CUADERNO DE TRABAJO · IES SALMEDINA

# DESAFÍOS MATEMÁTICOS

## TOMO 2

### Aritmética modular


2.º de Bachillerato · Ciencias

Teoría y ejercicios · Cuadernillo del alumnado

Francisco José Valladares Herrera

Curso 2026–2027

# ÍNDICE GENERAL

# TOMO 2

# ARITMÉTICA MODULAR

Si la combinatoria preguntaba *cuántas posibilidades hay*, la aritmética modular pregunta algo diferente, pero igual de útil: *¿qué información permanece cuando solo nos interesa el resto?*

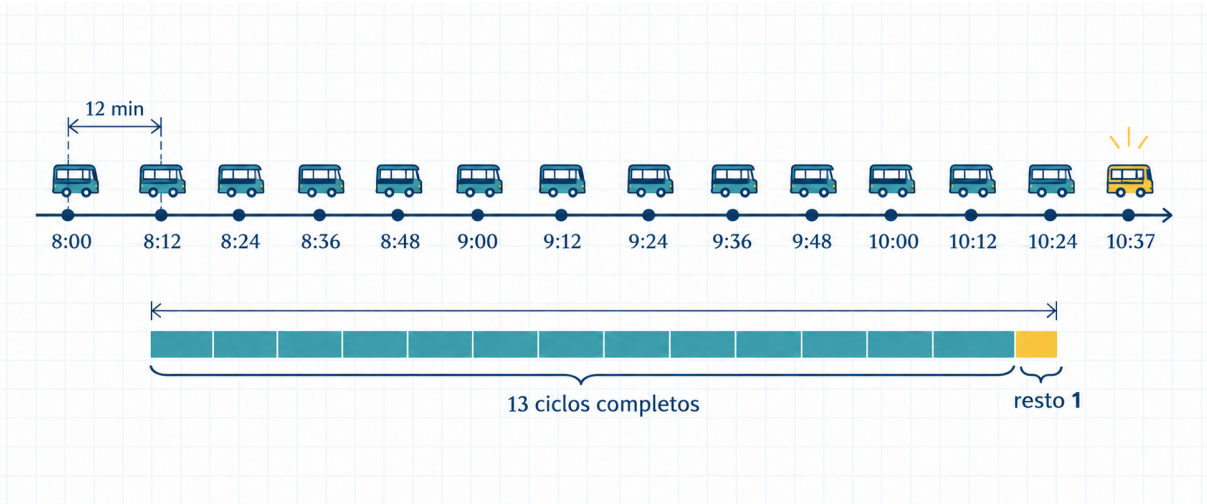
La usamos cada vez que aparece un ciclo: las horas de un reloj, los días de la semana, los turnos de un juego, las luces de un semáforo, una lista de reproducción que vuelve a empezar o un código que necesita comprobar que no se ha escrito mal.

No vamos a tirar las matemáticas por la ventana para quedarnos con el resto. Vamos a aprender a conservar exactamente la información que necesitamos y a ignorar el resto con mucho criterio. Esa es la idea central de la aritmética modular.

## 2.1. EL RESTO COMO INFORMACIÓN ÚTIL

**Problema inicial: El autobús de los doce minutos**

En la parada del instituto pasa un autobús cada 12 minutos. Si el primer autobús pasa a las 8:00, queremos saber si a las 10:37 acaba de pasar uno, está a punto de llegar o todavía falta un rato. ¿Necesitamos conocer todas las horas anteriores o basta con una pequeña parte de la información?




Lo importante no es recordar todos los autobuses que han pasado desde las ocho. Basta con

dividir el número de minutos transcurridos entre 12 y mirar el resto. Cuando el resto vuelve a ser 0, el ciclo completo vuelve a empezar.

**Definición**

Sean $a$ un entero y $n$ un entero positivo. Al dividir $a$ entre $n$, existen unos únicos enteros $q$ y $r$ tales que

$$a = qn + r, \qquad 0 \leq r < n$$

El número $q$ es el **cociente** y $r$ es el **resto de $a$ entre $n$**.

El resto siempre se elige entre 0 y $n-1$. Por eso, al trabajar *en el mundo del $n$*, donde solo habitan los números desde el 0 hasta justo el anterior del $n$, solo necesitamos $n$ restos posibles:

$$0, 1, 2, \ldots, n-1$$

El resto es precisamente la parte de la información que nos interesa.

**Ejemplo 1: Los minutos que sobran**

Al dividir 137 entre 12, obtenemos

$$137 = 11 \cdot 12 + 5$$

Por tanto, el resto es 5. Han pasado 11 ciclos completos y sobran 5 minutos.

## 2.2. Congruencia: números distintos que se comportan igual

**Problema inicial: El reloj que se ríe de los números grandes**

En un reloj de 12 horas, las 3:00, las 15:00 y las 27:00 apuntan a la misma posición. En la vida real no son la misma hora, pero para el reloj sí tienen el mismo comportamiento. ¿Cómo podemos escribir matemáticamente esta idea?

