NO.

DATE 30.08.20

Algebra Superior 2

Congruencias lineales

La ecuación lineal $ax = b$ con $a, b \in \mathbb{Z}$ tiene solución entera si y solo si $a \mid b$.
Esta sección del curso está dedicada al problema análogo de resolver la congruencia $ax \equiv b \pmod{m}$.

Empecemos con un ejemplo: $3x \equiv 2 \pmod{5}$.

Es fácil ver que 4, 9 y 14 satisfacen la congruencia y observamos que estos números son congruentes módulo 5.
Podríamos entonces formular la hipótesis de que todos los enteros x que sean congruentes con 4 módulo 5 satisfarán la congruencia.

dem.

Si $x \equiv 4 \pmod{5}$, entonces ①
$3x \equiv 3 \cdot 4 \pmod{5}$ y $\therefore$
$3x \equiv 2 \pmod{5}$. ②

En otras palabras todas las $x \in \mathbb{Z}$ que cumplen ① también cumplen ②.

Podemos también demostrar que estas son las únicas soluciones:
Supongamos que $x \in \mathbb{Z}$ es solución de la congruencia $3x \equiv 2 \pmod{5}$, entonces

$3x \equiv 2 \pmod{5}$ y $\therefore$
$3x \equiv 12 \pmod{5}$.
Ahora, como $(3,5) = 1$ se sigue (¿por qué?) que $x \equiv 4 \pmod{5}$ que es lo que queríamos.

Concluimos entonces que x cumple
$3x \equiv 2 \pmod{5}$ si y solo si $x \equiv 4 \pmod{5}$. ∎

NO.

DATE

Para poder describir las soluciones de congruencias lineales en general necesitamos hacer lo siguiente:

Sabemos ya que cada entero es congruente módulo m con uno y solo uno de los números $0, 1, 2, \ldots, m-1$.

Este resultado muestra que para cada $m \in \mathbb{N}$ existe una partición de $\mathbb{Z}$ en clases $X_0, X_1, \ldots, X_{m-1}$ en donde

$$X_r = \{ x \in \mathbb{Z} : \; x \equiv r \pmod{m} \}.$$

Si revisan las notas del 25·03·20, verán que las congruencias son una relación de equivalencia y como ya sabemos esto implica que los conjuntos $X_0, X_1, \ldots, X_{m-1}$ en efecto son una partición de $\mathbb{Z}$. Es decir, son ajenos dos a dos y cualquier entero se encuentra en uno de ellos.

Estos conjuntos son llamadas clases de congruencias módulo m o clases residuales módulo m.

Ejemplos: 1. Si $m = 2$, entonces $X_0 = \{ x \in \mathbb{Z} : x \equiv 0 \pmod 2 \}$ y $X_1 = \{ x \in \mathbb{Z} : x \equiv 1 \pmod 2 \}$.

Es decir, X_0 es el conjunto de enteros pares y X_1 es el conjunto de enteros impares.

2. Si $m = 4$, entonces

$$X_0 = \{ x \in \mathbb{Z} : x \equiv 0 \pmod 4 \} = \{ 4k : k \in \mathbb{Z} \}$$
$$X_1 = \{ x \in \mathbb{Z} : x \equiv 1 \pmod 4 \} = \{ 4k+1 : k \in \mathbb{Z} \}$$
$$X_2 = \{ x \in \mathbb{Z} : x \equiv 2 \pmod 4 \} = \{ 4k+2 : k \in \mathbb{Z} \}$$
$$X_3 = \{ x \in \mathbb{Z} : x \equiv 3 \pmod 4 \} = \{ 4k+3 : k \in \mathbb{Z} \}.$$

Obs. Sea $m \in \mathbb{N}$. Si dos enteros x, y están en la misma clase de congruencia módulo m, digamos X_r, entonces

$$x \equiv r \pmod{m} \quad \text{y} \quad y \equiv r \pmod{m}.$$

Se sigue entonces que $x \equiv y \pmod{m}$.

Y conversamente, si $x \equiv y \pmod{m}$ y $y \in X_r$ entonces $x \in X_r$.

Por tanto dos enteros x y y están en la misma clase de congruencia módulo m si y solo si

$$x \equiv y \pmod{m}.$$

Por tanto si x es solución de la congruencia lineal $ax \equiv b \pmod{m}$ entonces todo entero de la clase de congruencia módulo m en la que se encuentra x también es solución.

En el ejemplo $3x \equiv 2 \pmod{5}$ todo $x \in X_4$ es solución.

Es MUY importante que notemos que hay congruencias lineales con soluciones que pertenecen a más de una clase de congruencia módulo m:

$$2x \equiv 6 \pmod{12}$$

Y también que hay congruencias lineales sin solución:

$$2x \equiv 1 \pmod{6}.$$

Ejercicio: Comprueba estos resultados.