Congruencia

Prof. Jhon Fredy Tavera Bucurú

2025

Congruencias

Clases de Equivalencia

Congruencia

Definición (Definición de congruencia)

Sean $a, b, n \in \mathbb{Z}$. Decimos que a es congruente a b módulo n, y escribimos

$$a \equiv b \pmod{n}$$

si $n \mid (a - b)$, es decir, si a y b dejan el mismo resto en la división por n.

Por ejemplo, tenemos que

$$17 \equiv 3 \pmod{7} \quad \text{y} \quad 10 \equiv -5 \pmod{3}.$$

Teorema

Dos enteros a y b son congruentes módulo n si y solo si tienen el mismo residuo al dividirlos por n.

Demostración: Supongamos que $a \equiv b \pmod{n}$.
Sea r el residuo de dividir b por n. Entonces, por hipótesis, existe un entero k tal que:

$$a - b = kn,$$

y además:

$$b = qn + r \quad \text{con } 0 \leq r < n.$$

En consecuencia:

$$a = kn + b = kn + (qn + r) = n(k + q) + r \quad \text{con } 0 \leq r < n.$$

Por el algoritmo de la división, r es el residuo de dividir a por n.
Por lo tanto, a y b tienen el mismo residuo.
Ahora, en la dirección inversa, supongamos que:

$$a = q_1 n + r \quad \text{y} \quad b = q_2 n + r \quad \text{con } 0 \leq r < n.$$

Entonces:

$$a - b = (q_1 - q_2)n.$$

Por lo tanto, $n \mid (a - b)$, lo que implica que:

$$a \equiv b \pmod{n}.$$

Proposición (Relación de Equivalencia)

Para cualesquiera $a, b, c, d, n \in \mathbb{Z}$, *tenemos:*

1. *(**Reflexividad**)* $a \equiv a \pmod{n}$;
2. *(**Simetría**) si* $a \equiv b \pmod{n}$, *entonces* $b \equiv a \pmod{n}$;
3. *(**Transitividad**) si* $a \equiv b \pmod{n}$ *y* $b \equiv c \pmod{n}$, *entonces* $a \equiv c \pmod{n}$;

Demostración: Para el ítem (1), basta observar que:

$$n \mid (a - a) = 0.$$

En el ítem (2), si $n \mid (a - b)$, entonces:

$$n \mid -(a - b) \iff n \mid (b - a).$$

Para el ítem (3), si $n \mid (a - b)$ y $n \mid (b - c)$, entonces:

$$n \mid ((a - b) + (b - c)) \iff n \mid (a - c).$$

□

Teorema

Si $a \equiv b \pmod{n}$ *y* $c \equiv d \pmod{n}$, *entonces:*

1. *Para todo par de enteros* r *y* s,

$$ar + cs \equiv br + ds \pmod{n}.$$

2. $a + c \equiv b + d \pmod{n}$.
3. $a - c \equiv b - d \pmod{n}$.
4. $ac \equiv bd \pmod{n}$.
5. *Para todo entero positivo* k, $a^k \equiv b^k \pmod{n}$.
6. *Para todo entero* r, $a + r \equiv b + r \pmod{n}$.
7. *Para todo entero* r, $ar \equiv br \pmod{n}$.

Demostración:

1. La hipótesis dice que $n \mid (a-b)$ y $n \mid (c-d)$, luego, por el Teorema 2.1, tenemos que:

$$n \mid \{r(a-b)+s(c-d)\} = (ar+cs)-(br+ds),$$

y por lo tanto:

$$ar+cs \equiv br+ds \pmod{n}.$$

2. Se sigue de (1) tomando $r = s = 1$.
3. Se sigue de (1) tomando $r = 1$ y $s = -1$.
4. Basta observar que:

$$ac-bd = (a-b)c+b(c-d).$$

5. La demostración es por inducción sobre k:
6. Es suficiente aplicar (2) a las congruencias $a \equiv b \pmod{n}$ y $r \equiv r \pmod{n}$.
7. Es suficiente aplicar (4) a las congruencias $a \equiv b \pmod{n}$ y $r \equiv r \pmod{n}$.