La respuesta consiste en decir que dos números son equivalentes cuando difieren en un múltiplo del módulo.

**Definición**

Sean $a$ y $b$ enteros y sea $n \geq 1$. Decimos que $a$ es **congruente con $b$ módulo $n$**, y escribimos

$$a \equiv b \pmod{n}$$

si $n$ divide a $a-b$, es decir, si existe un entero $k$ tal que

$$a - b = kn$$

La definición tiene tres formas equivalentes de leerse:

**Propiedades**

Para enteros $a$, $b$ y $n \geq 1$, son equivalentes las afirmaciones:

a) $a \equiv b \pmod{n}$

b) $n \mid (a - b)$

c) $a$ y $b$ dejan el mismo resto al dividirlos entre $n$

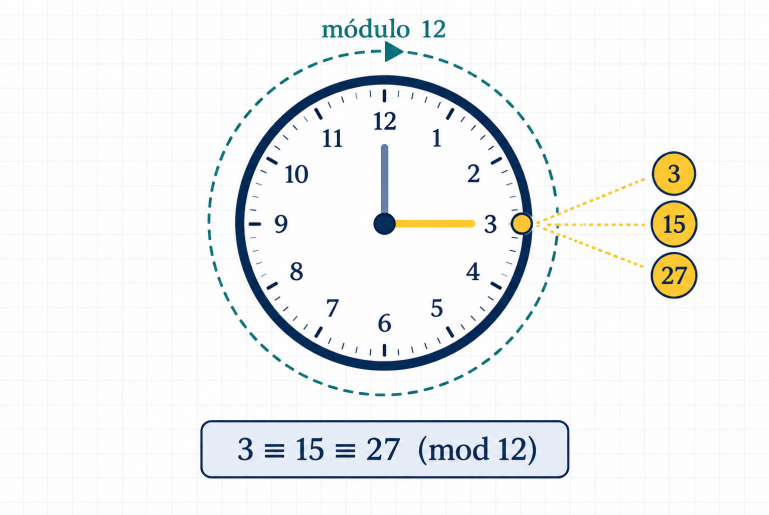
La primera forma es compacta, la segunda es útil para demostrar y la tercera suele ser la más intuitiva al empezar.

**Ejemplo 2: Horas y números con el mismo resto**

a) $29 \equiv 5 \pmod{12}$, porque $29 - 5 = 24$ es múltiplo de 12. En un reloj de doce horas, ambos números apuntan al mismo lugar.

b) $47 \equiv 2 \pmod{9}$, porque los dos dejan resto 2 al dividir entre 9.

c) $35 \not\equiv 4 \pmod{6}$, porque $35 - 4 = 31$ no es divisible por 6.




No debemos confundir $a \equiv b \pmod{n}$ con $a = b$. Por ejemplo, 17 y 5 son números distintos, pero $17 \equiv 5 \pmod{12}$. La congruencia dice que son indistinguibles cuando solo observamos los restos módulo 12.

**Proposición 1: La congruencia es una relación de equivalencia**

Para un módulo fijo $n$, la congruencia cumple:

a) **Reflexividad:** $a \equiv a \pmod{n}$

b) **Simetría:** si $a \equiv b \pmod{n}$, entonces $b \equiv a \pmod{n}$

c) **Transitividad:** si $a \equiv b \pmod{n}$ y $b \equiv c \pmod{n}$, entonces $a \equiv c \pmod{n}$.

**Demostración**

La reflexividad es inmediata porque $a - a = 0$, y 0 es múltiplo de $n$. Si $a - b = kn$, entonces $b - a = (-k)n$, de modo que la simetría también se cumple. Finalmente, si $a - b = kn$ y $b - c = \ell n$, al sumar obtenemos

