DATE 25 03 20

Algebra Superior 2

Congruencias

Def. Sea $m \in \mathbb{N}$ y sean $a, b \in \mathbb{Z}$. Se dice que a es congruente con b módulo m si $a-b$ es divisible por m, y en este caso escribimos $a \equiv b \pmod{m}$.

Nota. Lo que nos dice la definición es que

$$a \equiv b \pmod{m} \iff m \mid a-b.$$

· $a \equiv b \pmod{m}$ es llamada una congruencia.

Obs. Si $a, b \in \mathbb{Z}$, entonces $a \equiv b \pmod{1}$.

Teo. Sea $m \in \mathbb{N}$. Cada entero es congruente módulo m con uno y solo uno de los números $0, 1, 2, \ldots, m-1$.

Dem. Sabemos que si $a \in \mathbb{Z}$, entonces existen $q, r \in \mathbb{Z}$ (y son únicos) tales que $a = qm + r$ con $0 \leq r < m$.

Por tanto, $a - r = qm$. Es decir, $m \mid a-r$.

O lo que es lo mismo, $a \equiv r \pmod{m}$ ■

Obs.
1. $m \mid a \iff a \equiv 0 \pmod{m}$ para $m \in \mathbb{N}, a \in \mathbb{Z}$.
2. $a \equiv b \pmod{m} \iff a-b \equiv 0 \pmod{m}$ para $a, b \in \mathbb{Z}$ y $m \in \mathbb{N}$.

Algunos ejercicios: Sean $m \in \mathbb{N}$ y $a, b, c \in \mathbb{Z}$.

1. $a \equiv a \pmod{m}$.
2. Si $a \equiv b \pmod{m}$, entonces $b \equiv a \pmod{m}$.
3. Si $a \equiv b \pmod{m}$ y $b \equiv c \pmod{m}$, entonces $a \equiv c \pmod{m}$.

¿Cómo se llaman estas 3 propiedades? ¿Les recuerdan algo?

Teo. Sea $m \in \mathbb{N}$ y $a, b, c, d \in \mathbb{Z}$, se cumplen las siguientes propiedades:

1. Si $a \equiv b \pmod{m}$ y $c \equiv d \pmod{m}$, entonces
$$a + c \equiv b + d \pmod{m} \quad \text{y}$$
$$a - c \equiv b - d \pmod{m}.$$

2. Si $a \equiv b \pmod{m}$ y $c \equiv d \pmod{m}$, entonces
$$ac \equiv bd \pmod{m}.$$

3. Si $a \equiv b \pmod{m}$, entonces $ca \equiv cb \pmod{m}$.

4. Si $a \equiv b \pmod{m}$, entonces $a^n \equiv b^n \pmod{m}$ para cualquier $n \in \mathbb{N}$.

Dem. 1: Como $a \equiv b \pmod{m}$ entonces $m \mid a - b$ y como $c \equiv d \pmod{m}$ entonces $m \mid c - d$.

Así, existen $k, \ell \in \mathbb{Z}$ tales que
$$a - b = km \quad \text{y} \quad c - d = \ell m.$$

Ahora $(a+c) - (b+d) = (a-b) + (c-d) = km + \ell m$
$$= (k + \ell)m.$$
Es decir, $(a+c) - (b+d)$ es divisible por m y esto es lo que se tenía que probar.

La otra congruencia se obtiene de manera análoga.

2: $ac - bd = (a-b)(c-d) + ad + bc - 2bd$
$$= (a-b)(c-d) + d(a-b) + b(c-d).$$

Como $m \mid a-b$ existe k tq $a - b = km$ y como $m \mid c-d$ existe ℓ tq $c - d = \ell m$.

Por tanto, $ac - bd = (km)(\ell m) + d(km) + b(\ell m)$
$$= (k\ell m + dk + b\ell)m$$
$\therefore \; ac \equiv bd \pmod{m}$.

3: Como $a \equiv b \pmod{m}$ y por el ejercicio 1, $c \equiv c \pmod{m}$ el resultado deseado se sigue de la propiedad 2.

4: ¿Cómo lo demostrarían a partir de la propiedad 2?

Reto. Encontrar el residuo cuando se divide

$$1^{10} + 2^{10} + 3^{10} + \cdots + 99^{10} + 100^{100}$$ entre 7.