

Conferencia 1 - Principios de la Teoría de Números

November 1, 2024

Principio del Buen Ordenamiento. *Todo subconjunto no vacío de \mathbb{Z}_+ contiene un elemento mínimo. O sea, $\exists(m)$ tal que $\forall(x)x \in A \wedge x \neq m$ se cumple que $m < x$*

Principio de Inducción Matemática. *Dada una proposición P , si se cumple $P(n_0)$ con $n_0 \in \mathbb{Z}_+$ y, además, $\forall(n) n \geq n_0 \wedge P(n) \Rightarrow P(n+1)$ entonces $\forall(n) n \geq n_0 \wedge P(n)$*

Teorema. *El Principio del Buen Ordenamiento es equivalente al Principio de Inducción Matemática*

Demostración

Sea C el conjunto de los números naturales que no cumplen P y asumamos que $P \neq \emptyset$. Entonces, por el **Principio del Buen Ordenamiento** existe $m \in C$ tal que m es el mínimo elemento de C .

Ahora, asumamos a 1 como n_0 , luego como $P(1)$ se cumple entonces $m > 1$ por lo que $m - 1 \geq 1$.

Como $m - 1 < m$ entonces $m - 1 \notin C$ por lo que $P(m - 1)$ se cumple. Por tanto, como para todo $n > 1$ se tiene que $P(n) \Rightarrow P(n + 1)$ entonces dado que $P(m - 1)$ se cumple se tendría que $P(m)$ también se cumple ¡lo que es una contradicción!

Ejemplo Demuestre, utilizando el **Principio del Buen Ordenamiento**, que para toda n , $n \in \mathbb{Z}$, $n \geq 1$ se cumple que $\sum_{k=1}^n (2k - 1) = n^2$

Sea C el conjunto de los números naturales que no cumplen P y asumamos que $P \neq \emptyset$. Entonces, por el **Principio del Buen Ordenamiento** existe $m \in C$ tal que m es el mínimo elemento de C .

$P(1)$ se cumple pues $\sum_{k=1}^1 (2k - 1) = 2 - 1 = 1 = 1^2$, por tanto $m > 1$ por lo que $m - 1 \geq 1$. Ahora, como $m - 1 \geq m$ entonces $m - 1 \notin C$ por lo que $P(m - 1)$ se cumple. Entonces $\sum_{k=1}^{m-1} (2k - 1) = (m - 1)^2$.

$$\begin{aligned} \text{Ahora se tiene que} \\ \sum_{k=1}^m (2k - 1) &= \sum_{k=1}^{m-1} (2k - 1) + (2m - 1) \\ \sum_{k=1}^m (2k - 1) &= (m - 1)^2 + (2m - 1) \\ \sum_{k=1}^m (2k - 1) &= (m^2 - 2m + 1) + (2m - 1) \\ \sum_{k=1}^m (2k - 1) &= m^2 \end{aligned}$$

O sea, $P(m)$ se cumple, lo que es una ¡contradicción!

Definición. Sean a, b , $a \in \mathbb{Z}$, $b \in \mathbb{Z}$, $a \neq 0$, se dice que a divide a b o que a es múltiplo de b , denotado $a|b$, si $\exists(q) q \in \mathbb{Z}$ tal que $b = a * q$

Lema. *Todo número a , $a \in \mathbb{Z}$, es divisor de 0*

Teorema. *Sean a, b , $a \in \mathbb{Z}$, $b \in \mathbb{Z}$, si $b|a$ y $a \neq 0$ entonces $a \geq b$*

Teorema. *La relación **ser divisor de** es transitiva. O sea, si $a|b$ y $b|c$ entonces $a|c$*

Demostración

Teorema. Algoritmo de la División, sean a, b , $a \in \mathbb{Z}$, $b \in \mathbb{Z}$, $a > 0$, entonces existen q, r , $q \in \mathbb{Z}$, $r \in \mathbb{Z}$, únicos tales que $b = a * q + r$ donde $0 \leq r < b$

Demostración

Definición. Sea $a \in \mathbb{Z}$ tal que $n > 1$, se dice que n es un **número primo** si y solo sus únicos divisores positivos son 1 y n , de lo contrario se dice que n es un **número compuesto**

Corolario. $n, n \in \mathbb{Z}, n > 1$, es un **número compuesto** si y solo si $n = a * b$ con $a \in \mathbb{Z}, b \in \mathbb{Z}, 1 < a \leq b < n$

Lema. Todo número entero mayor que 1 tiene un divisor primo

Demostración

Teorema. Hay una infinita cantidad de números primos

Demostración