FECYT
FUNDACIÓN ESPAÑOLA PARA LA CIENCIA Y LA TECNOLOGÍA
UCC+i
RED DE UNIDADES DE CULTURA CIENTÍFICA Y DE LA INNOVACIÓN
GOBIERNO DE ESPAÑA
MINISTERIO DE EDUCACIÓN, CULTURA Y DEPORTE

**Preparación de Olimpiadas**

*(Introducción a las congruencias)*

---

# 1. Conceptos básicos

**Definición 1.1** (Congruencia)**.** Sean $a, b \in \mathbb{Z}$ y $n \in \mathbb{Z}_+$. Decimos que $a$ es *congruente* con $b$ módulo $n$ y escribimos

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

si $n$ divide a $a-b$, es decir, $n \mid (a-b)$.

*Ejemplo* 1.1. Vamos a entender qué significa una congruencia con ejemplos muy sencillos.

I. Si dividimos 17 entre 5, el cociente es 3 y el resto es 2. Eso quiere decir que 17 y 2 dejan el mismo resto al dividirlos por 5. Por tanto, escribimos:
$$17 \equiv 2 \pmod{5}.$$

II. Si dividimos 12 entre 4, el resto es 0. También el 8 entre 4 deja resto 0. Como los dos tienen el mismo resto al dividir por 4, decimos:
$$12 \equiv 0 \pmod{4}.$$
$$8 \equiv 0 \pmod{4}.$$
(De hecho, cualquier número múltiplo de 4 será congruente con 0 módulo 4.)

III. 10 y 3 dejan el mismo resto al dividir por 7 porque $10-3=7$ es múltiplo de 7. Así que:
$$10 \equiv 3 \pmod{7}.$$

IV. A veces se usa un número negativo: por ejemplo, $14 \equiv -1 \pmod{5}$, ya que $14-(-1)=15$ es múltiplo de 5. (Esto también se puede decir como 14 y $-1$ dejan el mismo resto al dividir entre 5.)

**Idea clave:** dos números son congruentes módulo $n$ si al dividirlos entre $n$ dejan el mismo resto. También se puede pensar que su diferencia es un múltiplo de $n$.

## 2. Operaciones y propiedades

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

$$\begin{aligned} a+c &\equiv b+d \pmod{n}, \\ a-c &\equiv b-d \pmod{n}, \\ ac &\equiv bd \pmod{n}. \end{aligned}$$

Sin embargo, la división no siempre está permitida: de $ac \equiv bc \pmod{n}$ no se puede concluir en general que $a \equiv b \pmod{n}$ a menos que $mcd(c,n) = 1$ (ver más abajo sobre inversos).

*Ejemplo* 2.1. Veamos ahora cómo se pueden hacer sumas, restas y multiplicaciones con congruencias. La idea es que, si los números tienen el mismo resto al dividir por $n$, entonces al sumarlos, restarlos o multiplicarlos, el resultado también tendrá el mismo resto.

I. **Suma:** Sabemos que $7 \equiv 2 \pmod{5}$ y que $4 \equiv 4 \pmod{5}$. Si los sumamos, $7+4 = 11$ y $2+4 = 6$. Como 11 y 6 dejan el mismo resto (1) al dividir por 5, se cumple:

$$7+4 \equiv 2+4 \pmod{5}.$$

Es decir, $11 \equiv 1 \pmod{5}$.

II. **Resta:** Si $12 \equiv 2 \pmod{5}$ y $7 \equiv 2 \pmod{5}$, entonces al restar también se mantiene la congruencia:

$$12-7 \equiv 2-2 \pmod{5}.$$

O sea, $5 \equiv 0 \pmod{5}$ .

III. **Multiplicación:** Si $8 \equiv 3 \pmod 5$, al multiplicar por 4 se cumple:

$$4 \cdot 8 \equiv 4 \cdot 3 \pmod 5.$$

En efecto, $32 \equiv 12 \pmod 5$ y ambos dejan resto 2 al dividir por 5.

