Dividir, ciclos y cifras

Congruencias II: inversos, teorema de Fermat y criterios de divisibilidad

---

En *Los restos también cuentan* viste que con las congruencias se puede sumar, restar, multiplicar y elevar a potencias, pero que **dividir es peligroso**. En esta ficha vas a ver cuándo sí se puede dividir, por qué los ciclos de las potencias acaban siempre cerrándose y de dónde salen los criterios de divisibilidad que usas desde Primaria.

1. ¿Por qué falló la división?

Recuerda el ejemplo del aviso: $6 \equiv 2 \pmod 4$, pero $3 \not\equiv 1 \pmod 4$. El problema es que el 2 por el que dividimos **comparte un factor con el módulo**. Si el número por el que divides no tiene factores comunes con el módulo, todo funciona.

Regla de simplificación

Si $a \cdot c \equiv b \cdot c \pmod n$ y $\text{mcd}(c,\ n) = 1$, entonces $a \equiv b \pmod n$.

Por ejemplo, de $4x \equiv 4 \cdot 3 \pmod 9$ se deduce $x \equiv 3 \pmod 9$, porque 4 y 9 no tienen factores comunes.

2. Inversos: la «división» de las congruencias

Con números racionales, dividir entre 3 es lo mismo que multiplicar por $\frac{1}{3}$, que es el número que multiplicado por 3 da 1. En el mundo de los restos hacemos lo mismo.

Definición

Un **inverso** de a módulo n es un entero b tal que

$$a \cdot b \equiv 1 \pmod n$$

El inverso existe **si y solo si** $\text{mcd}(a,\ n) = 1$.

Módulo 7, como 7 es primo, todos los restos distintos de 0 tienen inverso:

resto a	1	2	3	4	5	6
inverso de a	1	4	5	2	3	6

Comprueba alguno: $3 \cdot 5 = 15 = 14 + 1$, y $6 \cdot 6 = 36 = 35 + 1$. Fíjate en que $6 \equiv -1$, y $(-1)(-1) = 1$.

Módulo 6, en cambio, el 2 no tiene inverso: $2 \cdot b$ siempre es par, y un número par nunca deja resto 1 al dividirlo entre 6.

Ejemplo resuelto 1: una ecuación con congruencias

Resuelve $3x \equiv 5 \ (mod\ 7)$.

El inverso de 3 módulo 7 es 5. Multiplicamos los dos lados por 5:

$$15x \equiv 25 \ (mod\ 7) \quad \Rightarrow \quad x \equiv 4 \ (mod\ 7)$$

porque $15 \equiv 1$ y $25 \equiv 4$. Comprobación: $3 \cdot 4 = 12 \equiv 5 \ (mod\ 7)$. Las soluciones son todos los enteros de la forma $x = 7k + 4$.

Ejemplo resuelto 2: cuando no hay inverso

¿Tiene solución $4x \equiv 3 \ (mod\ 6)$? $4x$ es par y $6k + 3$ es impar, así que **no hay solución**.

¿Y $4x \equiv 2 \ (mod\ 6)$? Aquí sí: «6 divide a $4x - 2$» equivale a «3 divide a $2x - 1$», es decir, $2x \equiv 1 \ (mod\ 3)$. El inverso de 2 módulo 3 es 2, así que $x \equiv 2 \ (mod\ 3)$. Módulo 6 hay dos soluciones: $x \equiv 2$ y $x \equiv 5$.

> **Resultado clave**
>
> La ecuación $ax \equiv b \ (mod\ n)$ tiene solución **si y solo si** $d = \text{mcd}(a,\ n)$ divide a b. Si $d = 1$, la solución es única módulo n y se obtiene multiplicando por el inverso de a.

¿Y si el módulo es grande?

Para buscar el inverso de 17 módulo 43 no hace falta probar 42 números. Se usa el **algoritmo de Euclides** hacia atrás:

$$43 = 2 \cdot 17 + 9, \qquad 17 = 1 \cdot 9 + 8, \qquad 9 = 1 \cdot 8 + 1$$

Despejando los restos de abajo arriba:

$$1 = 9 - 8 = 9 - (17 - 9) = 2 \cdot 9 - 17 = 2(43 - 2 \cdot 17) - 17 = 2 \cdot 43 - 5 \cdot 17$$

Módulo 43, el término $2 \cdot 43$ desaparece y queda $-5 \cdot 17 \equiv 1$. El inverso es $-5 \equiv 38$. Comprobación: $17 \cdot 38 = 646 = 15 \cdot 43 + 1$.

3. El pequeño teorema de Fermat

En la ficha anterior viste que los restos de las potencias se repiten en ciclo. Mira ahora las potencias de 3 y de 2 módulo 7:

k	1	2	3	4	5	6
resto de 3^k	3	2	6	4	5	1
resto de 2^k	2	4	1	2	4	1

Las dos llegan a 1 en $k = 6$, que es $7 - 1$. No es casualidad.

Pequeño teorema de Fermat

Si p es primo y p no divide a a, entonces

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

En forma equivalente, $a^p \equiv a \ (mod\ p)$ para **todo** entero a.

