Teoria de Numeros

Christian Cardenas

Table of Contents

1. Información

Profesor: Carlos Andres Giraldo Hernandez

Notas:

Corte 1		
Taller	10%	?
Quiz	5%	11 Sep
Parcial	20%	25 Sep
Corte 2		
Taller	10%	?
Quiz	5%	16 Oct
Parcial	20%	30 Oct
Corte 3		
Parcial	30%	1 Dec

Tutorías: Jueves 10-12, Viernes 8-10 (Biblioteca)

Contenidos:
- Números Naturales
- Números Entero
- Numero Primos
- Divisibilidad
- Teorema Fundamental de la Aritmética
- Congruencias
- Teorema Chino del residuo
- Funciones de la Teoría de Números
- Ecuaciones Diofánticas

Bibliografía: ?

- Niven. I, Zuckerman. N, and Montgomery. H.L, An Introduction to the Theory of Numbers.
- T. Koshy, Elementary Number Theory with applications.

2. Clase 2025-08-25

2.1. Principio del buen orden | PBO

Definición 2.1 **Principio del buen orden**

Todo subconjunto no vació de los números naturales tiene mínimo

2.2. Algoritmo de la division

Algoritmo 2.2 **Algoritmo de la division**

Sean $a, b \in \mathbb{Z}$ con $b > 0$. Entonces existen $q, r \in \mathbb{Z}$ únicos tal que:

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

Ejemplo **Algoritmo 2.2**

- $-3, 7 : \quad -3 = 7(-1) + 4, \quad 0 \leq 4 < 7$
- $0, 6 : \quad 0 = 6(0) + 0, \quad 0 \leq 0 < 6$

Demostración del Algoritmo 2.2:

Sea $S = \{a - bx : x \in \mathbb{Z} \land a - bq \geq 0\} \subseteq \mathbb{N}$

Comprobamos que $S \neq \emptyset$
- Si $a \geq 0$:
  Sea $x = -1$, entonces $a - b(-1) = a + b$, ahora $a + b \geq 0$, tal que $a - b(-1) \in S$
- Si $a < 0$:

$$a - ba = a(1 - b) \quad \begin{cases} b = 0 \Longrightarrow a(1 - b) = 0 \\ b > 1 \Longrightarrow 1 - b < 0 \end{cases}$$

$$1 - b < 0 \land a < 0 \Longrightarrow a(1 - b) \geq 0$$

  Como $a - ba \geq 0 \Longrightarrow a - ba \in S$

Como S es un subconjunto no vació de $\mathbb{N}$ por el PBO, S tiene mínimo.
Sea $r = \min(S)$. Luego, existe $q \in \mathbb{Z}$ tal que $a - bq = r \Longrightarrow a = bq + r$

Comprobamos unicidad de q, r
- Como el mínimo es único, r es único.
- Supongamos que existe $q' \in \mathbb{Z}$, tal que $a - bq' = r$

$$\left.\begin{array}{l} a - bq = r \\ a - bq' = r \end{array}\right\} \quad a - bq = a - bq'$$

$$\begin{aligned} a - bq &= a - bq' \\ -bq &= -bq' \\ 0 &= bq - bq' \\ 0 &= b(q - q') \quad \begin{cases} b = 0 \text{ Falso} \\ q - q' = 0 \implies \boxed{q = q'} \end{cases} \end{aligned}$$

□

2.3. Principio de inducción matemática (débil) | PIM(D)

Definición 2.3 **PIM(D)**

Sea $S \subseteq \mathbb{N}$ que satisface

1. $\overbrace{0 \in S}^{\text{Paso base}}$
2. $\overbrace{\underbrace{n \in S}_{\text{HI}} \implies n + 1 \in S}^{\text{Paso Inductivo}}$

Entonces $S = \mathbb{N}$

Ejemplo **Definición 2.3**

$$1 + r + r^2 + \ldots + r^n = \frac{1 - r^{n+1}}{1 - r}, \quad r \in \mathbb{R} \setminus \{1\}$$