IV. **Combinando operaciones:** Si $6 \equiv 1 \pmod 5$ y $9 \equiv 4 \pmod 5$, entonces:

$$6 + 9 \equiv 1 + 4 \pmod 5,$$

así que $15 \equiv 5 \pmod 5$, y efectivamente ambos son múltiplos de 5.

V. **Cuidado con dividir:** No siempre se puede "dividir" en una congruencia. Por ejemplo, de $2x \equiv 4 \pmod 6$ no podemos dividir por 2 directamente, porque 2 y 6 tienen un divisor común (2). En estos casos hay que comprobar primero si la ecuación tiene solución (usando el máximo común divisor).

**Idea clave:** podemos sumar, restar y multiplicar dentro de una congruencia igual que con números normales, pero no siempre podemos dividir.

## 2.1. Inverso multiplicativo módulo $n$

Si $mcd(a,n) = 1$, existe un entero $x$ tal que

$$ax \equiv 1 \pmod n.$$

Dicho $x$ es el inverso multiplicativo de $a$ módulo $n$, denotado $a^{-1} \pmod n$. El método habitual para encontrarlo es el algoritmo extendido de Euclides.

*Ejemplo* 2.2. Queremos encontrar el inverso multiplicativo de 7 módulo 26, es decir, un entero $x$ tal que

$$7x \equiv 1 \pmod{26}.$$

**Paso 1: Comprobación de existencia**.

Existe inverso si y sólo si $mcd(7,26) = 1$.

$$26 = 3 \cdot 7 + 5, \quad 7 = 1 \cdot 5 + 2, \quad 5 = 2 \cdot 2 + 1, \quad 2 = 2 \cdot 1 + 0.$$

Como el último resto no nulo es 1, tenemos $mcd(7,26) = 1$, así que el inverso existe.

**Paso 2: Algoritmo extendido de Euclides**.

Retrocedemos para expresar 1 como combinación lineal de 7 y 26:

$$\begin{aligned} 5 &= 26 - 3 \cdot 7, \\ 2 &= 7 - 1 \cdot 5 = 7 - (26 - 3 \cdot 7) = 4 \cdot 7 - 26, \\ 1 &= 5 - 2 \cdot 2 = (26 - 3 \cdot 7) - 2(4 \cdot 7 - 26) = 3 \cdot 26 - 11 \cdot 7. \end{aligned}$$

De donde se deduce que

$$-11 \cdot 7 \equiv 1 \pmod{26}.$$

**Paso 3: Ajuste del inverso positivo**.

$-11 \equiv 15 \pmod{26}$ (porque $26 - 11 = 15$). Por tanto,

$$\boxed{7^{-1} \equiv 15 \pmod{26}}.$$

**Verificación**.

$$7 \cdot 15 = 105 \equiv 105 - 4 \cdot 26 = 105 - 104 = 1 \pmod{26}.$$

Así se verifica que el resultado es correcto.

## 2.2. Uso de las congruencias para determinar si un número es múltiplo de otro

**Idea principal.**

Decimos que un número $a$ es **múltiplo** de otro número $b$ si existe un número entero $k$ tal que:

$$a = b\,k.$$

En términos de **congruencias**, esto se expresa como:

$$a \equiv 0 \pmod{b}.$$

Es decir, $a$ es congruente con 0 módulo $b$ si y sólo si $a$ es múltiplo de $b$.

**Cómo usarlo.**

Si tenemos dos números $a$ y $b$:

I. Calculamos el resto de dividir $a$ entre $b$.

II. Si el resto es cero, entonces $a \equiv 0 \pmod{b}$, y por tanto $a$ es múltiplo de $b$.

**Ejemplos directos.**

- **¿Es 42 múltiplo de 7?**

$$42 = 7 \cdot 6 + 0 \Rightarrow 42 \equiv 0 \pmod{7}.$$

Sí, 42 es múltiplo de 7.