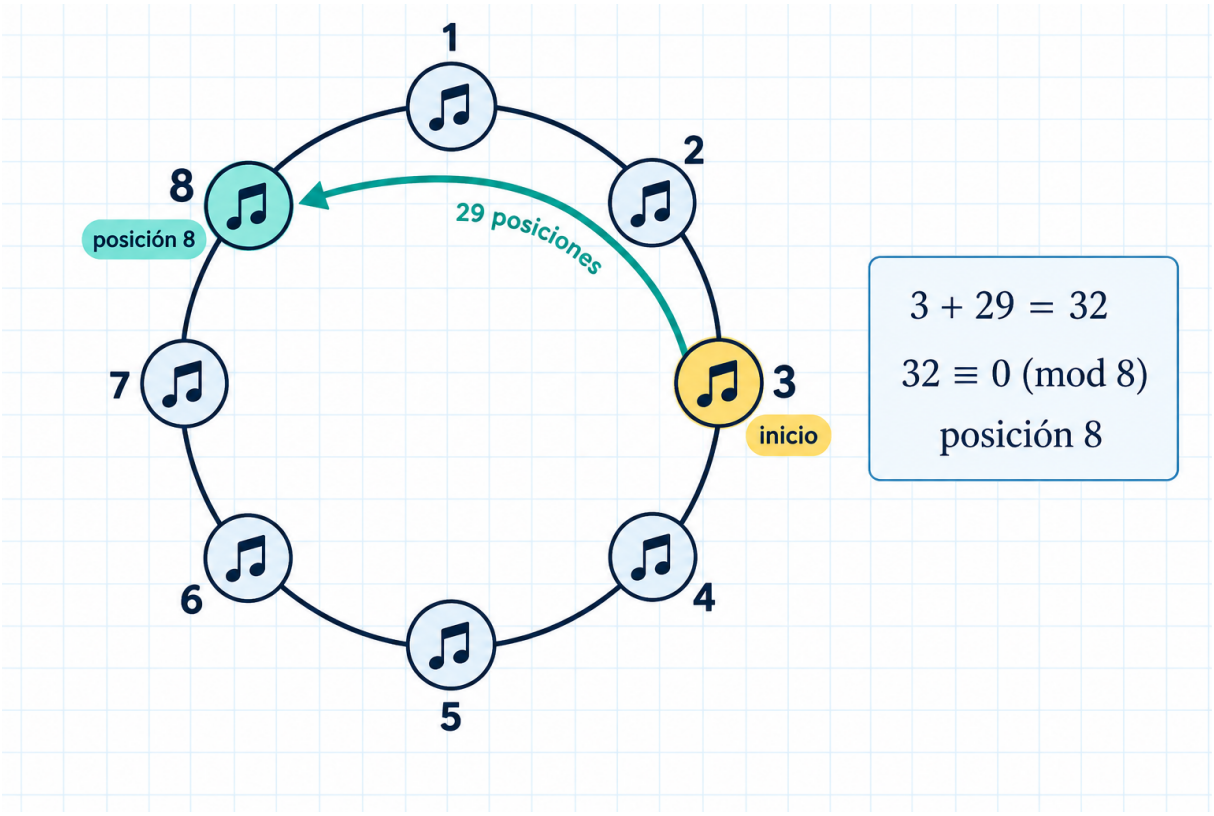
$$a - c = (a - b) + (b - c) = (k + \ell)n$$

Por tanto, $a \equiv c \pmod{n}$. La congruencia agrupa los enteros que se comportan igual respecto a un módulo.

## 2.3. Clases de restos y aritmética modular

**Problema inicial: La lista de reproducción circular**

Una lista tiene 8 canciones y, al terminar la última, vuelve a la primera. Si hoy escuchas la canción 3 y avanzas 29 posiciones, ¿en qué canción terminas? Contar una por una las vueltas sería posible, pero un poco dramático para una lista de solo ocho canciones.




Trabajar módulo 8 nos permite borrar las vueltas completas y conservar solo la posición final. La canción $3 + 29 = 32$ ocupa la posición correspondiente al resto de 32 entre 8, es decir, vuelve a la canción 8 si numeramos las posiciones desde 1.

**Definición**

El conjunto

$$\{0, 1, 2, \ldots, n - 1\}$$

se llama sistema completo de restos módulo $n$. Cada entero es congruente módulo $n$ con exactamente uno de esos restos.
La **clase de congruencia de $a$ módulo $n$** es el conjunto

$$[a]_n = \{b \in \mathbb{Z} : b \equiv a \pmod{n}\}$$

Por ejemplo, $[2]_5$ contiene todos los enteros que dejan resto 2 al dividir entre 5:

$$[2]_5 = \{\ldots, -8, -3, 2, 7, 12, 17, \ldots\}$$

En la práctica solemos trabajar con el representante 2, que es el resto no negativo más pequeño.

**Proposición 2: Suma y producto de congruencias**

Si $a \equiv b \pmod{n}$ y $c \equiv d \pmod{n}$, entonces

$$a + c \equiv b + d \pmod{n}$$

$$a - c \equiv b - d \pmod{n}$$

$$ac \equiv bd \pmod{n}$$

En consecuencia, podemos sustituir un número por otro congruente antes de sumar, restar o multiplicar.

**Demostración**

Como $a - b$ y $c - d$ son múltiplos de $n$, también lo es

$$(a + c) - (b + d) = (a - b) + (c - d)$$

La resta se obtiene de la misma manera. Para el producto,

$$ac - bd = a(c - d) + d(a - b)$$

Cada sumando es múltiplo de $n$, así que $ac - bd$ también lo es.

**Propiedades**

Las reglas anteriores permiten reducir los números antes de operar:

$$(a + b) \bmod n = ((a \bmod n) + (b \bmod n)) \bmod n$$

$$(ab) \bmod n = ((a \bmod n)(b \bmod n)) \bmod n$$

Para sumas y productos, reducir pronto evita trabajar con números enormes. La división requiere más cuidado: no siempre se puede «dividir» una congruencia por cualquier número.

