Matemática Discreta I
Clase 15 - Congruencias / Ecuación lineal de congruencia

FAMAF / UNC

11 de mayo de 2023

La utilidad de las congruencias reside principalmente en el hecho de que son compatibles con las operaciones aritméticas. Específicamente, tenemos el siguiente teorema.

Teorema

Sea m un entero positivo y sean x_1, x_2, y_1, y_2 enteros tales que

$$x_1 \equiv x_2 \pmod{m}, \qquad y_1 \equiv y_2 \pmod{m}.$$

Entonces

a) $x_1 + y_1 \equiv x_2 + y_2 \pmod{m}$,

b) $x_1 y_1 \equiv x_2 y_2 \pmod{m}$,

c) Si $x \equiv y \pmod{m}$ *y* $j \in \mathbb{N}$, *entonces* $x^j \equiv y^j \pmod{m}$.

Demostración

(a) Por hipótesis $\exists x, y$ tq $x_1 - x_2 = mx$ e $y_1 - y_2 = my$. Luego,

$$\begin{aligned}(x_1 + y_1) - (x_2 + y_2) &= (x_1 - x_2) + (y_1 - y_2)\\ &= mx + my\\ &= m(x + y),\end{aligned}$$

y por consiguiente el lado izquierdo es divisible por m.

(b) Aquí tenemos

$$\begin{aligned}x_1 y_1 - x_2 y_2 &= x_1 y_1 - x_2 y_1 + x_2 y_1 - x_2 y_2\\ &= (x_1 - x_2) y_1 + x_2 (y_1 - y_2)\\ &= mxy_1 + x_2 my\\ &= m(xy_1 + x_2 y),\end{aligned}$$

y de nuevo el lado izquierdo es divisible por m.

(c) Lo haremos por inducción sobre j.

Es claro que si $j = 1$ el resultado es verdadero.

Supongamos ahora que el resultado vale para $j - 1$, es decir

$$x^{j-1} \equiv y^{j-1} \pmod{m}.$$

Como $x \equiv y \pmod{m}$, por (b) tenemos que

$$x^{j-1}x \equiv y^{j-1}y \pmod{m},$$

es decir

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

□

Regla del nueve

Proposición

Sea $(x_n x_{n-1} \ldots x_0)_{10}$ *la representación del entero positivo* x *en base* 10*, entonces*

$$x \equiv x_0 + x_1 + \cdots + x_n \pmod{9}$$

Demostración

Observemos: $10 \equiv 1 \pmod{9} \Rightarrow 10^k \equiv 1^k \equiv 1 \pmod{9}$.

Por la definición de representación en base 10, tenemos que

$$x = x_0 + 10x_1 + \cdots + 10^n x_n,$$

Luego, $x_k 10^k \equiv x_k \pmod{9}$ y entonces $x \equiv x_0 + x_1 + \cdots + x_n \pmod{9}$.

□

Corolario

Sea $x = (x_n x_{n-1} \dots x_0)_{10}$, *entonces*

$$9|x \quad \Leftrightarrow \quad 9|x_0 + x_1 + \cdots + x_n.$$

Demostración

Por la proposición anterior

$$x \equiv x_0 + x_1 + \cdots + x_n \pmod{9} \tag{*}$$

Entonces,

$$\begin{aligned} 9|x \quad &\Leftrightarrow \quad x \equiv 0 \pmod{9} && \text{(por hipótesis)} \\ &\Leftrightarrow \quad x_0 + x_1 + \cdots + x_n \equiv 0 \pmod{9} && \text{(por (*))} \\ &\Leftrightarrow \quad 9|x_0 + x_1 + \cdots + x_n. && \square \end{aligned}$$

Ejemplo

Probar que $\quad 54\,321 \cdot 98\,765 \neq 5\,363\,013\,565.$

Demostración

Módulo 9:

$$\begin{array}{rcccccccl} 54\,321 & \equiv & 5+4+3+2+1 & \equiv & 15 & \equiv & 6 & \pmod{9} \\ 98\,765 & \equiv & 9+8+7+6+5 & \equiv & 35 & \equiv & 8 & \pmod{9} \end{array}$$

Entonces

$$54\,321 \cdot 98\,765 \equiv 6 \cdot 8 \equiv 48 \equiv 4+8 \equiv 12 \equiv 3 \pmod{9}$$

Mientras que

$$5\,363\,013\,565 \equiv 5+3+6+3+0+1+3+5+6+5 \equiv 37 \equiv 1 \pmod{9}$$

Luego $54\,321 \cdot 98\,765 \neq 5\,363\,013\,565.$ $\square$

Ecuación lineal de congruencia

Estudiaremos el problema de encontrar los $x \in \mathbb{Z}$ tal que

$$ax \equiv b \pmod{m}. \tag{1}$$

Una ecuación como (1) es llamada una *ecuación lineal de congruencia.*

El problema no siempre admite solución.

Por ejemplo, $2x \equiv 3 \pmod{2}$ no posee ninguna solución en $\mathbb{Z}$, pues cualquiera se $k \in \mathbb{Z}$, $2k - 3$ es impar, luego no es divisible por 2.

