MATEMÁTICA DISCRETA

Propiedades de los números enteros

- Principio del buen orden. Principio de Inducción Matemática.
- Divisibilidad. Números Primos.
- Algoritmo de la División. Notación en base b.

Principio del buen orden. Principio de Inducción Matemática.

$$\mathbb{Z} = \{..., -(n+1), -n, ..., -2, -1, 0, 1, 2, ..., n, n+1, ...\}$$

junto con las operaciones usuales de suma y producto satisface las siguientes propiedades:

- Op. internas: $\forall a, b \in \mathbb{Z}$ se tiene $a + b \in \mathbb{Z}$ y $a \cdot b \in \mathbb{Z}$.
- Conmutativas: $\forall a, b \in \mathbb{Z}$ se tiene $a + b = b + a$ y $a \cdot b = b \cdot a$.
- Asociativas: $\forall a, b, c \in \mathbb{Z}$ se tiene $(a + b) + c = a + (b + c)$ y $a \cdot (b \cdot c) = (a \cdot b) \cdot c$.
- Existencia de el. neutros: $\forall a \in \mathbb{Z}$ se tiene $a + 0 = a$ y $a \cdot 1 = a$.
- Existencia de el. opuesto para $+$: $\forall a \in \mathbb{Z}$, $\exists -a \in \mathbb{Z}$ tal que $a + (-a) = 0$.
- Distributiva: $\forall a, b, c \in \mathbb{Z}$ se tiene $a \cdot (b + c) = a \cdot b + a \cdot c$.

$$\mathbb{Z}^+ = \{x \in \mathbb{Z} : x > 0\} = \{x \in \mathbb{Z} : x \geq 1\}.$$

Principio del buen orden

Todo subconjunto no vacío de $\mathbb{Z}^+$ contiene un elemento que es el mínimo (Se dice que $\mathbb{Z}^+$ está *bien ordenado*).

Ejemplo

- El 2 es el mínimo en el conjunto formado por los números pares.
- El 1 es el mínimo de $\mathbb{Z}^+$,
- $\mathbb{R}^+$ no cumple el principio del buen orden.

Este principio sirve para distinguir $\mathbb{Z}^+$ de $\mathbb{R}^+$ o $\mathbb{Q}^+$.

Principio de Inducción Matemática

Sea $S(n)$ un enunciado matemático que depende de la variable $n \in \mathbb{Z}^+$.

(i) Si $S(1)$ es verdadero y;

(ii) Si siempre que $S(k)$ es verdadero (para algún $k \in \mathbb{Z}^+$ particular, pero elegido arbitrariamente), entonces $S(k+1)$ es verdadero;

entonces $S(n)$ es verdadero para todo $n \in \mathbb{Z}^+$.

- A la condición (i) se le llama *Paso base*.
- A la condición (ii) se le llama *Paso inductivo*.

Principio de Inducción matemática

Sea $S(n)$ un enunciado matemático que depende de la variable $n \in \mathbb{Z}^+$.

(i) Si $S(1)$ es verdadero y;

(ii) Si siempre que $S(k)$ es verdadero (para algún $k \in \mathbb{Z}^+$ particular, pero elegido arbitrariamente), entonces $S(k+1)$ es verdadero;

entonces $S(n)$ es verdadero para todo $n \in \mathbb{Z}^+$.

Demostración

Sea $S(n)$ un enunciado matemático que satisface las condiciones (i) y (ii).

Sea $F = \{x \in \mathbb{Z}^+ : S(x) \text{ es falso}\}$. Supongamos que $F \neq \emptyset$.

Por el Principio del buen orden, F tiene un elemento mínimo $s \in F$.

Por (i) se tiene que $S(1)$ es verdadero. Entonces $s > 1$, lo cual implica que $s-1 \in \mathbb{Z}^+$.Además observa que $s-1 \notin F$. ($S(s-1)$ es verdadero).

Por (ii) se tiene que $S((s-1)+1) = S(s)$ es verdadero, lo cual contradice el hecho de que $s \in F$.