Demostración: Prueba por inducción matemática

$$S = \left\{ n \in \mathbb{N} : 1 + r + r^2 + \ldots + r^n = \frac{1 - r^{n+1}}{1 - r} \right\}$$

1. Paso Base

$$r^0 = 1 = \frac{1 - r^{0+1}}{1 - r} = \frac{1 - r}{1 - r} \implies 0 \in S$$

2. Paso Inductivo:

Supongamos que $n \in S$, es decir

$$1 + r + r^2 + \ldots + r^n = \frac{1 - r^{n+1}}{1 - r} \quad \text{(HI)}$$

Ahora verificamos comprobamos para $n + 1$

$$\begin{aligned}
\underbrace{1 + r + r^2 + \ldots + r^n}_{\text{HI}} + r^{n+1} &= \frac{1 - r^{(n+1)+1}}{1 - r} \\
\frac{1 - r^{n+1}}{1 - r} + r^{n+1} &= \frac{1 - r^{n+2}}{1 - r} \\
\frac{1 - r^{n+1} + (1 - r)r^{n+1}}{1 - r} &= \frac{1 - r^{n+2}}{1 - r} \\
\frac{1 - \cancel{r^{n+1}} + \cancel{r^{n+1}} - r^{n-2}}{1 - r} &= \frac{1 - r^{n+2}}{1 - r} \\
\frac{1 - r^{n-2}}{1 - r} &= \frac{1 - r^{n+2}}{1 - r}
\end{aligned}$$

Entonces $n + 1 \in S$

Por lo tanto $S = \mathbb{N}$ □

Ejemplo **Definición 2.3**

$$3 | n^3 - n$$

Sea $S = \{n \in \mathbb{Z} : 3 | n^3 - n\}$

1. Paso Base

   $0^3 - 0 = 0 \wedge 3 | 0 \Longrightarrow 0 \in S$

2. Paso Inductivo

   Supongamos que $n \in S \Longrightarrow 3 | n^3 - n$

   Verificamos para $n + 1$

$$\begin{aligned}
(n + 1)^3 - (n + 1) &= n^3 + 3n^2 + 3n + \cancel{1} - n - \cancel{1} \\
&= n^3 - n + 3n^2 + 3n \\
&= (n^3 - n) + 3(n^2 + n)
\end{aligned}$$

   $\overbrace{3 | n^3 - n}^{\text{Por HI}} \wedge 3 | 3(n^2 - n) \Longrightarrow 3 | (n^3 - n) + 3(n^2 - n)$

   Luego $n + 1 \in S$

Por lo tanto $S = \mathbb{N}$

2.4. Ejercicios

Ejercicio 2.4

Demuestre que dadas $a, b \in \mathbb{Z}$ con $b \neq 0$, existen $q, r \in \mathbb{Z}$ unicos tal que

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

Demostración:

- Si $a \geq 0 \land$

$\square$

Ejercicio 2.5

Porque no es posible dividir por 0 en $\mathbb{Z}$?

Ejercicio 2.6

Demuestre que no hay enteros entre 0 y 1

Ejercicio 2.7

Se definen los números F_n de Fermat por $F_n = 2^{2^n} + 1, n = \{0, 1, 2, ...\}$

Demuestre que para todo $n \geq 1$

$$F_0 F_1 F_2 ... F_{n-1} + 2 = F_n$$

Ejercicio 2.8

Demuestre que $54 | 2^{2n+1} - 9n^2 + 3n - 2$

3. Clase 2025-08-28

3.1. PBO $\iff$ PIM(D)

Teorema 3.1

El Principio del buen orden es equivalente al Principio de inducción matemática

Demostración del Teorema 3.1: $\text{PBO} \iff \text{PIM(D)}$

1. $\text{PBO} \implies \text{PIM(D)}$: Sea $S \subseteq \mathbb{N}$, tal que
   1. $0 \in S$
   2. Si $n \in S$, entonces $n + 1 \in S$.

   Supongamos que $S \subsetneq \mathbb{N}$. Como S es no vació y $S \subsetneq \mathbb{N}$, S^c no es vació, luego por PBO, S_c tiene mínimo, Sea $m = \min(S)$. Veamos que $m - 1 \in S$. Si $m - 1 \notin S \implies m - 1 \in S^c$. Como $m - 1 < m$, entonces m no seria el minimo de S_c. Luego $m - 1 \in S$.

