Conferencia 1 - Principios de la Teoría de Números

February 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 $P \neq \varnothing$. 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 $P \neq \varnothing$. 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 $\sum_{k=1}^{m-1}(2k-1) = (m-1)^2$.

Ahora se tiene que

$\sum_{k=1}^{m}(2k-1) = \sum_{k=1}^{m-1}(2k-1) + (2m-1)$

$\sum_{k=1}^{m}(2k-1) = (m-1)^2 + (2m-1)$

$\sum_{k=1}^{m}(2k-1) = (m^2 - 2m + 1) + (2m-1)$

$\sum_{k=1}^{m}(2k-1) = m^2$

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

Definición. *Sean* a, b*,* $a \in \mathbb{Z}$*,* $b \in \mathbb{Z}$*, se dice que* c*,* $c \in \mathbb{Z}$*, es común divisor de* a *y* b *si* $c|a$ *y* $c|b$

Definición. *Sean* a, b*,* $a \in \mathbb{Z}$*,* $b \in \mathbb{Z}$*,* $a \neq 0$ *o* $b \neq 0$*, se denota* $mcd(a, b) = max\{d|d \in \mathbb{Z} \wedge d|a \wedge d|b\}$ *como el máximo común divisor de* a *y* b

El $mcd(a, b)$ también suele denotarse (a, b)

Propiedades. $mcd(a, b) = mcd(-a, b) = mcd(a, -b) = mcd(-a, -b)$

Teorema. *Sean* a, b*,* $a \in \mathbb{Z}$*,* $b \in \mathbb{Z}$*, si* $a|b$ *entonces* $mcd(a, b) = |a|$

Definición. *Sean* a, b*,* $a \in \mathbb{Z}$*,* $b \in \mathbb{Z}$*, si el* $mcd(a, b) = 1$ *entonces* a *y* b *son* ***primos relativos***

Definición. *Un entero* c *es combinación lineal de los enteros* $a_1, a_2, \ldots, a_n$ *si exiten enteros* $b_1, b_2, \ldots, b_n$ *tales que* $c = a_1 * b_1 + a_2 * b_2 + \ldots + a_b * b_n$

Teorema. *El máximo común divisor de* $a_1, a_2, \ldots, a_n$*, números enteros, no todos iguales a 0,* $mcd(a_1, a_2, \ldots, a_n)$ *es el menor entero positivo que puede ser expresado como combinación lineal de* $a_1, a_2, \ldots, a_n$

Demostración

Teorema. *Sean* a, b*,* $a \in \mathbb{Z}$*,* $b \in \mathbb{Z}$*, el conjunto de los divisores comunes de* a *y* b *coincide con el conjunto de los divisores del* $mcd(a, b)$

Corolario. *Si* $a_1, a_2, \ldots, a_n$ *son números enteros no todos iguales a 0 entonces* $mcd(a_1, a_2, \ldots, a_n) = mcd(a_!, mcd(a_2, a_3, \ldots, a_n))$

Corolario. *Sean* a, b*,* $a \in \mathbb{Z}$*,* $b \in \mathbb{Z}$*, no simultáneamente nulos, entonces* $\frac{a}{mcd(a.b)}$ *y* $\frac{b}{mcd(a.b)}$ *son* ***primos relativos****. O sea,* $mcd(\frac{a}{(a.b)}, \frac{b}{(a.b)}) = 1$

Teorema. *Sea* a*,* $a \in \mathbb{Z}$*,* $a \neq 0$*,* $b_i \in \mathbb{Z}$*,* $1 \leq i \leq n$*, si* $a|b_1 * b_2 * \ldots * b_n$ *y para todo* j*,* $1 \leq j \leq n - 1$*, se cumple que* $mcd(a, b_j) = 1$ *entonces* $a|b_n$

Corolario. *Sean* a, b, q, r *tales que* $a \in \mathbb{Z}$*,* $b \in \mathbb{Z}$*,* $q \in \mathbb{Z}$*,* $r \in \mathbb{Z}$*,* $b \neq 0$*, y* $a = q * b + r$ *entonces* $mcd(a, b) = mcd(b, r)$

Demostración

Definición. *Sean* a, b, c*,* $a \in \mathbb{Z}$*,* $b \in \mathbb{Z}$*,* $c \in \mathbb{Z}$*,* $a \neq 0$*,* $b \neq 0$ *se dice que* $ax + by = c$ *es una ecuación lineal diofantina si esta es resuelta con* $x \in \mathbb{Z}$ *y* $y \in \mathbb{Z}$