**Ejemplo 3: Reducir antes de calcular**

a) Para calcular $238+417 \pmod{10}$, basta observar

$$238 \equiv 8 \pmod{10}, \qquad 417 \equiv 7 \pmod{10}$$

Por tanto, el resto es 5.

b) Para calcular $37 \cdot 54 \pmod{7}$, sustituimos 37 por 2 y 54 por 5. Como $2 \cdot 5 = 10 \equiv 3 \pmod{7}$, el resto buscado es 3.

c) Si $a \equiv 4 \pmod{9}$, entonces

$$a^2 \equiv 4^2 \equiv 7 \pmod{9}$$

Podemos elevar una congruencia a una potencia entera no negativa.

## 2.4. Divisibilidad, restos y criterios rápidos

**Problema inicial: ¿Es divisible o solo parece importante?**

En una tarjeta de embarque aparece el número 7 482 315. Queremos comprobar rápidamente si es divisible por 3 o por 9, sin hacer una división larga que nos quite las ganas de viajar. ¿Podemos usar sus cifras?

La respuesta se basa en congruencias muy sencillas. Como $10 \equiv 1 \pmod{9}$, las potencias de 10 también son congruentes con 1 módulo 9. Por eso, al escribir un número en base diez, su resto módulo 9 coincide con el resto de la suma de sus cifras.

**Proposición 3: Criterios de divisibilidad por 3 y por 9**

Un número entero es divisible por 3 si y solo si la suma de sus cifras es divisible por 3. Es divisible por 9 si y solo si la suma de sus cifras es divisible por 9.

**Demostración**

Si $N = a_0 + 10a_1 + 10^2 a_2 + \cdots + 10^k a_k$ es la expresión decimal de $N$, como $10 \equiv 1 \pmod{9}$, tenemos

$$N \equiv a_0 + a_1 + \cdots + a_k \pmod{9}$$

Por tanto, $N$ y la suma de sus cifras dejan el mismo resto módulo 9, y también el mismo resto módulo 3. El criterio para 9 es inmediato; para 3, basta observar si esa suma de cifras es múltiplo de 3.

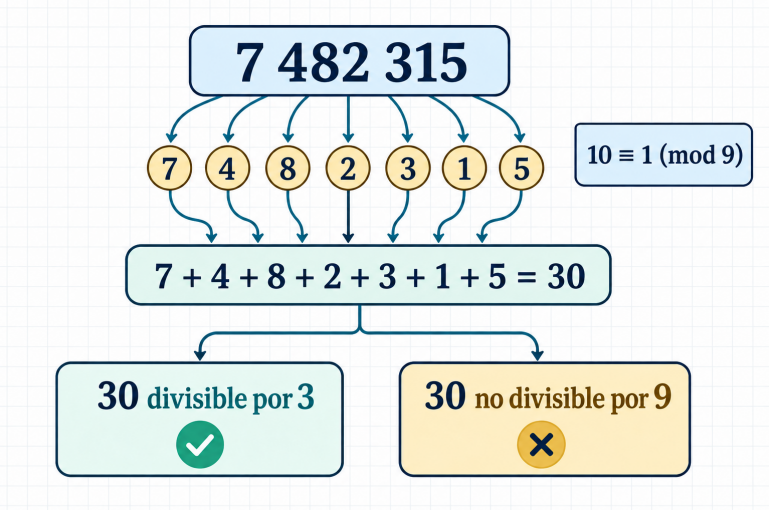
**Ejemplo 4: La tarjeta de embarque**

La suma de las cifras de 7 482 315 es

$$7+4+8+2+3+1+5 = 30$$

Como 30 es divisible por 3, el número también es divisible por 3. Como 30 no es divi-

sible por 9, el número no es divisible por 9.




El mismo lenguaje permite construir otros criterios. Por ejemplo, $10 \equiv -1 \pmod{11}$, así que las potencias de 10 alternan entre 1 y $-1$ módulo 11. De ahí sale el criterio de la suma alternada de cifras.

**Ejemplo 5: Un criterio con ritmo alterno**

Para $N = 4873$, calculamos la suma alternada

$$3 - 7 + 8 - 4 = 0$$

Como 0 es múltiplo de 11, 4873 es divisible por 11. La alternancia no es un capricho del profesor: aparece porque $10 \equiv -1 \pmod{11}$.

## 2.5. Inversos y congruencias lineales

**Problema inicial: El candado de la jornada**

Un candado digital transforma una posición $x$ mediante la regla $7x$ y solo conserva el resto módulo 12. Si queremos obtener el código 5, debemos resolver

$$7x \equiv 5 \pmod{12}$$

¿Cómo deshacemos la multiplicación sin cometer el clásico error de «dividir porque sí»?

Para deshacer una multiplicación módulo $n$, necesitamos un número que multiplicado por $a$ dé resto 1. Ese número es el inverso modular.

