MATEMÁTICA DISCRETA

Aritmética Modular. Ecuaciones de Congruencia Lineal.

- Ecuaciones Diofánticas Lineales.
- Aritmética Modular. Ecuaciones de Congruencia Lineal.

Ecuaciones Diofánticas Lineales.

Ejercicio

Encuentra las soluciones de la ecuación diofántica $20x+50y=430$.

Solución: Como $mcd(20,50)=10$ y $10 \mid 430$, entonces la ecuación diofántica sí tiene soluciones.

Sol. particular: $(x_0, y_0) = (-86, 43)$.

Sol. general: $(x,y) = (-86+5k, 43-2k)$, $k \in \mathbb{Z}$.

Ejercicio

¿Es posible llenar exactamente un depósito de 25 litros con recipientes de 6 y 8 litros?

Solución:

x: número de recipientes de 6 litros a utilizar.

y: número de recipientes de 8 litros a utilizar.

$$6x+8y=25$$

Como $mcd(6,8)=2$ y 2 no divide a 25, entonces NO es posible.

Aritmética Modular. Ecuaciones de Congruencia Lineal.

Definición

Sea $n \in \mathbb{N}$ y $a, b \in \mathbb{Z}$. Decimos que a **es congruente con** b **módulo** n, y lo denotamos por $a \equiv b \pmod{n}$ si $n \mid a - b$. (si a y b dan el mismo resto cuando se divide entre n.)

Ejemplos:

- $17 \equiv 2 \pmod{5}$ ya que $5 \mid 15 = 17 - 2$.
- $-7 \equiv -49 \pmod{6}$ ya que $6 \mid 42 = -7 - (-49)$.

Propiedades

Sean a, b, c y n números enteros. Entonces

- $a \equiv b \pmod{n} \quad \rightarrow \quad a \cdot c \equiv b \cdot c \pmod{n}$.
- $a \equiv b \pmod{n}$ y $c \equiv d \pmod{n} \quad \rightarrow \quad a + c \equiv b + d \pmod{n}$.
- $a \equiv b \pmod{n}$ y $c \equiv d \pmod{n} \quad \rightarrow \quad a \cdot c \equiv b \cdot d \pmod{n}$.
- $a \equiv b \pmod{n} \quad \rightarrow \quad a^k \equiv b^k \pmod{n}$ con $k > 0$.
- $a \equiv b \pmod{n}$ y $d \mid n \quad \rightarrow \quad a \equiv b \pmod{d}$.
- $a \cdot c \equiv b \cdot c \pmod{n}$ y $d = mcd(c, m) \quad \rightarrow \quad a \equiv b \pmod{\frac{n}{d}}$.

Relación de equivalencia

Dado $n \in \mathbb{N}$, la relación de conguencia módulo n en $\mathbb{Z}$ es una relación de equivalencia.

Sean a, b y n números enteros. Entonces:

- $a \equiv a \pmod{n}$ (reflexiva).
- $a \equiv b \pmod{n} \leftrightarrow b \equiv a \pmod{n}$ (simétrica).
- $a \equiv b \pmod{n}$ y $b \equiv c \pmod{n} \rightarrow a \equiv c \pmod{n}$.

Clases de equivalencia

Dado $n \in \mathbb{N}$, para cada elemento $a \in \mathbb{Z}$, se define la clase de equivalencia:

$$[a]_n = \{x \in \mathbb{Z} : x \equiv a \pmod{n}\} = \{\ldots, a-2n, a-n, a, a+n, a+2n, \ldots\}$$

quedando $\mathbb{Z}$ dividido en n clases de equivalencia correspondientes a los posibles n restos de dividir un número cualquiera entre n:

$$[0]_n,\ [1]_n,\ \ldots,\ [n-1]_n$$

El conjunto $\mathbb{Z}_n$

Para cada $n \in \mathbb{N}$, el conjunto de las n clases de equivalencia lo denotamos por $\mathbb{Z}_n$, y se conoce como el conjunto de los enteros módulo n:

$$\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$$

donde los elementos $a \in \mathbb{Z}_n$ representan a sus respectivas clases de equivalencia módulo n.