Teorema. *La ecuación lineal $ax+by=c$ tiene solución si y solo si $mcd(a,b)|c$*

Demostración

Teorema. ***Algoritmo de Euclides**. Sean a, b, $a \in \mathbb{Z}$, $b \in \mathbb{Z}$, $a > b$, si se realizan los siguientes cálculos:*
$a = q_1 * b + r_1 \; 0 \leq r_1 < b$
$b = q_2 * r_1 + r_2 \; 0 \leq r_2 < r_1$
$r_1 = q_3 * r_2 + r_3 \; 0 \leq r_3 < r_2$
$r_2 = q_4 * r_3 + r_4 \; 0 \leq r_4 < r_3$
$\ldots$
$\ldots$
$\ldots$
$r_{k-2} = q_k * r_{k-1} + r_k \; 0 \leq r_k < r_{k-1}$
$r_{k-1} = q_{k+1} * r_k \; 0 = r_{k+1}$
donde r_k es el último resto diferente de 0, entonces $r_k = mcd(a,b)$

Ejemplo Para calcular el máximo común divisor de 3088 y 456:
$3088 = 6 * 456 + 352$
$456 = 1 * 352 + 104$
$352 = 3 * 104 + 40$
$104 = 2 * 40 + 24$
$40 = 1 * 24 + 16$
$24 = 1 * 16 + 8$
$16 = 2 * 8 + 0$
Entonces 8 es el último resto distinto de 0. Por tanto $mcd(3088, 456) = 8$

A partir del **Algoritmo de Euclides** también se puede calcular la combinación lineal de la siguiente forma:
$A_1 = 1 \; B_1 = -q_k$
$A_2 = B_1 \; B_2 = A_1 - q_{k-1} * B_1$
$\ldots$
$A_{i+1} = B_i \; B_{i+1} = A_i - q_{k-i} * B_i$
$\ldots$
$A_{k-1} = B_{k-2} \; B_{k-1} = A_{k-2} - q_2 * B_{k-2}$
$A_k = B_{k-1} \; B_k = A_{k-1} - q_1 * B_{k-1}$
Luego $r_k = a * A_k + b * B_k$ y, por lo tanto, $r_k = a * A_k + b * B_k = mcd(a,b)$

Ejemplo Para calcular la combinación lineal de 3088 y 456 con la que se obtiene su mcd se tiene:
$3088 = 6 * 456 + 352 \; A_1 = 1 \; B_1 = -1$
$456 = 1 * 352 + 104 \; A_2 = -1 \; B_2 = 1 - 1 * (-1) = 2$
$352 = 3 * 104 + 40 \; A_3 = 2 \; B_3 = -1 - 2 * 2 = -5$
$104 = 2 * 40 + 24 \; A_4 = -5 \; B_4 = 2 - 3 * (-5) = 17$
$40 = 1 * 24 + 16 \; A_5 = 17 \; B_5 = -5 - 1 * 17 = -22$
$24 = 1 * 16 + 8 \; A_6 = -22 \; B_6 = 17 - 6 * (-22) = 149$
$16 = 2 * 8 + 0$
Por tanto $8 = mcd(3088, 456) = 3088 * (-22) + 456 * 149$

Teorema. *Si x_0, y_0 son una solución de la ecuación diofantina $ax + by = c$ entonces $x = x_0 + k\frac{b}{(a,b)}$ y $y = y_0 - k\frac{a}{(a,b)}$ con $k \in \mathbb{Z}$*

Demostración

Definición. *Sean a, b, c, $a \in \mathbb{Z}$, $b \in \mathbb{Z}$, $c \in \mathbb{Z}$, los tres distintos de 0, se dice que c es múltiplo común de a y b si c es múltiplo de a y c es múltiplo de b. Se dice que c es el mínimo común múltiplo de a y b, si es el menor entero positivo múltiplo común de de a y b, lo que se denota $mcm(a, b)$.*

El $mcm(a, b)$ también suele denotarse $[a, b]$

Teorema. *Sean a, b, $a \in \mathbb{Z}_+$, $b \in \mathbb{Z}_+$, todo múltiplo común de a y b se expresa como $k\frac{a*b}{(a,b)}$ donde $k \in \mathbb{Z}$*

Corolario. *El $mcm(a, b) = \frac{|a*b|}{mcd(a,b)}$, lo que es lo mismo $(a, b) = \frac{|a*b|}{[a,b]}$*

Corolario. *Todo múltiplo común de a y b es múltiplo común de $[a, b]$*