Determine el último digito de 3^{2016}

Corolario

Si $a \equiv b \pmod{n}$ *y* $P(x)$ *es un polinomio con coeficientes enteros, entonces:*

$$P(a) \equiv P(b) \pmod{n}.$$

Proposición

Un entero positivo expresado en forma decimal es divisible por 3 si y solo si la suma de sus dígitos es divisible por 3.

Ejemplo

Sean a y b enteros cualesquiera y p un número primo, veamos que:

$$(a+b)^p \equiv a^p + b^p \pmod{p}.$$

En efecto, por el Teorema del Binomio, tenemos:

$$(a+b)^p = \sum_{k=0}^{p} \binom{p}{k} a^{p-k} b^k,$$

lo que implica:

$$(a+b)^p = a^p + \binom{p}{1} a^{p-1} b + \cdots + \binom{p}{p-1} a b^{p-1} + b^p.$$

Por lo tanto:

$$(a+b)^p - (a^p + b^p) = \binom{p}{1} a^{p-1} b + \cdots + \binom{p}{p-1} a b^{p-1} = tp,$$

puesto que los coeficientes binomiales $\binom{p}{k}$ con $k = 1, 2, \ldots, p-1$ son divisibles por p.
En consecuencia:

$$(a+b)^p \equiv a^p + b^p \pmod{p}.$$

Teorema (eliminación)

Si $ac \equiv bc \pmod{n}$ *y* $d = (c, n)$, *entonces:*

$$a \equiv b \pmod{\frac{n}{d}}.$$

Demostración: Por hipótesis, $n \mid (ac - bc)$, es decir, $c(a-b) = kn$ con k entero.
Por otra parte, como $d = (c, n)$, tenemos que $c = dC$ y $n = dN$, donde $(C, N) = 1$. Por lo tanto, tenemos:

$$dC(a-b) = kdN,$$

y entonces:

$$C(a-b) = kN.$$

Luego, $N \mid C(a-b)$, y como $(C, N) = 1$, entonces:

$$N \mid (a-b).$$

En otros términos, $a \equiv b \pmod{N}$, o sea:

$$a \equiv b \pmod{\frac{n}{d}}.$$

□

Teorema

Sean $n_1, n_2, \ldots, n_r$ *enteros positivos. Si para cada* $i = 1, \ldots, r$,

$$a \equiv b \pmod{n_i},$$

entonces:

$$a \equiv b \pmod{[n_1, \ldots, n_r]},$$

donde $[n_1, \ldots, n_r]$ *denota el mínimo común múltiplo de* $n_1, \ldots, n_r$.

Definición (Clase de equivalencia)

Para cada $a \in \mathbb{Z}$, representamos su clase de equivalencia por $\overline{a}$. donde $\overline{a}$ está definida por:

$$\begin{aligned}\overline{a} &= \{x \in \mathbb{Z} \mid x \equiv a \pmod{n}\} \\ &= \{x \in \mathbb{Z} \mid x = a + kn, \text{ para algún } k \in \mathbb{Z}\}.\end{aligned}$$

Note que $\overline{a} = \overline{b}$ si y solamente si $a \equiv b \pmod{n}$.

El conjunto de todos los $\overline{r}$ donde $0 \leq r < n$ es llamado las *clases residuales módulo n* y lo notamos así

$$\mathbb{Z}/(n),\ \mathbb{Z}/n\mathbb{Z},\ \mathbb{Z}/n \text{ o a veces } \mathbb{Z}_n.$$

Veamos ahora que el conjunto cociente de $\mathbb{Z}$ por esta relación está formado precisamente por las clases

$$\overline{0}, \overline{1}, \overline{2}, \ldots, \overline{n-1}.$$

En efecto, si a es un entero arbitrario, por el algoritmo de la división podemos representarlo en la forma

$$a = qn + r \quad \text{con } 0 \leq r < n,$$

luego:

$$a \equiv r \pmod{n} \quad \text{y en consecuencia } \overline{a} = \overline{r}.$$

Sobre $\mathbb{Z}_n$ podemos definir una adición y una multiplicación mediante las fórmulas siguientes:

$$\overline{x} + \overline{y} = \overline{x + y}, \quad \overline{x} \cdot \overline{y} = \overline{xy}.$$

Estas operaciones están bien definidas ya que siempre producen resultados que pertenecen a $\mathbb{Z}_n$.