Notemos además que si x_0 es solución de la ecuación (1), también lo es $x_0 + km$ de manera que si la ecuación posee una solución, posee infinitas soluciones.

Ejemplo

La solución general de la ecuación $3x \equiv 7 \pmod{11}$ es $6 + k11$ con $k \in \mathbb{Z}$.

Demostración

Si probamos con los enteros x tal que $0 \leq x < 11$, veremos que la ecuación admite una única solución, a saber $x = 6$.

Otras soluciones se obtienen tomando $6 + 11k$.

Por otra parte si u es también solución de la ecuación, se tiene

$$3u \equiv 7 \pmod{11}, \quad 3 \cdot 6 \equiv 7 \pmod{11} \quad \Rightarrow \quad 3u \equiv 3 \cdot 6 \pmod{11}.$$

Por lo tanto $3(u - 6)$ es múltiplo de 11.

Como 11 no divide a 3 se tiene que $11|(u - 6)$, o sea $u = 6 + 11k$. $\square$

Ejemplo

Encontrar $0 \leq x < 109$ solución de la ecuación $74x \equiv 5 \pmod{109}$.

Solución

- $1 = (74, 109)$, por lo tanto, existen $s, t \in \mathbb{Z}$ tal que
$$1 = s \cdot 74 + t \cdot 109 \tag{2}$$
- Luego,
$$1 \equiv s \cdot 74 \pmod{109}. \tag{3}$$
- Multiplicando por 5 la ecuación (3), obtenemos
$$5 \equiv (5s) \cdot 74 \pmod{109}. \tag{4}$$

Eso implica que $5s$ es solución de $74x \equiv 5 \pmod{109}$.

Con el algoritmo de Euclides obtenemos,

$$1 = 28 \cdot 74 + (-19) \cdot 109.$$

Por lo anterior, $5 \cdot 28 = 140$ es solución de la ecuación, es decir,

$$74 \cdot 140 \equiv 5 \pmod{109}.$$

Pero $140 > 109$. Pero $31 = 140 - 109$ también es solución, pues $109 \equiv 0 \pmod{109}$.

Luego la solución es $x = 31$, pues

$$74 \cdot 31 \equiv 5 \pmod{109}. \qquad \text{y} \qquad 0 \leq 31 < 109.$$

$\square$

Analicemos ahora la situación general de la ecuación $ax \equiv b \pmod{m}$.

Teorema

Sean a, b números enteros y m un entero positivo y denotemos $d = \operatorname{mcd}(a, m)$. La ecuación

$$ax \equiv b \pmod{m} \tag{5}$$

admite solución si y sólo si $d|b$, y en este caso dada x_0 una solución, todas las soluciones son de la forma

$$x = x_0 + kn, \qquad \text{con } k \in \mathbb{Z} \text{ y } n = \frac{m}{d}$$

Demostración

($\Leftarrow$) Muy similar al ejemplo anterior (p. 10). Como

$$d = s \cdot a + t \cdot m, \qquad \text{para algunos } s, t \in \mathbb{Z},$$

tenemos

$$d \equiv s \cdot a \pmod{m}.$$

Como $d|b$, tenemos $b = dq$. Por lo tanto,

$$b = dq \equiv qs \cdot a \pmod{m}.$$

Es decir

$$a(qs) \equiv b \pmod{m}.$$

Es decir, $x_0 = qs$ es solución de $ax \equiv b \pmod{m}$.

Veamos ahora que si $n = \frac{m}{d}$ y $k \in \mathbb{Z}$, entonces $x_0 + kn$ también es solución.

Es decir
$$a(x_0 + kn) \equiv b \pmod{m}.$$

Como $d|a \Rightarrow a = dr$, luego $akn = dr\frac{m}{d} = rm \equiv 0 \pmod{m}$.

Luego
$$a(x_0 + kn) \equiv ax_0 + akn \equiv ax_0 \equiv b \pmod{m}.$$

($\Rightarrow$) Ver apunte.

Ejemplo

Encontrar todos los $x \in \mathbb{Z}$ tales que

$$6x \equiv 18 \pmod{21}. \qquad (*)$$

Solución

Como $3 = (6, 21)$ y $3|18$, la ecuación (*) tiene solución.
Por otro lado, por el algoritmo de Euclides,

$$\begin{array}{ccccc} 3 & = & (-3)\cdot 6 + 1\cdot 21 & & \Longrightarrow \\ 3 & \equiv & (-3)\cdot 6 & \pmod{21} & \overset{\text{multiplicando por 6}}{\Longrightarrow} \\ 18 & \equiv & (-18)\cdot 6 & \pmod{21} & \Longrightarrow \\ 6\cdot(-18) & \equiv & 18 & \pmod{21} & . \end{array}$$

Es decir $x_0 = -18$ es solución de la ecuación (*) y todas las soluciones son $-18 + k\cdot(\frac{21}{3})$, $k \in \mathbb{Z}$. $\square$