**Definición**

Decimos que $u$ es un **inverso de $a$ módulo $n$** si

$$au \equiv 1 \pmod{n}$$

En ese caso escribimos $u \equiv a^{-1} \pmod{n}$. El inverso existe si y solo si $a$ y $n$ son coprimos, es decir,

$$\mathrm{mcd}(a, n) = 1$$

**Proposición 4: Cómo encontrar un inverso modular**

Si $\mathrm{mcd}(a, n) = 1$, el algoritmo de Euclides permite encontrar enteros $u$ y $v$ tales que

$$au + nv = 1$$

Al reducir módulo $n$, obtenemos $au \equiv 1 \pmod{n}$. Por tanto, $u$ es un inverso de $a$ módulo $n$.

**Demostración**

El algoritmo de Euclides no solo calcula el máximo común divisor: también permite escribirlo como combinación lineal de $a$ y $n$. Si el máximo común divisor es 1, existen $u$ y $v$ con $au + nv = 1$. Al pasar a congruencias módulo $n$, el término $nv$ desaparece y queda $au \equiv 1 \pmod{n}$.

Recíprocamente, si $au \equiv 1 \pmod{n}$, entonces $au - 1$ es múltiplo de $n$. Cualquier divisor común de $a$ y $n$ debe dividir también a 1, así que el máximo común divisor solo puede ser 1.

**Ejemplo 6: Abrir el candado sin dividir a ciegas**

Queremos resolver $7x \equiv 5 \pmod{12}$. Como

$$7 \cdot 7 = 49 \equiv 1 \pmod{12}$$

7 es su propio inverso módulo 12. Multiplicamos ambos lados por 7:

$$x \equiv 7 \cdot 5 \equiv 35 \equiv 11 \pmod{12}$$

Las soluciones son todos los enteros congruentes con 11 módulo 12.


Los restos 7 y 7 son inversos multiplicativos módulo 12.

$$7x \equiv 5 \pmod{12}$$

$$7 \cdot 7 = 49 \equiv 1 \pmod{12}$$

Multiplica ambos lados por 7 (módulo 12).

$$\begin{aligned} 7 \cdot (7x) &\equiv 7 \cdot 5 \pmod{12} \\ (7 \cdot 7)x &\equiv 35 \pmod{12} \\ 1 \cdot x &\equiv 35 \pmod{12} \\ x &\equiv 35 \pmod{12} \\ x &\equiv 11 \pmod{12} \end{aligned}$$

$$x \equiv 11 \pmod{12}$$

**Teorema 1: Congruencias lineales**

Sea $ax \equiv b \pmod{n}$ y sea $d = \gcd(a, n)$. Entonces:

a) La congruencia tiene solución si y solo si $d \mid b$

b) Si tiene solución, posee exactamente $d$ soluciones módulo $n$

c) Si $d = 1$, existe una única solución módulo $n$, que se encuentra usando el inverso de $a$.

**Demostración**

Si $ax \equiv b \pmod{n}$, existe un entero $k$ tal que $ax - b = kn$. Todo divisor común de $a$ y $n$ divide entonces a $b$, así que $d \mid b$ es necesario. Si $d \mid b$, dividimos la congruencia por $d$ y obtenemos una congruencia equivalente

$$\frac{a}{d}x \equiv \frac{b}{d} \pmod{\frac{n}{d}}$$

Ahora el coeficiente $a/d$ es coprimo con $n/d$, por lo que tiene inverso. Hay una única solución módulo $n/d$, que produce $d$ soluciones distintas al volver a trabajar módulo $n$.

**Ejemplo 7: Cuando aparecen varias soluciones**

Resolvamos $6x \equiv 9 \pmod{15}$. Como

$$\gcd(6, 15) = 3$$

y $3 \mid 9$, hay solución. Dividimos por 3:

$$2x \equiv 3 \pmod{5}$$

El inverso de 2 módulo 5 es 3, así que $x \equiv 9 \equiv 4 \pmod{5}$. Al expresarlo módulo 15,

obtenemos

$$x \equiv 4,\ 9,\ 14 \pmod{15}$$

Hay tres soluciones porque el máximo común divisor inicial era 3.

## 2.6. Potencias, ciclos y el pequeño teorema de Fermat

**Problema inicial: La última cifra de una potencia monstruosa**

Una calculadora recibe $7^{2025}$, pero decide que no quiere trabajar tanto y nos pregunta solo por la última cifra. ¿Tenemos que escribir 7 dos mil veinticinco veces o podemos detectar un ciclo?

Las potencias módulo $n$ suelen repetir sus restos. Cuando encontramos ese periodo, podemos sustituir un exponente enorme por otro mucho más pequeño.