Definición

Un grupo $(G, *)$ es un conjunto G provisto de una operación binaria $*$ que satisface las siguientes propiedades:

1. ***Propiedad clausurativa:*** *Para todo $a, b \in G$, el resultado de la operación $a * b$ pertenece a G, es decir:*

$$a * b \in G.$$

2. ***Propiedad asociativa:*** *Para todo $a, b, c \in G$, se cumple que:*

$$a * (b * c) = (a * b) * c.$$

3. ***Elemento neutro:*** *Existe un elemento $e \in G$ tal que para todo $a \in G$:*

$$a * e = e * a = a.$$

Este elemento se llama la identidad.

4. ***Elemento inverso:*** *Para cada $a \in G$, existe un elemento $a' \in G$ tal que:*

$$a * a' = a' * a = e,$$

Definición

Un grupo G se llama abeliano o conmutativo si satisface además la condición:

$$a * b = b * a \quad \textit{para todo } a, b \in G.$$

Definición

Un anillo $(A, +, \cdot)$ es un conjunto A provisto de dos operaciones, $+$ y $\cdot$, llamadas adición y multiplicación, que satisfacen los siguientes axiomas:

A-1 $(A, +)$ *es un grupo abeliano.*

A-2 *La multiplicación $\cdot$ es asociativa.*

A-3 *Las dos operaciones están relacionadas por las propiedades distributivas:*

$$a \cdot (b + c) = a \cdot b + a \cdot c, \quad (b + c) \cdot a = b \cdot a + c \cdot a,$$

para todo $a, b, c \in A$.

Definición

Un anillo conmutativo es un anillo donde la multiplicación es conmutativa, es decir, $a \cdot b = b \cdot a$ para todo $a, b \in A$.
Un anillo que además tiene una identidad para la multiplicación, usualmente representada por 1, se denomina anillo con identidad.

Proposición

$(\mathbb{Z}_n, +, \cdot)$ es un anillo conmutativo con identidad. La identidad de este anillo es precisamente $\overline{1}$. Este anillo se llama el anillo de los enteros módulo n.

Definición

Decimos que un anillo $(A, +, \cdot)$ *tiene divisores de cero si existen elementos* $a, b \in A$*, distintos de cero, pero tales que:*

$$ab = 0.$$

Por ejemplo el anillo $\mathbb{Z}_6$ tiene divisores de cero. También observamos que en este anillo no se cumple la ley cancelativa para la multiplicación, ya que tenemos, por ejemplo:

$$\overline{3} \cdot \overline{2} = \overline{3} \cdot \overline{4} \quad \text{pero} \quad \overline{2} \neq \overline{4}.$$

Proposición

Sean $a, n \in \mathbb{Z}$ *y* $n > 0$. *Entonces, existe* $b \in \mathbb{Z}$ *tal que:*

$$ab \equiv 1 \pmod{n}$$

si, y solo si, $\gcd(a, n) = 1$.

Decimos, por lo tanto, que a es *invertible* módulo n cuando $\gcd(a, n) = 1$, y llamamos a b, con $ab \equiv 1 \pmod{n}$, el *inverso multiplicativo* de a módulo n.
El inverso es siempre único módulo n: si $ab \equiv ab' \equiv 1 \pmod{n}$, tenemos:

$$b \equiv b \cdot 1 \equiv b \cdot (ab') \equiv (ba) \cdot b' \equiv 1 \cdot b' \equiv b' \pmod{n}.$$

Así, $\overline{b}$ está bien definido y, en términos de clases de congruencia, tenemos que:

$$\overline{a} \cdot \overline{b} = \overline{1}.$$

Denotamos $\overline{b}$ por $(\overline{a})^{-1}$.

Proposición (Caracterización clases residuales)

Sean $\overline{a} \in \mathbb{Z}_n$ Entonces $\overline{a}$ es una unidad o es un divisor de cero.

Definición (cuerpo)

Un cuerpo es un anillo conmutativo con identidad en el cual todo elemento distinto de cero tiene un inverso para la multiplicación.

Teorema

$\mathbb{Z}_n$ es un cuerpo si y solo si n es un número primo.