# CURSO BREVE DE CONGRUENCIAS EN TEORÍA DE NÚMEROS

Sean $a, b$ y $m$ números enteros. Diremos que $a$ y $b$ son **congruentes módulo** $m$ si $m \mid a - b$. En símbolos

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

Esta es una noción que simplifica muchas consideraciones en teoría de números. En este escrito discutiremos, principalmente mediante ejemplos, algunas de sus propiedades más relevantes en el ámbito olímpico.

## Observaciones y ejemplos numéricos

a) A lo largo de esta exposición nos restringiremos a módulos $m > 1$.

b) $2020 \equiv -2 \pmod{2}$, $11 \equiv 1 \pmod{2}$. En gral., dos números enteros $a$ y $b$ son congruentes módulo 2 si y sólo si los dos son pares o los dos son impares.

c) En el reloj aparecen bastante las congruencias módulo 12. Por ejemplo, para recordar qué hora en el intervalo $(0, 12)$ le corresponde a una hora dada del rango $(12, 24)$ basta con recordar las congruencias módulo 12: $13 \equiv 1 \pmod{12}$, $14 \equiv 2 \pmod{2}$, etc.

## Un par de hechos fundamentales

**1.** Todo número entero $a$ es congruente, módulo $m$, con el resto que $a$ deja en la división por $m$.

En consecuencia, si $a$ es un entero y $r$ es un entero del intervalo $[0, m)$ tal que $a \equiv r \pmod{m}$ entonces $r$ es el resto que deja $a$ cuando se le divide por $m$.

Así pues, tenemos que las tres afirmaciones siguientes son equivalentes:

a) $a$ deja resto 0 cuando se le divide entre $m$

b) $a$ es de la forma $mq$ para algún número entero $q$

c) $a \equiv 0 \pmod{m}$

**2.** Dos número enteros $a$ y $b$ son congruentes, módulo $m$, si y sólo si $a$ y $b$ dejan el mismo resto en la división por $m$.

## Propiedades para la manipulación de congruencias

i) (Reflexividad) Para cada número $a$ se cumple que $a \equiv a \pmod{m}$

ii) (Simetría) Si $a \equiv b \pmod{m}$, entonces $b \equiv a \pmod{m}$.

iii) (Transitividad) Si $a \equiv b \pmod{m}$ y $b \equiv c$, entonces $a \equiv c \pmod{m}$.

iv) Si $a \equiv b \pmod{m}$, entonces $a + c \equiv b + c \pmod{m}$.

v) Si $a \equiv b \pmod{m}$, entonces $ac \equiv bc \pmod{m}$.

vi) Si $a_1 \equiv b_1 \pmod{m}$, $a_2 \equiv b_2 \pmod{m}$, entonces $a_1 + a_2 \equiv b_1 + b_2 \pmod{m}$.

vii) Si $a_1 \equiv b_1 \pmod{m}$, $a_2 \equiv b_2 \pmod{m}$, entonces $a_1 a_2 \equiv b_1 b_2 \pmod{m}$.

viii) Si $a \equiv b \pmod{m}$ y $n$ es un número entero, entonces $a^n \equiv b^n \pmod{m}$.

ix) Si $a \equiv b \pmod{m}$ y $f(x)$ es un polinomio de coeficientes enteros, entonces $f(a) \equiv f(b) \pmod{m}$.

x) Si $ac \equiv bc \pmod{m}$ y $\text{mcd}(c, m) = 1$, entonces $a \equiv b \pmod{m}$.

## Problemas

**1.** (Determinación del dígito de las unidades de alguna potencia.) Halle la cifra de las unidades de $17^{15}$.

*Sol.* Congruencias módulo 10 o por periodicidad.

**2.** (Determinación del resto que deja algún número en la división por otro.) Si $11n$ deja resto 6 cuando se divide entre 7, ¿qué resto deja $5n$ cuando se le divide entre 7?

**3.** (4a. OMM, 3/1990) Demuestre que $n^{n-1} - 1$ es divisible entre $(n-1)^2$ para todo número entero $n \geq 2$.

*Sol.* Congruencias módulo $n - 1$.

**4.** (7a. OMM, 6/1993) Sean $f(x) = x(x+1)(x+2)(x+3) + 1$ y $p$ un número primo impar. Demuestre que $p \mid f(n)$ para algún número entero $n$ si y sólo si $p \mid m^2 - 5$ para algún entero $m$.

**5.** Sea $p$ un número primo positivo. Demuestre que existe un número entero $\alpha$ tal que $p \mid \alpha(\alpha - 1) + 3$ si y sólo existe un número entero $\beta$ tal que $p \mid \beta(\beta - 1) + 25$.

**6.** (Pruebas de imposibilidad) Si $p$ es un número primo impar entonces $p \equiv 1 \pmod{4}$ o $p \equiv 3 \pmod{4}$. Todo primo $p \equiv 1 \pmod{4}$ se puede expresar como una suma de dos cuadrados perfectos pero ninguno número primo $p \equiv 3 \pmod{4}$ se puede expresar de esa manera.

**7.** (Regional del Centro, 2019) Sean $a$, $b$ y $c$ números enteros mayores que cero. Demuestre que los números $2a^2 + b^2 + 3$, $2b^2 + c^2 + 3$ y $2c^2 + a^2 + 3$ no pueden ser cuadrados perfectos simultáneamente.

*Sol.* Congruencias módulo 4.

**8.** (5a. OMM, 5/1991) La suma de los cuadrados de dos números enteros consecutivos puede ser un cuadrado perfecto: por ejemplo, $3^2 + 4^2 = 5^2$.

a) Demuestre que la suma de los cuadrados de 3 números enteros consecutivos no puede ser un cuadrado perfecto.

b) Demuestre que la suma de los cuadrados de 6 números enteros consecutivos no puede ser un cuadrado perfecto.

c) Encuentre un ejemplo de 11 números positivos consecutivos cuya suma de cuadrados sea un cuadrado perfecto.

**9.** (El criterio de divisibilidad por 11)

### El Pequeño Teorema de Fermat

Sea $p$ un número primo. Para cada número entero $n$ se cumple que $n^p \equiv n \pmod{p}$.

**Ejemplos.**

a) Encuentre el resto que deja $7^{122}$ en la división por 11.

b) (11a. OMM, 1/1997) Encuentre todos los números primos positivos $p$ tales $8p^4 - 3003$ también es un número primo.

c) (15a. OMM, 1/2001) Encuentre todos los números de 7 dígitos que son múltiplos de 3 y 7 y cuyos son dígitos son 3 o 7.

d) Determine todos los números primos $p$ que satisfacen la congruencia $2011^p \equiv 1 \pmod{p}$.

e) Demuestre que si $n$ es un número natural mayor que 1 entonces $n \nmid 2^n - 1$.