Los restos también cuentan

Introducción a las congruencias (aritmética modular)

Muchos problemas de olimpiada piden demostrar que algo **no** puede ocurrir: que un número no puede ser un cuadrado, que una ecuación no tiene soluciones enteras… Probar casos nunca basta, porque los números son infinitos. La herramienta que vas a aprender aquí permite cerrar esos problemas mirando solo **los restos** de las divisiones.

1. Una idea que ya usas sin saberlo

Son las 15:00 y quedan 14 horas para un examen. ¿A qué hora será? No hace falta contar: 15 + 14 = 29, y como el reloj vuelve a empezar cada 24 horas, 29 − 24 = 5. Será a las 5:00.

Otra: hoy es domingo. ¿Qué día de la semana será dentro de 100 días? Las semanas se repiten cada 7 días y 100 = 7 · 14 + 2. Las 14 semanas completas no cambian nada; solo importan los 2 días que sobran. Será **martes**.

En ambos casos hemos hecho lo mismo: **olvidarnos de los ciclos completos y quedarnos con el resto**. Esa es toda la idea de la aritmética modular.

2. Restos y división

Al dividir un entero a entre un entero positivo n obtenemos un cociente q y un resto r:

$$a = n \cdot q + r, \quad 0 \leq r < n$$

El resto siempre es uno de los valores $0, 1, 2, \ldots, n-1$. Por ejemplo, al dividir entre 3 solo hay tres restos posibles: 0, 1 y 2. Eso significa que **todos** los enteros se reparten en tres familias: los de la forma $3k$, los de la forma $3k+1$ y los de la forma $3k+2$.

3. Congruencias: escribir «tienen el mismo resto»

> **Definición**
>
> Decimos que a es **congruente** con b módulo n, y lo escribimos
>
> $$a \equiv b \ (mod\ n)$$
>
> cuando a y b dejan el mismo resto al dividirlos entre n. Es lo mismo que decir que n divide a la diferencia $a - b$.

Ejemplos:

- $17 \equiv 2 \ (mod\ 5)$, porque los dos dejan resto 2 (y $17 - 2 = 15$ es múltiplo de 5).
- $100 \equiv 2 \ (mod\ 7)$: es el cálculo del domingo y el martes.

- $29 \equiv 5 \ (mod\ 24)$: es el cálculo del reloj.
- $-1 \equiv 7 \ (mod\ 8)$, porque $7 - (-1) = 8$.

Este último ejemplo es un truco muy útil: a veces es más cómodo usar un **resto negativo**. Por ejemplo, $3 \equiv -1 \ (mod\ 4)$ y $9 \equiv 1 \ (mod\ 8)$. Pronto verás por qué conviene.

4. Las reglas del juego

Lo que hace potentes a las congruencias es que se pueden **operar casi como igualdades**.

> **Propiedades**
>
> Si $a \equiv a' \ (mod\ n)$ y $b \equiv b' \ (mod\ n)$, entonces:
>
> - Suma y resta: $a + b \equiv a' + b' \ (mod\ n)$ y $a - b \equiv a' - b' \ (mod\ n)$
> - Producto: $a \cdot b \equiv a' \cdot b' \ (mod\ n)$
> - Potencias: $a^k \equiv a'^k \ (mod\ n)$ para cualquier natural k
>
> En la práctica: **puedes sustituir cualquier número por su resto en cualquier momento del cálculo**.

Ejemplo resuelto

¿Qué resto deja 2^{100} al dividirlo entre 3?

Calcular 2^{100} es imposible a mano, pero no hace falta. Como $2 \equiv -1 \ (mod\ 3)$, por la regla de las potencias:

$$2^{100} \equiv (-1)^{100} = 1 \ (mod\ 3)$$

El resto es 1. Fíjate en lo útil que ha sido el resto negativo.

> **Cuidado**
>
> Con las congruencias **no siempre se puede dividir**. Por ejemplo, $6 \equiv 2 \ (mod\ 4)$, pero si dividimos entre 2 obtenemos $3 \equiv 1 \ (mod\ 4)$, que es falso. Suma, resta, multiplicación y potencias: sí. División: solo con mucha precaución.

5. Las potencias se repiten

Cuando calculas los restos de las potencias de un número, tarde o temprano **se repiten en ciclo**. Mira las potencias de 3 módulo 8:

k	0	1	2	3	4	5
3^k	1	3	9	27	81	243
resto de 3^k entre 8	1	3	1	3	1	3

¿Por qué se repite con período 2? Porque $3^2 = 9 \equiv 1\ (mod\ 8)$. Cada vez que multiplicas por 3^2 estás multiplicando por 1 en el mundo de los restos. Por tanto:

$$3^k \equiv 1\ (mod\ 8) \text{ si } k \text{ es par} \qquad 3^k \equiv 3\ (mod\ 8) \text{ si } k \text{ es impar}$$

Moraleja: **cuando una potencia es congruente con 1, el ciclo se cierra**. Encontrar ese momento es la clave para manejar potencias enormes.

6. Los restos de los cuadrados

Esta es la parte más importante para los problemas del tipo «¿puede esto ser un cuadrado perfecto?».

