Ecuaciones lineales de Congruencia

Matemática Discreta – UCA

M. Julia Bolívar

Recuerdo

Vamos a usar que:

- ❖ Sean $a, b \in \mathbb{Z}$ no ambos nulos. Entonces existen $s, t \in \mathbb{Z}$ tales que $mcd(a, b) = sa + tb$

- ❖ Sean $a, b, c \in \mathbb{Z}$, entonces

$\exists\, s, t \in \mathbb{Z}$ tales que $c = sa + tb$ si y solo si c es múltiplo $mcd(a, b)$

También vamos a usar que:

- $a \equiv b(m) \Leftrightarrow ac \equiv bc(mc)$ con $c \in \mathbb{N}$

- Sean $a, b, c \in \mathbb{Z}$, $m \in \mathbb{N}$ tal que $mcd(c, m) = 1$, entonces:

$$ac \equiv bc\ (m) \Leftrightarrow a \equiv b\ (m)$$

Ecuaciones lineales de Congruencia

Dados $a, b \in \mathbb{Z}$, queremos hallar todos los $x \in \mathbb{Z}$ que satisfacen:

$$ax \equiv b(m)$$

Notemos que:

Existe $x \in \mathbb{Z}$ solución de $ax \equiv b(m)$ si y solo si existen $x, k \in \mathbb{Z}$ tal que $ax - b = km$ si y solo si existen $x, k \in \mathbb{Z}$ tal que $ax + (-k)m = b$

Con lo cual la ecuación $ax + (-k)m = b$ tiene solución si y solo si b es múltiplo de $mcd(a, m)$

$ax \equiv b(m)$ tiene solución si y solo si b es múltiplo de $mcd(a, m)$

$ax \equiv b(m)$ tiene solución si y solo si $mcd(a,m) \mid b$

Ejemplos

1) La ecuación $14x \equiv 5(21)$ no tiene solución ya que $mcd(14{,}21) = 7$ y 7 no divide a 5

2) La ecuación $6x \equiv 31(7)$ tiene solución ya que $mcd(6{,}7) = 1$ y 31 es múltiplo de 1 (o lo que es lo mismo 1 divide 31)

Decidir si $x = 1, x = 2, x = 4$ son soluciones de la ecuación dada

¿ $6.1 \equiv 31(7)$? 

¿ $6.2 \equiv 31(7)$? 

¿ $6.4 \equiv 31(7)$? 

¿Tendrá más soluciones?

Cantidad de soluciones

$ax \equiv b(m)$ tiene solución si y solo si b es múltiplo de $mcd(a, m)$

Además si $d = mcd(a, m)$, la ecuación tendrá d soluciones x que satisfacen $0 \leq x < m$

Si $d = mcd(a, m)$, la ecuación $ax \equiv b(m)$ es equivalente a $\frac{a}{d}x \equiv \frac{b}{d}\left(\frac{m}{d}\right)$

Resolveremos la última y usaremos que las soluciones de la primera serán de la forma:

$$x_k = x_0 + k\frac{m}{d} \qquad con \ \ k = 0, 1, \dots, d-1$$

Donde x_0 es la solución de la ecuación $\frac{a}{d}x \equiv \frac{b}{d}\left(\frac{m}{d}\right)$

En el ejemplo anterior vimos que $x = 4$ es solución de $6x \equiv 31(7)$

Lo dicho anteriormente asegura que esta será la única solución entre 0 y 7

ya que $mcd(6,7) = 1$

Si consideramos todo $\mathbb{Z}$ la ecuación tiene infinitas soluciones pero todas

serán congruentes a 4 módulo 7, es decir

$$S = \{x \in \mathbb{Z}: \; x = 7k + 4, \quad con\, k \; \in \mathbb{Z} \}$$

En el ejemplo anterior sabíamos que $x = 4$ era solución de $6x \equiv 31(7)$

¿Cómo haríamos para obtener 4 ?

Partimos de $6x \equiv 31(7)$

La idea será usar propiedades para ir encontrando ecuaciones más simples

Por ejemplo podemos usar que $31 \equiv 3(7)$

Así que por transitividad $6x \equiv 3(7)$

Si $mcd(c, m) = 1$, entonces: $ac \equiv bc\ (m) \Leftrightarrow a \equiv b\ (m)$

Como $mcd(6,7) = 1$ $\quad 6x \equiv 3(7) \quad \Leftrightarrow \quad 36x \equiv 18(7)$

$6x \equiv 3(7) \quad \Leftrightarrow \quad 36x \equiv 18(7)$

$36 \equiv 1(7) \quad \Rightarrow \quad 36x \equiv x(7)$ y $18 \equiv 4(7)$

Así que debe ser $x \equiv 4(7)$

Veamos otro ejemplo, resolver $39x \equiv 24(45)$

Primero vemos si tiene solución

$mcd(39{,}45) = 3 \qquad y \qquad 3\ divide\ a\ 24$

Sabemos que habrá 3 soluciones entre 0 y 45, el resto serán congruentes módulo 45.

Dividimos toda la ecuación por 3: $13x \equiv 8(15)$

Buscamos una solución de esta ecuación (la cual estará entre 0 y 15)

La idea es buscar el inverso multiplicativo de 13 módulo 15, es decir un valor a tal que $13a \equiv 1(15)$

Podría buscarlo a “ojo” o usando el algoritmo de Euclides

$13a \equiv 1(15) \Longleftrightarrow 13a - 1 = 15k \Longleftrightarrow 13a - 15k = 1$

Usando el algoritmo de Euclides

$$\begin{aligned} 15 &= 13.1 + 2 \\ 13 &= 6.2 + 1 \\ 2 &= 2.1 \end{aligned}$$

$15 = 13.1 + 2$

$13 = 6.2 + 1 \quad \rightarrow \quad 1 = 13 - 6.2 = 13 - 6.(15 - 13) = 7.13 - 6.15$

Así que $a = 7$ $\qquad 13x \equiv 8(15) \rightarrow \; 7.13x \equiv 56(15) \rightarrow x \equiv 56(15) \rightarrow x \equiv 11(15)$

$x = 15q + 11 \quad q \in \mathbb{Z}$ Son las infinitas soluciones enteras de la ecuación

Hay 3 soluciones entre 0 y 45 $(x = 11,\; x = 26,\; x = 41)$, el resto será congruentes a ellas módulo 45

Pequeño Teorema de Fermat

p un número primo positivo y sea $a \in \mathbb{Z}$. Si $p \nmid a$ (p no divide a a) entonces

$$a^{p-1} \equiv 1(p)$$

Ejercicio: *Hallar el resto de la división de* 7^{45206} $por\ 13$

13 es primo y $13 \nmid 7$ entonces por el Pequeño Teorema de Fermat: $7^{12} \equiv 1(13)$

Por otro lado: $45206 = 3767.12 + 2 \quad \rightarrow \quad 7^{45206} = (7^{12})^{3767} 7^2$

Así que: $(7^{12})^{3767} 7^2 \equiv 1.49(13)$ y $49 \equiv 10(13)$

Con lo cual el resto de la división es 10