ y 8 es divisible entre 4

Se nota por $\equiv$

$$1 \equiv 9 \ (mod\ 4)$$

<u>¡Importante!:</u> Si un número (a) es múltiplo de otro (n), entonces $a \equiv 0 \ (mod\ n)$

OPERACIONES MODULARES

La suma:

$$a \equiv b \ (mod\ n) \Leftrightarrow a + c \equiv b + c \ (mod\ n)$$

Ejemplo:

$$3 \equiv 15 \ (mod\ 6)$$

$$3 + 2 \equiv 15 + 2 \ (mod\ 6)$$

$$5 = 0 \cdot 6 + \mathbf{5} \qquad 17 = 2 \cdot 6 + \mathbf{5}$$

OPERACIONES MODULARES

<u>El producto:</u>

$$a \equiv b \ (mod\ n) \Rightarrow a \cdot c \equiv b \cdot c \ (mod\ n)$$

Ejemplo:

$$3 \equiv 9 \ (mod\ 6)$$
$$3 \cdot 5 \equiv 9 \cdot 5 \ (mod\ 6)$$
$$15 = 2 \cdot 6 + 3 \qquad 45 = 7 \cdot 6 + 3$$

<u>Consecuencia:</u>

$$a \equiv b \ (mod\ n) \Rightarrow a^c \equiv b^c \ (mod\ n)$$

OPERACIONES MODULARES

⚠La división:

$$a \equiv b\ (mod\ n) \not\Leftrightarrow a \cdot c \equiv b \cdot c\ (mod\ n)$$

$$9 \equiv 3(mod\ 6)$$

Pero

$$\frac{9}{3} = 3 \not\equiv \frac{3}{3} = 1(mod\ 6)$$

OPERACIONES MODULARES

⚠La raíz:

$$a \equiv b \ (mod\ n) \not\Rightarrow a^c \equiv b^c \ (mod\ n)$$

Ejemplo:

$$4 \equiv 9 \ (mod\ 5)$$
$$2^2 \equiv 3^2 \ (mod\ 5)$$

Pero

$$2 \not\equiv 3 \ (mod\ 5)$$

EL PEQUEÑO TEOREMA DE FERMAT

Si p es un número primo:

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

Además, si p NO divide a a:

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

Por ejemplo:

$$4^5 = 1024 \equiv 4(mod\ 5)$$
$$5^3 = 125 = 3 \cdot 40 + 5 \equiv 5(mod\ 3)$$

PROBLEMA 1

Criterio de divisibilidad del 3:

¿Por qué un número es divisible entre tres cuando la **suma de sus cifras** es múltiplo de tres?

$$123 \Rightarrow 1 + 2 + 3 = 6$$
$$124 \Rightarrow 1 + 2 + 4 = 7$$

Pista: ¡Usa congruencias!

PROBLEMA 1

Criterio de divisibilidad del 3:

Veámoslo en congruencias:

$$a = a_n a_{n-1} \dots a_1 a_0$$

$$a = 10^n \cdot a_n + 10^{n-1} \cdot a_{n-1} + \cdots + 10 \cdot a_1 + a_0$$

$$10^n = 999 \dots 99 + 1 \equiv 1 (mod\ 3)$$

$$a = 10^n \cdot a_n + 10^{n-1} \cdot a_{n-1} + \cdots + 10 \cdot a_1 + a_0 \equiv$$
$$\equiv 1 \cdot a_n + 1 \cdot a_{n-1} \dots + 1 \cdot a_1 + 1 \cdot a_0 = a_n + a_{n-1} + \cdots + a_1 + a_0$$

PROBLEMA 2

Sea k un número Natural (0 **no** es un número Natural)

Demuestra que:

$$2^{k+1} + 2^k + 3$$

Nunca es un número **primo**

PROBLEMA 2

Veámoslo en módulo 3:

$$2^k \equiv 2 \text{ ó } 1 \ (mod\ 3)$$

$$2^{k+1} \equiv 2 \cdot 2^k \equiv 2 \cdot 2 \text{ ó } 2 \cdot 1 \equiv 1 \text{ ó } 2 \ (mod\ 3)$$

$$2^{k+1} + 2^k + 3 \equiv 1 + 2 + 3 \equiv 0 \ (mod\ 3)$$

ó

$$2^{k+1} + 2^k + 3 \equiv 2 + 1 + 3 \equiv 0 \ (mod\ 3)$$

PROBLEMA 3

¿Puede ser el siguiente número:

$$n^2 + 2018mn + 2019m + n - 2019m^2$$

un número **primo** para algunos naturales n y m?

