CONGRUENCIAS

Sea *m* un número entero positivo.

Definición: se dice que **un número entero *a* es congruente con otro entero *b* módulo *m*** si y sólo si, al ser divididos entre *m*, ambos dejan el mismo resto. Se expresa: $a \equiv b \pmod{m}$.

Ejemplos: $25 \equiv 13 \pmod 6$, $18 \equiv 3 \pmod 5$

Otras definiciones equivalentes son:

I) $a \equiv b \pmod m \Leftrightarrow a - b = \dot{m}$ (*a*-*b* es múltiplo de *m*)

II) $a \equiv b \pmod m \Leftrightarrow a = b + k\,m \;\; con \;\; k \in \mathbb{Z}$ (demuéstrelas el alumno)

La relación de congruencia módulo *m* es una relación de equivalencia en el conjunto $\mathbb{Z}$ de los números enteros, pues cumple las propiedades:

Reflexiva: $a \equiv a \pmod m \;\; \forall a \in \mathbb{Z}$. Es decir, todo entero es congruente con sí mismo módulo *m*.

Simétrica: *Si* $a \equiv b \pmod m$ entonces $b \equiv a \pmod m$

Transitiva: *Si* $a \equiv b \pmod m$ *y* $b \equiv c \pmod m$ entonces $a \equiv c \pmod m$

Esta relación de equivalencia establece en $\mathbb{Z}$ una clasificación. En cada clase de equivalencia están todos los elementos que son congruentes entre sí módulo *m*. El conjunto cociente (conjunto cuyos elementos son las distintas clases de equivalencia) se denota por $\mathbb{Z}/m$ y recibe el nombre de **clases residuales módulo *m***.

Por ejemplo: el conjunto $\mathbb{Z}/4$ de las clases residuales módulo 4 consta de cuatro elementos (o clases): $\mathbb{Z}/4 = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}\}$ que son:

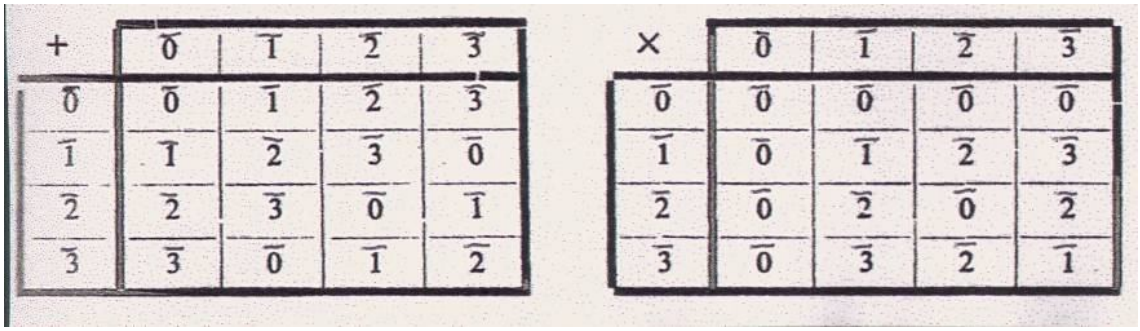
Clase 0 : $\overline{0} = \{..., -8, -4, 0, 4, 8, 12, ...\}$ (múltiplos de 4)

Clase 1: $\overline{1} = \{..., -7, -3, 1, 5, 9, 13, ...\}$ (múltiplos de 4 +1)

Clase 2: $\overline{2} = \{..., -6, -2, 2, 6, 10, 14...\}$ (múltiplos de 4 +2)

Clase 3: $\overline{3} = \{..., -5, -1, 3, 7, 11, 15, ...\}$ (múltiplos de 4 +3)

Las operaciones adición (+) y multiplicación (×) de $\mathbb{Z}$ inducen en $\mathbb{Z}/4$ las operaciones adición y multiplicación de clases que se resumen en las tablas siguientes:



+	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{3}$	$\overline{0}$	$\overline{1}$
$\overline{3}$	$\overline{3}$	$\overline{0}$	$\overline{1}$	$\overline{2}$

×	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{0}$	$\overline{2}$
$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

Notemos que para nombrar una clase se recurre por lo general al representante más sencillo (en nuestro caso el comprendido entre 0 y 3),
Pero también se puede recurrir a cualquier otro representante, sobre todo si resulta más cómodo. Así, en $\mathbb{Z}/4$, la clase 3 podría ser nominada como la clase -1 ya que la clase 1 es opuesta de la clase 3.

En el lenguaje de congruencias es lo mismo decir, por ejemplo, $12 \equiv 5 \pmod 7$, que decir $12 \equiv -2 \pmod 7$.

OPERACIONES CON CONGRUENCIAS

1) La suma de dos congruencias respecto de un mismo módulo *m* es otra congruencia respecto del mismo módulo. Es decir:

$$\left.\begin{array}{l} a_1 \equiv b_1 \pmod m \\ a_2 \equiv b_2 \pmod m \end{array}\right\} \Rightarrow a_1 + a_2 \equiv b_1 + b_2 \pmod m$$

   Es fácil de demostrar, así como de extender al caso de *n* sumandos.

2) El producto de dos congruencias respecto de un mismo módulo *m* es otra congruencia respecto del mismo módulo. Es decir:

$$\left.\begin{array}{l} a_1 \equiv b_1 \pmod m \\ a_2 \equiv b_2 \pmod m \end{array}\right\} \Rightarrow a_1 \cdot a_2 \equiv b_1 \cdot b_2 \pmod m$$

   También fácil de demostrar y de extender al caso de *n* factores.