Ejemplos: $\mathbb{Z}_2 = \{0, 1\}$, $\mathbb{Z}_6 = \{0, 1, 2, 3, 4, 5\}$.

Operaciones

- $[a]_n + [b]_n = [a+b]_n$
- $[a]_n - [b]_n = [a-b]_n$
- $[a]_n \cdot [b]_n = [a \cdot b]_n$

Tablas de multiplicar: $\mathbb{Z}_5$, $\mathbb{Z}_6$, $\mathbb{Z}_7$:

$\mathbb{Z}_5$	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

$\mathbb{Z}_6$	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

$\mathbb{Z}_7$	0	1	2	3	4	5	6
0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6
2	0	2	4	6	1	3	5
3	0	3	6	2	5	1	4
4	0	4	1	5	2	6	3
5	0	5	3	1	6	4	2
6	0	6	5	4	3	2	1

Resultados

- Se dice que $p \in \mathbb{Z}_n$ tiene **inverso** si existe $p^{-1} \in \mathbb{Z}_n$ tal que $p \cdot p^{-1} = 1$. (No siempre existe inverso en $\mathbb{Z}_n$).
- $p \in \mathbb{Z}_n$ tiene inverso en $\mathbb{Z}_n$ si y sólo si $mcd(p,n) = 1$.

¿Cómo calcular el inverso de $p \in \mathbb{Z}_n$ en $\mathbb{Z}_n$?

- Comprobar si existe p^{-1} en $\mathbb{Z}_n$ (comprobar si $mcd(p,n) = 1$)
- En caso afirmativo, usar la identidad de Bézout para obtenerlo:

  Existen $u, v \in \mathbb{Z}$ tal que:

  $$1 = mcd(p,n) = u \cdot p + v \cdot n \quad \rightarrow \quad p^{-1} \equiv u \pmod{n}.$$

Ejemplo: Calcula, si existe, 27^{-1} en $\mathbb{Z}_{34}$.

Solución: 27^{-1} en $\mathbb{Z}_{34}$ es 29.

Ecuación de congruencia lineal

Una ecuación de congruencia lineal es una ecuación del tipo

$$ax \equiv b \mod n$$

con $a, b \in \mathbb{Z}_n$, donde la solución (o soluciones) x se busca también en $\mathbb{Z}_n$.

Método de resolución

1. Si existe a^{-1} en $\mathbb{Z}_n$, existe una solución única que se obtiene multiplicando ambos lados por dicho inverso.
2. Si no existe a^{-1} en $\mathbb{Z}_n$, entonces $MCD(a, n) = d \neq 1$ y se tiene:
    1. Si d no divide a b no existe solución.
    2. si $d \mid b$ existe solución x en $\mathbb{Z}_n$, no necesariamente única, que se calcula mediante una ecuación diofántica.

NOTA: Resolver una ecuación de congruencia lineal consiste en hallar todas sus soluciones.

Ejemplo

Resuelve, si es posible, la ecuación $3x \equiv 1 \pmod{7}$.

Solución:

1. ¿ Existe 3^{-1} en $\mathbb{Z}_7$? Como $mcd(7,3) = 1$ entonces si existe 3^{-1} en $\mathbb{Z}_7$.
2. Calcular 3^{-1} en $\mathbb{Z}_7$. Usando la Identidad de Bézout, se obtiene que 3^{-1} en $\mathbb{Z}_7$ es 5.
3. Resolver la ecuación. $x \equiv 3^{-1} \cdot 1 \pmod{7} \quad \rightarrow \quad x \equiv 5 \pmod{7}$

Ejemplo

Resuelve, si es posible, la ecuación $3x \equiv 5 \pmod{9}$.

Solución:

1. ¿ Existe 3^{-1} en $\mathbb{Z}_9$? Como $mcd(9,3) = 3$ entonces NO existe 3^{-1} en $\mathbb{Z}_9$.
2. Por tanto, la ecuación no tiene solución.