Por tanto, $F = \emptyset$, y el teorema queda demostrado.

Ejercicio

Sea $n \in \mathbb{Z}^+$. Demuestra que $\sum_{i=1}^{n} i = \frac{n(n+1)}{2}$.

Demostración

Sea $S(n) : \sum_{i=1}^{n} i = \frac{n(n+1)}{2}$.

Observa que $S(1) : \frac{1 \cdot 2}{2} = 1$ es verdadero (Paso base).

Asumamos que $S(k)$ es verdadero, i.e., $S(k) : \sum_{i=1}^{k} i = \frac{k(k+1)}{2}$ es verdadero (hipótesis inductiva).

Necesitamos demostrar que $S(k+1)$ es verdadero (Paso inductivo).

Observa que: $S(k+1) : \sum_{i=1}^{k+1} i = (\sum_{i=1}^{k} i) + (k+1)$

$$= \frac{k(k+1)}{2} + (k+1)$$

$$= \frac{(k+1)(k+2)}{2}$$

Lo anterior implica que $S(k+1)$ es verdadero. Por tanto, por el Principio de Inducción Matemática, $S(n)$ es verdadero para todo $n \in \mathbb{Z}^+$.

Divisibilidad. Números Primos.

Definición

Sean $a, b \in \mathbb{Z}$ y $a \neq 0$. Diremos que *a divide a b* (y se escribe $a \mid b$) si existe un entero n tal que $b = an$.

En este caso, diremos que:

- a es un divisor de b.
- b es un múltiplo de a.

Teorema

Para cualesquiera $a, b, c \in \mathbb{Z}$,

(a) $1 \mid a \quad$ y $\quad a \mid 0$.

(b) Si $a \mid b \quad$ y $\quad b \mid a$, entonces $a = \pm b$.

(c) Si $a \mid b \quad$ y $\quad b \mid c$, entonces $a \mid c$.

(d) Si $a \mid b \quad$ y $\quad a \mid c$, entonces $a \mid (bx + cy)$ para todo $x, y \in \mathbb{Z}$.

Ejemplo

¿Existen enteros $x, y, z \in \mathbb{Z}$ tal que $6x + 9y + 15z = 107$?

Solución:

Supongamos que tales enteros $x, y, z \in \mathbb{Z}$ existen.

Como $3 \mid 6$, $3 \mid 9$ y $3 \mid 15$, entonces $3 \mid 107$, lo cual es falso.

Por tanto, NO existen $x, y, z \in \mathbb{Z}$ tal que $6x + 9y + 15z = 107$.

Ejemplo

Sean $a, b \in \mathbb{Z}$ tal que $2a + 3b$ es un múltiplo de 17. Demuestra que 17 divide a $9a + 5b$.

Solución:

Observa que si $17 \mid (2a + 3b)$, entonces $17 \mid [-4(2a + 3b)]$.

Por otra parte, $17 \mid (17a + 17b)$.

Por tanto, $17 \mid [-4(2a + 3b) + (17a + 17b)]$, i.e., $17 \mid (9a + 5b)$.

Definición

Sea $n > 1$ un entero positivo.

- Diremos que n es un número primo si sus únicos divisores positivos son 1 y n.
- Diremos que n es un número compuesto si NO es un número primo.

Ejemplo

- 100 es un número compuesto.
- 2 es un número primo.
- 11 es un número primo.
- 27 es un número compuesto.

Proposición

Si $n \in \mathbb{Z}^+$ es un número compuesto, entonces existe un número primo p tal que $p \mid n$.

Demostración:

- Sea S el conjunto de todos los compuestos que no tienen divisores primos.
- Supongamos que $S \neq \emptyset$. Por el Principio del buen orden, S tiene un elemento mínimo $m \in S$.
- Como m es un número compuesto, entonces $m = m_1 \cdot m_2$, donde $m_1, m_2 \in \mathbb{Z}^+$ $(1 < m_1 < m$ y $1 < m_2 < m)$.
- Como $m_1 \notin S$, entonces m_1 es un número primo o es un múltiplo de un número primo.
- Entonces, existe un primo p tal que $p \mid m$, una contradicción.
- Por tanto, $S = \emptyset$, lo cual implica que la declaración es verdadera.