Si $x \equiv r\ (mod\ n)$, entonces $x^2 \equiv r^2\ (mod\ n)$. Así que para saber qué restos pueden dejar los cuadrados **basta con probar los restos** $r = 0, 1, \dots, n-1$. Son finitos: una tabla y listo.

Módulo 3

resto de x	0	1	2
resto de x^2	0	1	1

Módulo 4

resto de x	0	1	2	3
resto de x^2	0	1	0	1

Módulo 8

resto de x	0	1	2	3	4	5	6	7
resto de x^2	0	1	4	1	0	1	4	1

> **Resultados clave**
>
> - Módulo 3, un cuadrado solo deja resto **0 o 1**. Nunca 2.
> - Módulo 4, un cuadrado solo deja resto **0 o 1**. Nunca 2 ni 3.
> - Módulo 8, un cuadrado solo deja resto **0, 1 o 4**. Nunca 2, 3, 5, 6 ni 7.

Comprueba tú la tabla módulo 8 y también la de módulo 5 y módulo 10. ¿Qué restos aparecen?

7. Cómo se usa: demostrar que algo es imposible

La estrategia es siempre la misma:

1. Elige un módulo n adecuado.

2. Calcula qué resto deja un lado de la igualdad.
3. Calcula qué restos puede dejar el otro lado.
4. Si no coinciden nunca, la igualdad es **imposible**.

Ejemplo resuelto 1

¿Existen enteros x, y con $x^2 + y^2 = 4003$?

Trabajamos módulo 4. Cada cuadrado deja resto 0 o 1, así que $x^2 + y^2$ deja resto 0, 1 o 2. Pero $4003 = 4 \cdot 1000 + 3$, que deja resto 3. **No existen.** Y lo hemos demostrado sin probar ni un solo caso.

Ejemplo resuelto 2

¿Puede $5^n + 2$ ser un cuadrado perfecto para algún natural n?

Módulo 4: como $5 \equiv 1 \ (mod\ 4)$, tenemos $5^n + 2 \equiv 1 + 2 = 3 \ (mod\ 4)$. Un cuadrado nunca deja resto 3. **Nunca es un cuadrado.**

¿Qué módulo elijo?

No hay una receta, pero sí pistas:

- Si buscas cuadrados, los módulos 3, 4 y 8 descartan muchos restos.
- Si aparecen potencias de un número p, elige un módulo donde p o p^2 sea congruente con 1 o -1. Así las potencias se vuelven periódicas y fáciles de manejar.
- Si un módulo no descarta nada, no te rindas: prueba otro. A veces hay que combinar dos módulos distintos para cubrir todos los casos.

8. Extra: los factores primos de un cuadrado

Otra herramienta que se combina muy bien con las congruencias. Si descompones un cuadrado perfecto en factores primos, **todos los exponentes son pares**, porque al elevar al cuadrado se duplican:

$$x = 2^3 \cdot 5 \quad \Rightarrow \quad x^2 = 2^6 \cdot 5^2$$

Consecuencia útil: si $3^a \cdot N$ es un cuadrado perfecto y N **no** es múltiplo de 3, entonces el exponente a tiene que ser par y N tiene que ser, él solo, un cuadrado perfecto. Los factores 3 no se pueden «repartir» entre las dos partes.

Para saber si N es múltiplo de 3 o no, de nuevo… ¡mira su resto módulo 3!

9. Practica

1. ¿Qué resto deja 2^{2026} al dividirlo entre 3?
2. ¿En qué cifra termina 3^{2026}? Pista: trabaja módulo 10 y busca el ciclo.
3. Demuestra que ningún cuadrado perfecto termina en 2, 3, 7 u 8.

4. ¿Existe algún entero n tal que $n^2 + 2$ sea múltiplo de 4?
5. Demuestra que un número que deja resto 7 al dividirlo entre 8 no puede escribirse como suma de tres cuadrados perfectos.
6. **Reto.** Si $x^2 + y^2 = z^2$ con x, y, z enteros, demuestra que x o y es múltiplo de 3.

Soluciones breves

1. $2 \equiv -1\ (mod\ 3)$, luego $2^{2026} \equiv (-1)^{2026} = 1$. Resto 1.
2. Las potencias de 3 terminan en 3, 9, 7, 1 y se repiten cada 4, porque $3^4 = 81 \equiv 1\ (mod\ 10)$. Como $2026 = 4 \cdot 506 + 2$, termina igual que 3^2: en **9**.
3. Módulo 10 los cuadrados solo terminan en 0, 1, 4, 5, 6 o 9 (basta probar las cifras 0 a 9).
4. No. Módulo 4, $n^2 + 2$ deja resto 2 o 3, nunca 0.
5. Módulo 8 cada cuadrado deja 0, 1 o 4. Sumando tres de esos valores se obtienen los restos 0, 1, 2, 3, 4, 5 y 6, pero nunca 7.
6. Módulo 3 los cuadrados dejan 0 o 1. Si ni x ni y fueran múltiplos de 3, los dos cuadrados dejarían resto 1, y z^2 dejaría resto 2, lo cual es imposible.