Conferencia 1 - Principios de la Teoría de Números

September 9, 2025

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 (PBO) es equivalente al Principio de Inducción Matemática (PIM)*

Demostración que el Principio del Buen Ordenamiento implica al Principio de Inducción Matemática

Demostremos que el PBO implica PIM

Sea C el conjunto de los números naturales que no cumplen P.

Asumamos que $C \neq \varnothing$.

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! Entonces C es vacío y se cumple para todos.

Se debe demostar también que el PIM implica PBO

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.

Asumamos que $C \neq \varnothing$.

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 $m > m - 1$ 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! Luego, C es vacío y se cumple para todos.

Definición. *Sean* a, b*,* $a \in \mathbb{Z}$*,* $b \in \mathbb{Z}$*,* $a \neq 0$*, se dice que* a *divide a* b *o que* b *es múltiplo de* a*, 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

Se debe demostrar que si $a|b$ y $b|c$ entonces $a|c$

Como $a|b$ entonces existe $q_1, q_1 \in \mathbb{Z}$ tal que $b = aq_1$ Del mismo modo, como $b|c$ existe $q_2, q_2 \in \mathbb{Z}$ tal que $c = bq_2$

Ahora, como $c = bq_2 = aq_1q_2$ entonces tomando $q = q_1q_2 \in \mathbb{Z}$ se tiene entonces que $c = a * q$ y, por tanto, $a|c$

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

Demostración

Por una parte, si $b|a$ entonces existe $q \in \mathbb{Z}$ tal que $a = bq$, luego, para este caso con $r = 0$ se cumple que $a = bq + r$

En el otro caso, si $b \nmid a$ entonces se puede construir el conjunto

$S = \{a - sb | a - sb > 0, s \in \mathbb{Z}\}$, noten que este es el conjunto los posibles r.

Ahora se debe demostrar que S no es vacío.

Veamos para $a > 0$, entonces para este caso se toma $s = 0$ y es evidente aquí que el conjunto posee al menos al elemento a.

Para $a < 0$ tomamos a $s = a - 1$ y por tanto

$a - sb = a - (a - 1)b$

$a - sb = a - ab - b$

$a - sb = a(1 - b) + b$

Como $a < 0$ y $1 - b < 0$ (pues $b > 0$ y $b \nmid a$) entonces $a(1 - b)$ es mayor que 0 y, por tanto, $a(1 - b) + b$ también lo es.

Luego, sea r el elemento mínimo de S y sea $s = q$ se tiene que $a - bq = r$ entonces $a = bq + r$

Ahora se debe demostrar que $0 \leq r < b$.

Se sabe que $r = a - sb > 0$

Supongamos que $r > b$ por tanto

$r - b > 0$ y como $r = a - bq$ entonces $r - b = a - qb - b > 0$ y estos es lo mismo que $r - b = a - q(b + 1) > 0$, luego $r - b \in \mathbb{Z}$ y como $r > r - b$ esto es una contradicción pues r era el elemento mínimo de S.

Ahora se debe demostrar que q y r son únicos.

Supongamos que existen q_1, r_1 tal que $q_1 \neq q$ o $r_1 \neq r$ y $a = bq_1 + r_1 = bq + r$

Entonces $b(q - q1) = r_1 - r$

y como se cumple que $0 \leq r < b$ y $0 \leq r_1 < b$

se tiene que $-b < r_1 - r < b$ y, por tanto,

$-b < b(q - q_1) < b$

$-1 < q - q_1 < 1$

Como $q - q_1 \in \mathbb{Z}$ ello implica que $q - q_1 = 0$ y $q = q_1$ por tanto $r = r_1$ y esto es una contradicción, luego q y r son únicos.

Definición. *Sea $n \in \mathbb{Z}$ tal que $n > 1$, se dice que n es un **número primo** si y solo si 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
Demostración 1
Para $n > 1$
Si n es primo ya está demostrado.
Si n no es primo es compuesto, entonces $n = ab$, $1 < a, b < n$
Si a es primo o b es primo ya queda demostrado.
Sino a es compuesto y es de la forma $a = a_1 b_1$, $1 < a_1, b_1 < a$
...
...
Como no existe descenso infinito para números positivos, este proceso debe terminar encontrando un número a_i primo que por transitividad divide a n.
Demostración 2
Para $n = 3$ se cumple.
Luego hasta $n - 1$ se cumple.
Entonces si n es primo ya, sino $n = ab$, $1 < a, b < n$.
Si a es primo se cumple sino a es compuesto y como $a < n$ entonces tiene divisores primos los que, por transitividad, también lo son de n.
Demostración 3
Si n es primo, ya está demostrado. Sino, se tiene $D = \{d | \, d|n, 1 < d < n\}$ y sea m el mínimo elemento de D.
Supongamos que m es compuesto, luego existe $p < m$ tal que $p|m$, entonces por transitividad $p|n$ y $p < m$, y esto es un contradicción. Luego m es primo.

Teorema. *Hay una infinita cantidad de números primos*

Demostración
Si tenemos el conjunto de k números primos distintos,$A = \{p_1, p_2, \ldots, p_k\}$ entonces tomemos $m = p_1 p_2 \ldots p_k + 1$
Ahora, si $p_i | m (1 \leq i \leq k)$ como $p_i | p_1 p_2 \ldots p_k$ entonces $p_i | 1$ lo que es una contradicción.
Luego, existe q primo tal que $q|m$ y $q \notin A$