   En particular:

3) Si multiplicamos los dos miembros de una congruencia por un mismo número entero, obtendremos otra congruencia respecto del mismo módulo. Es decir:

$$a \equiv b \pmod m \Rightarrow a \cdot c \equiv b \cdot c \pmod m \quad \forall c \in \mathbb{Z}$$

   El recíproco no es cierto, ya que si

$$a \cdot c \equiv b \cdot c \pmod m \Rightarrow a \cdot c - b \cdot c = \dot{m} \Rightarrow (a-b) \cdot c = \dot{m} \not\Rightarrow a - b = \dot{m}$$

   (La última implicación sólo sería cierta en el caso en que *c* fuese primo con *m*)

4) *Si* $a \equiv b \pmod m$ entonces $a^n \equiv b^n \pmod m \quad \forall n \in \mathbb{N}$.

   En general:

5) Si en un polinomio de coeficientes enteros $c_n x^n + c_{n-1} x^{n-1} + \cdots + c_1 x + c_0$ se sustituye la indeterminada *x* por cada uno de los miembros de una congruencia de módulo *m*, resulta otra congruencia respecto del mismo módulo. Es decir:

$$a \equiv b \pmod m \Rightarrow c_n a^n + c_{n-1} a^{n-1} + \cdots + c_0 \equiv c_n b^n + c_{n-1} b^{n-1} + \cdots + c_0 \pmod m$$

RESTOS POTENCIALES de una base *a* respecto del módulo *m*

Son los restos de las divisiones entre *m* de las sucesivas potencias de $a \in \mathbb{N}$ con $a \geq 2$,
$a^0 \equiv r_0 = 1 \pmod{m}$; $a^1 \equiv r_1 \pmod{m}$; $a^2 \equiv r_2 \pmod{m}$; $\cdots$; $a^n \equiv r_n \pmod{m}$

Conviene tener en cuenta que:

● El número de restos diferentes es menor o igual que *m-1* , por lo que se llegarán a repetir de forma periódica.

● Para su cálculo es útil la propiedad: $a^k \equiv r_k \pmod{m} \Rightarrow a^{k+1} = a^k \cdot a \equiv r_k \cdot a \pmod{m}$

● Conviene utilizar los restos por exceso (negativos) cuando su valor absoluto sea menor que el correspondiente resto por defecto.

Como ejemplo, calculemos los restos potenciales de base 10 respecto al módulo 11:

$10^0 \equiv 1 \pmod{11}$
$10^1 \equiv 10 \pmod{11}$ mejor: $10^1 \equiv -1 \pmod{11}$
$10^2 \equiv -10 \pmod{11}$ mejor: $10^2 \equiv 1 \pmod{11}$
$10^3 \equiv 10 \pmod{11}$ mejor: $10^3 \equiv -1 \pmod{11}$ *etc.*

De modo que tales restos son $r_0 = 1$; $r_1 = -1$; $r_2 = 1$; $r_3 = -1$; $\cdots$*etc.*

CRITERIO GENERAL DE DIVISIBILIDAD

Un número natural N que escrito en el sistema de base *a* se puede poner en la forma $c_n a^n + c_{n-1} a^{n-1} + \cdots + c_1 a + c_0$ será divisible por *m* si y sólo si $c_n r_n + c_{n-1} r_{n-1} + \cdots + c_1 r_1 + c_0$ es múltiplo de *m,* siendo $r_1, r_2, \cdots, r_n$ los restos potenciales de la base *a* respecto del módulo *m*.

Los criterios de divisibilidad más conocidos por el alumno corresponden al sistema decimal (caso *a*=10). Esta es buena ocasión para recordarlos y fundamentarlos. Como tenemos a mano los restos potenciales de la base 10 respecto del módulo 11, podemos deducir el criterio de divisibilidad por 11 de un número N que en el sistema decimal es $N = c_n \cdot 10^n + c_{n-1} \cdot 10^{n-1} + \cdots + c_1 \cdot 10 + c_0$

N será divisible por 11 si y sólo si $c_0 - c_1 + c_2 - c_3 + \cdots + (-1)^n c_n$ es múltiplo de 11.

También obtendremos fácilmente el criterio de divisibilidad por 9, ya que en este caso los restos potenciales de la base 10 con respecto al módulo 9 son todos iguales a 1:

N será divisible por 9 si y sólo si $c_0 + c_1 + c_2 + \cdots + c_n$ es múltiplo de 9.

¿Cómo será el criterio de divisibilidad por 7?

TRES TEOREMAS ENUNCIADOS EN TÉRMINOS DE CONGRUENCIAS

1. PEQUEÑO TEOREMA DE FERMAT

Enunciado 1: Si p es primo y a es natural, entonces $a^p \equiv a \pmod{p}$

Enunciado 2: Si p es primo y a es primo con p, entonces $a^{p-1} \equiv 1 \pmod{p}$

2. TEOREMA DE WILSON

Si p es primo, entonces $(p-1)! \equiv -1 \pmod{p}$

3. TEOREMA CHINO DEL RESTO

Si $m_1, m_2, ..., m_k$ son enteros positivos primos entre sí dos a dos, entonces el sistema:

$$\begin{cases} x \equiv a_1 \pmod{p_1} \\ x \equiv a_2 \pmod{p_2} \\ \quad \vdots \\ x \equiv a_k \pmod{p_k} \end{cases}$$ tiene solución única módulo $p_1 \cdot p_2 \cdot \cdots \cdot p_k$