- **¿Es 45 múltiplo de 9?**

$$45 = 9 \cdot 5 + 0 \Rightarrow 45 \equiv 0 \pmod{9}.$$

Sí, 45 es múltiplo de 9.

- **¿Es 37 múltiplo de 4?**

$$37 = 4 \cdot 9 + 1 \Rightarrow 37 \equiv 1 \pmod 4.$$

No, porque el resto no es cero.

**Aplicación: criterios de divisibilidad con congruencias.**
El uso de congruencias permite demostrar de forma elegante los criterios de divisibilidad clásicos:

- **Divisibilidad por 3:**

$$10 \equiv 1 \pmod 3.$$

Por tanto, si un número $n = a_k 10^k + a_{k-1} 10^{k-1} + \cdots + a_0$, entonces:

$$n \equiv a_k + a_{k-1} + \cdots + a_0 \pmod 3.$$

Es decir, un número es divisible por 3 si la suma de sus cifras también lo es.

- **Divisibilidad por 11:**

$$10 \equiv -1 \pmod{11}.$$

Entonces:

$$n \equiv a_0 - a_1 + a_2 - a_3 + \cdots \pmod{11}.$$

Por tanto, un número es divisible por 11 si la diferencia entre la suma de las cifras en posiciones pares e impares es múltiplo de 11.

## Resumen

| **Propiedad** | **Forma con congruencias** | **Interpretación** |
|---|---|---|
| $a$ es múltiplo de $b$ | $a \equiv 0 \pmod b$ | El resto de dividir $a$ entre $b$ es 0 |
| $a$ y $b$ dejan el mismo resto al dividir por $m$ | $a \equiv b \pmod m$ | $m$ divide a $a-b$ |

## *¡Retos!*

**Reto 1.** ¿En qué última cifra acaba el número $3^{200}$?

**Reto 2.** Vamos a aplicar las congruencias a la multiplicidad: Demuestre que el número $4^{n+1}+5^{2n-1}$ es múltiplo de 21, $\forall n \in \mathbb{N}$.

# 3. Ecuaciones congruenciales lineales

Consideremos la congruencia lineal

$$ax \equiv b \pmod{n}.$$

Sea $d = mcd(a,n)$. Entonces la congruencia tiene solución si y solo si $d \mid b$. Si $d \mid b$, existen exactamente $d$ soluciones módulo $n$, y dividiendo por $d$ se obtendrá una solución única módulo $n/d$.

*Ejemplo* 3.1. Resolver $6x \equiv 8 \pmod{14}$.

*Solución.* $mcd(6,14) = 2$ y como 2 divide a 8 entonces sí existen soluciones. Dividimos todo entre 2:

$$3x \equiv 4 \pmod{7}$$

como $mcd(3,7) = 1$, $3^{-1} \equiv 5 \pmod{7}$, luego

$$x \equiv 5 \cdot 4 \equiv 20 \equiv 6 \pmod{7}$$

Las soluciones módulo 14 son $x \equiv 6 \pmod{7}$, es decir $x \equiv 6, 13 \pmod{14}$. □

# 4. Teoremas fundamentales

## 4.1. Función $\varphi$ de Euler

**Definición 4.1.** Para $n \in \mathbb{Z}_+$, la función de Euler $\varphi(n)$ cuenta los enteros $1 \leq k \leq n$ que son coprimos con $n$, es decir, que no tienen divisores comunes con $n$ aparte del 1.

Propiedades importantes:

- Si $p$ es primo, $\varphi(p) = p - 1$.
- Si $p$ es primo y $\alpha \geq 1$, entonces $\varphi(p^\alpha) = p^\alpha - p^{\alpha-1} = p^{\alpha-1}(p-1)$.
- Si $m, n$ son coprimos, $\varphi(mn) = \varphi(m)\varphi(n)$ (multiplicatividad).