**Propiedades**

Si $a \equiv b \pmod{n}$, entonces para todo entero $k \geq 0$,

$$a^k \equiv b^k \pmod{n}$$

Además, si $\mcd(a, n) = 1$, las potencias de $a$ módulo $n$ terminan repitiéndose. El primer exponente positivo $t$ para el que

$$a^t \equiv 1 \pmod{n}$$

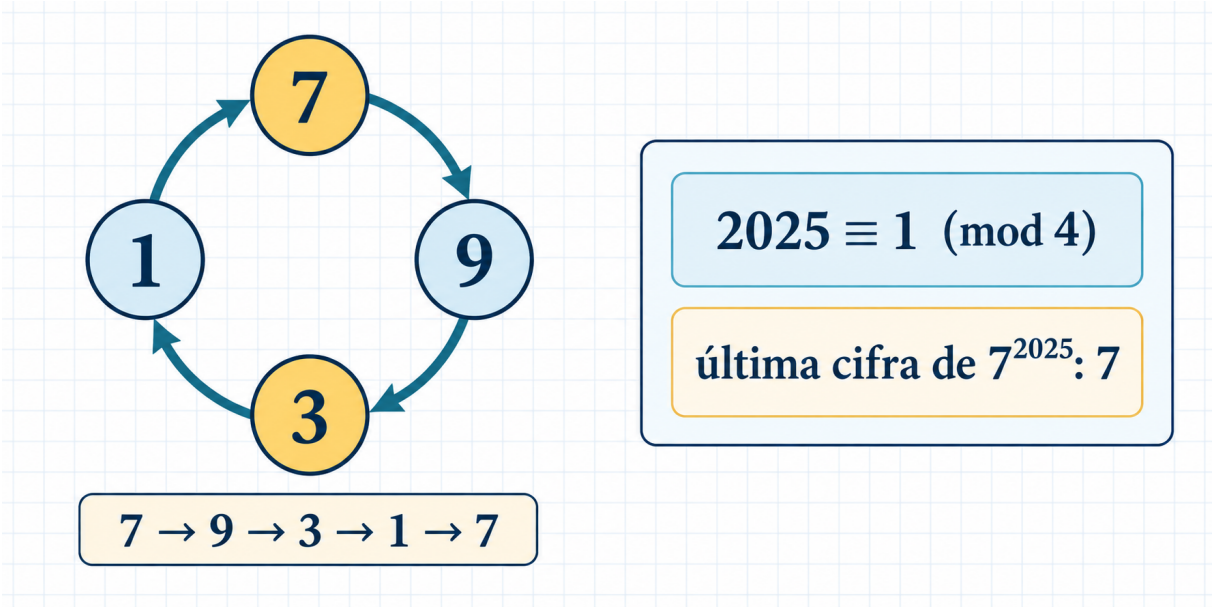
se llama **orden de $a$ módulo $n$**.

**Ejemplo 8: El ciclo de la última cifra**

Las últimas cifras de las potencias de 7 son

$$7,\ 9,\ 3,\ 1,\ 7,\ 9,\ 3,\ 1, \ldots$$

El periodo es 4. Como $2025 \equiv 1 \pmod{4}$, la última cifra de $7^{2025}$ es la primera del ciclo: 7.




Para justificar muchos ciclos basta con el siguiente resultado.

**Teorema 2: Pequeño teorema de Fermat**

Si $p$ es primo y $p \nmid a$, entonces

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

De forma equivalente,

$$a^p \equiv a \pmod{p}$$

para cualquier entero $a$.

**Demostración**

Consideremos los $p-1$ restos no nulos

$$1, 2, \ldots, p-1$$

Al multiplicarlos por $a$, como $a$ no es divisible por $p$, no aparece ningún resto 0, y tampoco se repite ningún resto: si $ar \equiv as \pmod{p}$, podemos cancelar $a$ porque tiene inverso módulo $p$, y obtenemos $r \equiv s \pmod{p}$. Por tanto, los productos $a, 2a, \ldots, (p-1)a$ son los mismos restos que $1, 2, \ldots, p-1$, aunque estén reordenados. Al multiplicarlos todos,

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

Como $p$ no divide a ninguno de los factores de $(p-1)!$, ese producto tiene inverso módulo $p$ y podemos cancelarlo. Queda $a^{p-1} \equiv 1 \pmod{p}$.

**Ejemplo 9: Una potencia con exponente enorme**

Para calcular $2^{100} \pmod{7}$, aplicamos Fermat:

$$2^6 \equiv 1 \pmod{7}$$

Como $100 = 16 \cdot 6 + 4$, basta conservar el exponente 4:

$$2^{100} \equiv 2^4 \equiv 16 \equiv 2 \pmod 7$$

La potencia parecía gigantesca; el módulo la convirtió en una pequeña cuenta.

## 2.7. Varios relojes a la vez: el teorema chino del resto

**Problema inicial: Dos alarmas con ritmos distintos**

Una alarma suena cada 3 horas y, según su horario, lo hará a las 2:00. Otra suena cada 5 horas y lo hará a las 3:00. Si observamos una hora $x$ que cumple

$$x \equiv 2 \pmod 3, \qquad x \equiv 3 \pmod 5$$

¿podemos encontrar una única respuesta dentro de un ciclo común?

Este tipo de problema combina varias condiciones modulares. Cuando los módulos son coprimos, las condiciones encajan con precisión y determinan una única clase de restos módulo el producto.

