Aritmética modular, parte II

Ejemplo 1. Encuentre (si existe) la solución de la congruencia lineal $9x \equiv 3 \pmod{15}$

Primero calculamos el mcd(15,9) usando el algoritmo de Euclides:

$$15 = 1 \cdot 9 + 6$$
$$9 = 1 \cdot 6 + 3$$
$$6 = 2 \cdot 3$$

$\therefore$ mcd(15,9) = 3 y como mcd(15,9) = 3 | $b = 3$, entonces la congruencia lineal sí tiene solución.

De la definición de congruencia modular tenemos:

$$9x \equiv 3 \pmod{15} \leftrightarrow 15 \mid (9x - 3) \leftrightarrow 9x - 3 = 15k \leftrightarrow 9x + 15(-k) = 3 \text{ [ec. diofántica]}$$

Para encontrar x usamos la identidad de Bézout:

$$3 = 9 - 1 \cdot 6 = 9 - 1 \cdot (15 - 1 \cdot 9) = 9 - 15 + 9 = 9(2) + 15(-1) \rightarrow x = 2$$

⚠ La solución general para la variable $x = 2 + \lambda \cdot (15/3) = 2 + 5\lambda$

Estamos buscando todas las soluciones de la congruencia lineal en $\mathbb{Z}_{15}$, es decir, $0 \leq x \leq 14$:

$\lambda = -1 \rightarrow x = 2 - 5 = -3 \notin \mathbb{Z}_{15}$
$\lambda = 0 \rightarrow x = 2 \in \mathbb{Z}_{15}$
$\lambda = 1 \rightarrow x = 2 + 5 = 7 \in \mathbb{Z}_{15}$
$\lambda = 2 \rightarrow x = 2 + 10 = 12 \in \mathbb{Z}_{15}$
$\lambda = 3 \rightarrow x = 2 + 15 = 17 \notin \mathbb{Z}_{15}$

En conclusión, las tres soluciones de la congruencia lineal $9x \equiv 3 \pmod{15}$ son $x \equiv 2, 7$ & $12 \pmod{15}$.

Ejemplo 2. Encuentre (si existe) la solución de la congruencia lineal $8x \equiv 12 \pmod{20}$.

Primero calculamos el mcd(20,8):

$$20 = 2 \cdot 8 + 4$$
$$8 = 2 \cdot 4$$

$\therefore$ mcd(20,8) = 4 y como mcd(20,8) = 4 | $b = 12$, la congruencia lineal sí tiene solución

$$8x \equiv 12 \pmod{20} \rightarrow 8x + 20(-k) = 12 \text{ [ec. diofántica]}$$

Por la identidad de Bézout sabemos que existen v y w tales que $8v + 20w = 4$.

$$4 = 20 + 8(-2) \rightarrow v = -2 \text{ \& } w = 1$$

Luego multiplicamos ambos lados de la ecuación por 3:

$$12 = 20(3) + 8(-6) \rightarrow x = -6$$

La solución general para la variable x es: $x = -6 + \lambda(20/4) = -6 + 5\lambda$

⚠ Recordemos que buscamos soluciones en $\mathbb{Z}_{20}$, es decir, $0 \leq x \leq 19$:

$\lambda = 2 \rightarrow x = 4$
$\lambda = 3 \rightarrow x = 9$
$\lambda = 4 \rightarrow x = 14$
$\lambda = 5 \rightarrow x = 19$

En conclusión, las cuatro soluciones de la congruencia lineal $8x \equiv 12 \pmod{20}$ son

$$x \equiv 4, 9, 14 \ \& \ 19 \pmod{20}$$

En resumen, dada una congruencia lineal $ax \equiv b \pmod{n}$ tenemos:

- si $\text{mcd}(a,n) = 1 \rightarrow$ la congruencia lineal tiene solución única
- si $\text{mcd}(a,n) \neq 1$ y
  - $\text{mcd}(a,n) \mid b \rightarrow$ la congruencia lineal tiene exactamente $\text{mcd}(a,n)$ soluciones
  - $\text{mcd}(a,n) \nmid b \rightarrow$ la congruencia lineal tiene no tiene solución

Sistemas de congruencias lineales

Definición. Se le llama **sistema de congruencias lineales** a un conjunto de dos o más congruencias lineales.

Ejemplo 3. Encuentre (si existe) la solución del siguiente sistema de congruencias lineales:

$x \equiv 2 \pmod{3}$
$x \equiv 3 \pmod{5}$

💡 Vamos a *construir* la solución de la siguiente manera $x = x_1 + x_2$, en donde x_1 es un múltiplo de 5 y x_2 es un múltiplo de 3:

$$x_1 = 5k_1 \ \& \ x_2 = 3k_2$$

de manera que al evaluar en la primera ecuación $x \equiv 2 \pmod{3}$ tenemos:

$5k_1 + 3k_2 \equiv 2 \pmod{3} \rightarrow 5k_1 + 3k_2 - 2 = 3k \rightarrow 5k_1 + 3(k_2 - k) = 2$ [ec. diofántica]

$5 = 1 \cdot 3 + 2$
$3 = 1 \cdot 2 + 1$
$2 = 2 \cdot 1$

$1 = 3 - 2 = 3 - (5 - 3) = 3(2) + 5(-1) \rightarrow 2 = 3(4) + 5(-2) \rightarrow k_1 = -2$

Similarmente al evaluar x en la segunda ecuación $x \equiv 3 \pmod{5}$ tenemos:

$5k_1 + 3k_2 \equiv 3 \pmod{5} \rightarrow 5k_1 + 3k_2 - 3 = 5k \rightarrow 5(k_1 - k) + 3k_2 = 3$ [ec. diofántica]

$1 = 3 - 2 = 3 - (5 - 3) = 3(2) + 5(-1) \rightarrow 3 = 3(6) + 5(-3) \rightarrow k_2 = 6$

En conclusión, $x = 5k_1 + 3k_2 = 5(-2) + 3(6) = 8$ y la solución del sistema de congruencias lineales es:

$$x \equiv 8 \pmod{15}$$

Teorema. (*Teorema chino del residuo*)

Un sistema de congruencias lineales de la forma $a_i \equiv b_i \pmod{n_i}$ tiene solución única si:

$\text{mcd}(n_i, n_j) = 1$ con $i \neq j$, es decir, los módulos son primos relativos a pares

Ejercicio 4. Encuentre (si es posible) la solución del sistema de congruencias lineales:

$x \equiv 3 \pmod{5}$
$x \equiv 4 \pmod{7}$
$x = 9 \pmod{11}$

Ayuda: Tome $x = (7 \cdot 11)x_1 + (5 \cdot 11)x_2 + (5 \cdot 7)x_3$