¿Por qué es cierto? Toma $p = 7$ y $a = 3$. Multiplica por 3 los restos $1,2,3,4,5,6$: obtienes $3,6,9,12,15,18$, que módulo 7 son $3,6,2,5,1,4$. ¡Son los mismos seis restos, en otro orden! Si multiplicas todos:

$$3^6 \cdot (1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6) \equiv 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 \ (mod\ 7)$$

Y como $6!$ no tiene factores comunes con 7, la regla de simplificación de la sección 1 permite tacharlo: $3^6 \equiv 1 \ (mod\ 7)$. El mismo razonamiento funciona con cualquier primo.

El 2 llega a 1 antes, en $k = 3$. El ciclo puede ser más corto que $p - 1$, pero su longitud **siempre divide** a $p - 1$.

Ejemplo resuelto 3

¿Qué resto deja 2^{100} al dividirlo entre 13?

Por Fermat, $2^{12} \equiv 1 \ (mod\ 13)$. Como $100 = 12 \cdot 8 + 4$:

$$2^{100} = (2^{12})^8 \cdot 2^4 \equiv 1^8 \cdot 16 \equiv 3 \ (mod\ 13)$$

El resto es 3.

Ejemplo resuelto 4

Demuestra que $n^5 - n$ es múltiplo de 30 para todo entero n.

Como $30 = 2 \cdot 3 \cdot 5$, basta ver que es múltiplo de 2, de 3 y de 5:

- **Módulo 5:** por Fermat, $n^5 \equiv n$.
- **Módulo 3:** por Fermat, $n^3 \equiv n$, así que $n^5 = n^3 \cdot n^2 \equiv n \cdot n^2 = n^3 \equiv n$.
- **Módulo 2:** n^5 y n tienen la misma paridad.

Un número múltiplo de 2, de 3 y de 5 es múltiplo de 30.

Extra: Euler y las últimas cifras

Fermat solo vale para módulos primos. Para un módulo cualquiera n, Euler demostró que $a^{\varphi(n)} \equiv 1 \ (mod\ n)$ si $\text{mcd}(a,\ n) = 1$, donde $\varphi(n)$ es la cantidad de números entre 1 y n sin factores comunes con n. Por ejemplo, $\varphi(10) = 4$ (son 1, 3, 7 y 9). Eso explica por qué en la ficha anterior las potencias de 3 terminaban en un ciclo de 4 cifras.

Para las **dos últimas cifras** se trabaja módulo 100. Por ejemplo, $7^4 = 2401 \equiv 1 \ (mod\ 100)$, y como $2026 = 4 \cdot 506 + 2$, 7^{2026} acaba igual que $7^2 = 49$: en **49**.

Cuidado

Fermat exige que p sea **primo** y que p **no divida** a a. Por ejemplo, $2^3 = 8 \equiv 0 \ (mod\ 4)$, no 1: 4 no es primo.

4. De dónde salen los criterios de divisibilidad

Un número como 5 371 es $5 \cdot 10^3 + 3 \cdot 10^2 + 7 \cdot 10 + 1$. Si sustituimos el 10 por su resto, las potencias de 10 se vuelven muy sencillas.

Criterio del 9 (y del 3). Como $10 \equiv 1 \ (mod\ 9)$, todas las potencias de 10 son $\equiv 1$:

$$5371 \equiv 5 + 3 + 7 + 1 = 16 \equiv 7 \ (mod\ 9)$$

Un número y la suma de sus cifras dejan **el mismo resto** al dividirlos entre 9 (y entre 3).

Criterio del 11. Como $10 \equiv -1 \ (mod\ 11)$, las potencias de 10 valen alternativamente 1 y -1. Se suman las cifras **alternando el signo**, empezando por las unidades. Por ejemplo, para 918 082:

$$2 - 8 + 0 - 8 + 1 - 9 = -22 \equiv 0 \ (mod\ 11)$$

Así que 918 082 es múltiplo de 11 (en efecto, $918\,082 = 11 \cdot 83\,462$).

Criterio del 7, 11 y 13 a la vez. Como $1001 = 7 \cdot 11 \cdot 13$, tenemos $1000 \equiv -1$ módulo 7, 11 y 13. Se separa el número en bloques de tres cifras desde la derecha y se suman alternando el signo. Para 123 456 789:

$$789 - 456 + 123 = 456 = 7 \cdot 65 + 1$$

Así que 123 456 789 deja resto 1 al dividirlo entre 7.

Ejemplo resuelto 5

¿Puede ser un cuadrado perfecto un número cuyas cifras suman 2027?

El número deja el mismo resto que 2027 al dividirlo entre 3, y $2027 = 3 \cdot 675 + 2$. Pero un cuadrado nunca deja resto 2 módulo 3 (lo viste en la ficha anterior). **No puede ser un cuadrado.**

5. Practica

1. Halla el inverso de 5 módulo 12.
2. Resuelve $7x \equiv 3 \ (mod\ 10)$.
3. ¿Tiene solución $6x \equiv 4 \ (mod\ 9)$? ¿Y $6x \equiv 3 \ (mod\ 9)$?
4. ¿Qué resto deja 3^{2026} al dividirlo entre 7?
5. ¿En qué dos cifras termina 3^{2026}? Pista: busca la primera potencia de 3 que deja resto 1 módulo 100.
6. Demuestra que $n^7 - n$ es múltiplo de 42 para todo entero n.
7. Si reordenas las cifras de un número N y obtienes otro número M, demuestra que $N - M$ es múltiplo de 9.
8. **Reto** (IMO 1964). Halla todos los naturales n para los que $2^n - 1$ es múltiplo de 7. Demuestra que $2^n + 1$ nunca es múltiplo de 7.