**Teorema 3: Teorema chino del resto, caso coprimo**

Sean $m$ y $n$ enteros positivos coprimos. Para cualesquiera enteros $a$ y $b$, el sistema

$$x \equiv a \pmod m, \qquad x \equiv b \pmod n$$

tiene una solución. Además, todas las soluciones son congruentes módulo $mn$.

**Demostración**

Como $m$ y $n$ son coprimos, $m$ tiene un inverso módulo $n$. Escribimos $x = a + mk$ y sustituimos en la segunda condición:

$$a + mk \equiv b \pmod n$$

Esto se convierte en una congruencia lineal para $k$, cuyo coeficiente $m$ tiene inverso módulo $n$. Por tanto, existe una única clase de soluciones para $k$ módulo $n$, y las soluciones para $x$ quedan determinadas módulo $mn$.

**Ejemplo 10: Las dos alarmas**

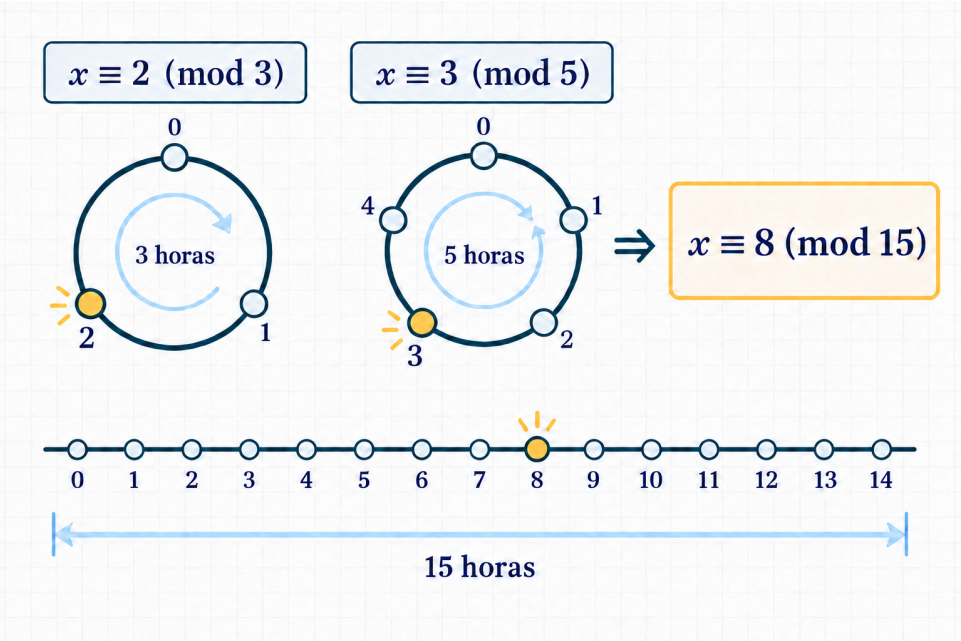
Resolvamos

$$x \equiv 2 \pmod 3, \qquad x \equiv 3 \pmod 5$$

Los números congruentes con 2 módulo 3 son $2, 5, 8, 11, \ldots$. De ellos, 8 es congruente con 3 módulo 5. Por tanto,

$$x \equiv 8 \pmod{15}$$

La siguiente coincidencia aparece cada 15 horas.




Si los módulos no son coprimos, no siempre hay solución. La condición correcta es que las dos congruencias sean compatibles con el máximo común divisor de los módulos.

**Proposición 5: Compatibilidad de dos congruencias**

El sistema

$$x \equiv a \pmod m, \qquad x \equiv b \pmod n$$

tiene solución si y solo si

$$\mathrm{mcd}(m,n) \mid (b-a)$$

Cuando existe, la solución es única módulo $\mathrm{mcm}(m,n)$.

**Ejemplo 11: Cuando los ciclos no encajan**

Consideremos

$$x \equiv 1 \pmod 4, \qquad x \equiv 2 \pmod 6$$

Como $\mathrm{mcd}(4,6) = 2$ y $2 \mid (2-1)$ es falso, no existe ningún entero que cumpla las dos condiciones. Los dos ciclos se cruzan cerca, pero no llegan a coincidir. La aritmética modular también sabe decir «no hay solución».

## 2.8. Un mapa para resolver problemas modulares

**Propiedades**

Cuando aparezca un problema de aritmética modular, sigue este orden:

1. Identifica el ciclo: reloj, días, posiciones, cifras o turnos
2. Elige el módulo adecuado
3. Sustituye los números por restos más pequeños

4. Para potencias, busca un ciclo o aplica Fermat cuando proceda
5. Para $ax \equiv b \pmod{n}$, calcula primero $\mcd(a, n)$ y decide si existe solución
6. Si hay varias condiciones, comprueba si los módulos son coprimos y usa el teorema chino del resto cuando sea posible

La pregunta que evita la mayoría de los errores es: *¿qué significa exactamente que dos resultados sean iguales en este problema?*

La aritmética modular no consiste en hacer desaparecer números porque sí. Consiste en elegir una escala adecuada para el fenómeno que estamos estudiando: 12 para un reloj, 7 para los días de la semana, 10 para la última cifra, 9 para la suma de cifras o el producto de varios módulos cuando combinamos ciclos.