- En general, si $n = \prod_i p_i^{\alpha_i}$, entonces

$$\varphi(n) = \prod_i p_i^{\alpha_i - 1}(p_i - 1).$$

*Ejemplo* 4.1. Calculemos $\varphi(5)$: Los números del 1 al 5 son: $1,2,3,4,5$. Como 5 es primo, todos los números menores que 5 son coprimos con él. Por tanto:

$$\varphi(5) = 4.$$

*Ejemplo* 4.2. Calculemos $\varphi(8)$:

Los números del 1 al 8 son: $1,2,3,4,5,6,7,8$. Miremos cuáles son coprimos con 8:

$$mcd(1,8) = 1, \quad mcd(2,8) = 2, \quad mcd(3,8) = 1, \quad mcd(4,8) = 4,$$

$$mcd(5,8) = 1, \quad mcd(6,8) = 2, \quad mcd(7,8) = 1, \quad mcd(8,8) = 8.$$

Son coprimos: $1,3,5,7$. Así que:

$$\varphi(8) = 4.$$

*Ejemplo* 4.3. Calculemos $\varphi(10)$:
Los números del 1 al 10: $1,2,3,4,5,6,7,8,9,10$. El número $10 = 2 \cdot 5$. Debemos quitar los que tengan factores 2 o 5. Coprimos con 10: $1,3,7,9$. Así que:

$$\varphi(10) = 4.$$

*Ejemplo* 4.4. Si un número se puede escribir como producto de primos, podemos usar la fórmula:

$$\varphi(n) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\ldots$$

Por ejemplo, $n = 12 = 2^2 \cdot 3$, entonces:

$$\varphi(12) = 12\left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{3}\right) = 12 \cdot \frac{1}{2} \cdot \frac{2}{3} = 4.$$

**Idea clave:** $\varphi(n)$ cuenta cuántos números "no comparten divisores" con $n$, y se puede calcular fácilmente usando sus factores primos.

## 4.2. Teorema de Euler (enunciado y demostración)

**Teorema 4.2** (Euler)**.** *Si* $m.c.d(a,n) = 1$*, entonces*

$$a^{\varphi(n)} \equiv 1 \pmod{n}.$$

Como caso particular, si $n = p$ primo, obtenemos el pequeño teorema de Fermat: $a^{p-1} \equiv 1 \pmod{p}$ para $p \nmid a$.

## *¡Más retos!*

**Reto 1:** Resuelve la congruencia lineal $15x \equiv 10 \pmod{35}$ y explica cuántas soluciones hay modulo 35.

**Reto 2:** Halla el inverso multiplicativo de 17 módulo 43 (si existe). Usa el algoritmo extendido de Euclides.

**Reto 3:** Calcula $\varphi(360)$.

**Reto 4:** Usa el teorema de Euler para encontrar el resto de $7^{100} \pmod{20}$.

**Reto 5:** (Prueba corta) Demuestra que si $p$ es primo impar, entonces $2^{p-1} \equiv 1 \pmod{p}$ y deduce que $2^p - 2$ es divisible por $p$.

*NIVEL OLÍMPICO:*

**Reto 6:** Ya hemos visto lo sencillo que es hallar la última cifra de una gran potencia... ¿cuales son las **dos** últimas cifras del número $2019^{2020}$?

**Reto 7:** Demuestre que si $n \geq 0$, el número $14^n + 11$ no es primo.

**Reto 8:** Demuestre que $a^5 - a$ es múltiplo de 30, para cualquier número entero $a \in \mathbb{Z}$.

**Reto 9:** *(IMO, 1964)*Encuentre todos los enteros positivos $n$ tales que $2^n - 1$ es divisible entre 7.

**Reto 10:** *(OME Nacional, 1972)* Demuestre que, para todo entero positivo $n$, el número

$$A_n = 5^n + 2 \cdot 3^{n-1} + 1$$

es múltiplo de 8.