PROBLEMA 3

Veámoslo módulo 2:

$2019 \equiv 1$ y $2018 \equiv 0\ (mod\ 2)$

$$n^2 + 2018mn + 2019m + n - 2019m^2 \equiv n^2 + 0 + m + n - m^2 \equiv$$
$$\equiv n(n+1) - m(m-1)$$

$$n(n+1) \equiv 0 \text{ y } m(m-1) \equiv 0$$

$$n(n+1) - m(m-1) \equiv 0 - 0 \equiv 0$$

PROBLEMA 4

- Determina la **última cifra** de $3^{43598} - 5$

Pista: Míralo módulo 10

PROBLEMA 4

Primero, vamos a ver que la última cifra de 3^{43598} es 9.

- $43598 \equiv 43600 - 2 \equiv -2 \equiv 2(mod\ 4)$
- Si $n \equiv 2(mod\ 4)$, la última cifra de 3^n es 9 (se puede demostrar por congruencias)

Por tanto, la última cifra de $3^{43598} - 5$ es 4

PROBLEMA 5

Sean a, b y c números **primos distintos.** Demuestra que el número:

$$(ab)^{c-1} + (bc)^{a-1} + (ca)^{b-1} - 1$$

Es múltiplo de $a \cdot b \cdot c$

Pista: Usa el pequeño teorema de Fermat

PROBLEMA 5

Si es múltiplo de a, de b y de c, lo será también de a·b·c, comprobémoslo para cada uno:

- Para a vamos a mirar la igualdad módulo a:

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

$$(ac)^{b-1} \equiv a^{b-1} \cdot c^{b-1} \equiv 0 \qquad (ab)^{c-1} \equiv a^{c-1} \cdot b^{c-1} \equiv 0$$

$$(ab)^{c-1} + (bc)^{a-1} + (ca)^{b-1} - 1 \equiv 0 + 1 + 0 - 1 \equiv 0$$

PROBLEMA 6 (Fase local 2024)

Hallar el **menor** entero positivo n tal que la suma de los n términos

$$A(n) = 1 + 11 + 111 + \cdots + 11\ldots11$$

es divisible entre **45**

$$A(1) = 1$$
$$A(2) = 1 + 11 = 12$$
$$A(3) = 1 + 11 + 111 = 123$$
$$\ldots$$

PROBLEMA 6 (Fase local 2024)

Un número es divisible entre 45 si y solo si es divisible entre 5 y entre 9. tenemos que encontrar el primer n tal que A(n) es múltiplo de 5 y de 9

- Divisibilidad entre 5: miremos A(n) módulo 5

$$A(n) \equiv (1 + 11 + 111 + \cdots + 11 \ldots 11)(mod\ 5)$$

$$A(n) \equiv \big(1 + (1 + 10) + (1 + 110) + \cdots + (1 + 11 \ldots 10)\big)(mod\ 5)$$

$$A(n) \equiv (1 + 1 + 1 + \cdots + 1)(mod\ 5)$$

$$A(n) \equiv n(mod\ 5)$$

Por tanto, n tiene que ser un múltiplo de 5

PROBLEMA 6 (Fase local 2024)

- Divisibilidad del 9: vamos a mirar A(n) módulo 9

$$A(n) \equiv (1 + 11 + 111 + \cdots + 11 \ldots 11)(mod\ 9)$$

$$A(n) \equiv \left(1 + (1 + 10) + (1 + 10 + 10^2) + \cdots + (1 + 10 + \cdots + 10^n)\right)(mod\ 9)$$

$$A(n) \equiv \left(1 + (1 + 1) + (1 + 1 + 1) + \cdots + (1 + 1 + \cdots + 1)\right)(mod\ 9)$$

$$A(n) \equiv (1 + 2 + 3 + \cdots + n)(mod\ 9)$$

$$A(n) \equiv \frac{n \cdot (n+1)}{2}\ (mod\ 9)$$

Por tanto, n tiene que ser tal que $\frac{n\cdot(n+1)}{2}$ es múltiplo de 9 $\Leftrightarrow$ n es múltiplo de 9 o n+1 es múltiplo de 9

PROBLEMA 6 (Fase local 2024)

La solución del problema es el primer n que cumple ambos criterios. Podemos hallarlo comprobando si los primeros múltiplos de 5 cumplen el criterio del 9:

- 5: ni 5 ni 6 son múltiplos de 9
- 10: ni 10 ni 11 son múltiplos de 9

…

- 30: ni 30 ni 31 son múltiplos de 9
- 35: 36 es múltiplo de 9

Solución: 35 es el primer natural n tal que A(n) es divisible entre 45