En los ejercicios de esta sección practicaremos primero con restos y congruencias, después con inversos y potencias, y finalmente con problemas en los que varios ciclos se cruzan. La meta no será sobrevivir a una colección de trucos, sino aprender a reconocer la estructura que hay detrás de cada problema.

# EJERCICIOS

**Trabajo individual.** En esta colección empezamos observando restos y ciclos sencillos y terminamos combinando varias congruencias. Antes de operar, escribe siempre qué módulo describe mejor la situación: un reloj, una cifra final, un ciclo de publicaciones o varios ritmos a la vez. Si el número parece enorme, probablemente el módulo tenga algo interesante que contarnos.
**Tiempo orientativo:** dos sesiones de 50 minutos.

### Ejercicio 1 — Restos con sentido

Calcula los restos y decide las congruencias siguientes:

a) El resto de 157 al dividir entre 12

b) El resto de $-23$ al dividir entre 7

c) Decide si $86 \equiv 2 \pmod 7$ y si $86 \equiv 2 \pmod 9$

Escribe en cada caso una igualdad de la forma $a = qn + r$, con $0 \le r < n$.

### Ejercicio 2 — Reloj y calendario

Responde usando congruencias, sin enumerar todas las horas o todos los días:

a) Si ahora son las 22:00, ¿qué hora será dentro de 37 horas?

b) Si hoy es jueves, ¿qué día de la semana será dentro de 100 días?

c) Un reloj de 24 horas marca las 11:00. ¿Qué otras horas de la forma $11 + 24k$ representan la misma posición?

### Ejercicio 3 — Reducir antes de hacer cuentas

Calcula los restos sin multiplicar ni sumar los números completos:

a) $(238 + 417) \bmod 10$

b) $(37 \cdot 54) \bmod 7$

c) $2^{10} \bmod 7$

En el apartado c), busca primero un ciclo corto de potencias de 2 módulo 7.

**Ejercicio 4 — Una matrícula que quiere ser divisible**

Considera el número $N = 6\,172\,839$.

a) Decide si $N$ es divisible por 3

b) Decide si $N$ es divisible por 9

c) Usa la suma alternada de cifras para decidir si $N$ es divisible por 11

Justifica cada respuesta con el criterio de divisibilidad adecuado.

**Ejercicio 5 — Abrir una cerradura modular**

Resuelve y razona:

a) Encuentra el inverso de 5 módulo 12

b) Resuelve $5x \equiv 7 \pmod{12}$

c) Explica por qué 6 no tiene inverso módulo 15.

**Ejercicio 6 — Cuando aparecen varias soluciones**

Resuelve las dos congruencias y escribe todas las soluciones módulo el módulo indicado:

a) $14x \equiv 8 \pmod{20}$

b) $9x \equiv 6 \pmod{15}$

c) En cada caso, indica cuántas soluciones distintas aparecen en un sistema completo de restos.

**Ejercicio 7 — La calculadora perezosa**

Trabaja con ciclos de últimas cifras:

a) Determina la última cifra de $7^{2025}$

b) Determina la última cifra de $3^{2026}$

c) Determina la última cifra de $7^{2025} + 3^{2026}$.

**Ejercicio 8 — Dos relojes que se ponen de acuerdo**

Encuentra todas las horas $x$ que cumplen

$$x \equiv 1 \pmod{4}, \qquad x \equiv 4 \pmod{7}$$

Escribe la menor solución no negativa y las dos siguientes. Indica también el periodo con el que se repiten.

**Ejercicio 9 — Ciclos que comparten piezas**

Resuelve el sistema

$$x \equiv 2 \pmod 6, \qquad x \equiv 5 \pmod 9$$

Antes de buscar la solución, comprueba si las dos condiciones son compatibles. Después escribe la solución general y la menor solución no negativa.

**Ejercicio 10 — La misión de las acreditaciones**

Una acreditación válida debe cumplir simultáneamente

$$x \equiv 4 \pmod 7, \qquad x \equiv 6 \pmod 9, \qquad x \equiv 2 \pmod 5$$

Encuentra la menor solución no negativa y todas las soluciones entre 0 y 999. Explica qué periodo común estás utilizando.

# BIBLIOGRAFÍA Y WEBGRAFÍA

**Material docente de partida**

[1] VALLADARES HERRERA, F. J. (2026). *Desafíos matemáticos. Cuadernillo completo*. IES Salmedina. Apuntes docentes para 2.º de Bachillerato de ciencias; apartado «Aritmética modular» del capítulo «Introducción a la matemática discreta». Versión de septiembre de 2026, utilizada como material de partida de este tomo.