Teorema(Euclides)

Existen infinitos número primos.

Teorema fundamental de la aritmética

Todo número entero positivo $n > 1$ o es un número primo o se puede descomponer como producto de números primos. Además, esta descomposición es única salvo el orden de los factores.

Ejemplo:

- 17 es un número primo.
- $21 = 3 \cdot 7$.
- $50 = 2 \cdot 5^2$.
- $64 = 2^6$.

Algoritmo de la División. Notación en base b.

Teorema(Algoritmo de la División)

Si $a, b \in \mathbb{Z}$ con $b > 0$, entonces existen dos únicos enteros $q, r \in \mathbb{Z}$ tal que:

$$a = bq + r, \;\; 0 \leq r < b.$$

Ejemplo:

- Si $a = 170$ y $b = 11$, entonces $170 = 15 \cdot 11 + 5$ $(q = 15$ y $r = 5)$.
- Si $a = 98$ y $b = 7$, entonces $98 = 14 \cdot 7$ $(q = 14$ y $r = 0)$.
- Si $a = -45$ y $b = 8$, entonces $-45 = (-6)8 + 3$ $(q = -6$ y $r = 3)$.

Notación Decimal

Si $n = a_k a_{k-1} \ldots a_1 a_0 \in \mathbb{Z}^+$, entonces:

$$n = a_0 + a_1 \cdot 10 + \cdots + a_{k-1} \cdot 10^{k-1} + a_k \cdot 10^k.$$

Sea $b \in \mathbb{Z}^+$, con $b > 1$. Todo número $n \in \mathbb{Z}^+$ se puede expresar de forma única como:

$$n = a_0 + a_1 \cdot b + a_2 b^2 + \cdots + a_{k-1} \cdot b^{k-1} + a_k \cdot b^k.$$

para un cierto $k \in \mathbb{Z}^+$, con $a_0, a_1, \ldots, a_k \in \mathbb{Z}^+$, $a_1, \ldots, a_k < b$ y $a_k \neq 0$.

En este caso, escribiremos $n = a_k a_{k-1} \ldots a_1 a_{0_b}$.

$b = 10 \rightarrow$ Notación decimal

$b = 16 \rightarrow$ Notación hexadecimal

$b = 2 \rightarrow$ Notación binaria

$b = 8 \rightarrow$ Notación octal

Algoritmo de expresión de un número natural n (decimal) en base b

1. Dividimos n entre b: $n = q_0 b + a_0, \quad 0 \leq a_0 < b$.
2. Dividimos q_0 entre b: $q_0 = q_1 b + a_1, \quad 0 \leq a_1 < b$, luego

$$n = (q_1 b + a_1)b + a_0 = q_1 b^2 + a_1 b + a_0.$$

3. Repetimos hasta tener $q_k = 0$: $q_1 = q_2 b + a_2, \quad 0 \leq a_2 < b$, luego

$$\begin{aligned} n =& (q_2 b + a_2)b^2 + a_1 b + a_0 = q_2 b^3 + a_2 b^2 + a_1 b + a_0 \\ =& (q_3 b + a_3)b^3 + a_2 b^2 + a_1 b + a_0 = \ldots \\ =& a_k b^k + a_{k-1} b^{k-1} + \ldots + a_2 b^2 + a_1 b + a_0 \\ =& a_k a_{k-1} \ldots a_2 a_1 a_{0_b}. \end{aligned}$$

Ejercicio

Expresa el número 6137 en base octal.

Solución:

$$6137 = a_0 + a_1 \cdot 8 + a_2 \cdot 8^2 + \cdots + a_{k-1} \cdot 8^{k-1} + a_k \cdot 8^k.$$

$$6137 = 1 \cdot 8^4 + 3 \cdot 8^3 + 7 \cdot 8^2 + 7 \cdot 8 + 1 = 13771_8.$$