   Por *2.* Se tiene que $(m - 1) + 1 = m \in S$ lo cual es una contradiccion $\rightarrow\leftarrow$
2. $\text{PIM(D)} \implies \text{PBO}$: Sea $S \subseteq \mathbb{N}$ no vacio.

   Caso 1 ($0 \in S$): Entonces $\min(S) = 0$

   Caso 2 ($0 \notin S$): Sea $T = \{x \in \mathbb{N} : \forall s \in S, \quad x < s\} \subseteq S^c$. Como 0 es cota inferior de S y $0 \notin S$, entonces $0 \in T$, ademas $T \neq \mathbb{N}$, para T se satifase *1.* ($0 \in T$), si *2.* es satisfecho por T, entoncecs por el PIM(D) se concluye que $T = \mathbb{N}$ lo cual es una contradiccion $\rightarrow\leftarrow$

Por lo tanto $\text{PBO} \iff \text{PIM(D)}$ □

3.2. Principio de inducción matemática (general) | PIM(G)

Definición 3.2 **PIM(G)**

Sea $S \subseteq \{x \in \mathbb{N} : x \geq k\} = \mathbb{N} \geq k$ que satisface

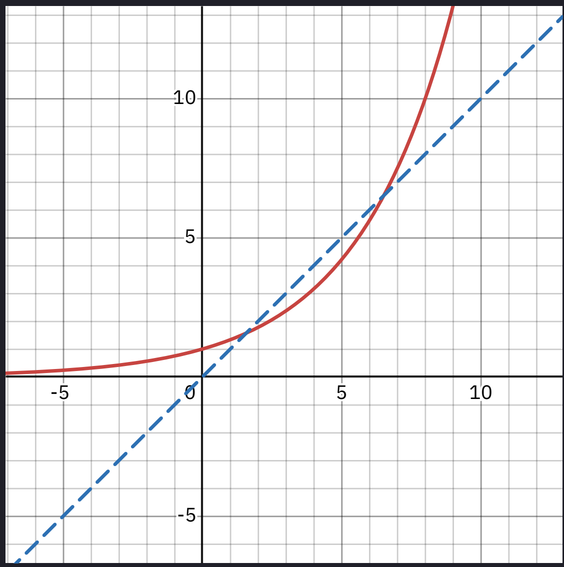
1. $k \in S$
2. Si $n \in S$, entonces $n + 1 \in S$

Entonces $S = \mathbb{N}_k = \{k, k + 1, k + 2, \dots\}$

Ejemplo **PIM(G)**

Demuestre que $\left(\frac{4}{3}\right)^n > n$

n	$\left(\frac{4}{3}\right)^n > 0$
0	$1 > 0$
1	$1.33 > 1$
2	$1.71 \ngtr 2$
3	$2.37 \ngtr 3$
4	$3.16 \ngtr 4$
5	$4.21 \ngtr 5$
6	$5.62 \ngtr 6$
7	$7.49 > 7$
8	$9.99 > 8$



Demostración:

Caso Base: $n = 7$, $\left(\frac{4}{3}\right)^7 \approx 7.49 > 7$

Paso Inductivo: Supongamos que $\left(\frac{4}{3}\right)^k > k$ para $k \geq 7$ (HI)

$$\left(\frac{4}{3}\right)^k > k$$

$$\left(\frac{4}{3}\right)\left(\frac{4}{3}\right)^k > \frac{4}{3}k$$

$$\left(\frac{4}{3}\right)^{k+1} > \left(1 + \frac{1}{3}\right)k$$

$$\left(\frac{4}{3}\right)^{k+1} > k + \frac{k}{3}$$

Como $k \geq 7$, entonces $\frac{k}{3} \geq \frac{7}{3} > 1$, ahora $k + \frac{k}{3} > k + 1$ por lo tanto

$$\left(\frac{4}{3}\right)^{k+1} > k + 1$$

$\square$

3.3. Principio de inducción matemática (fuerte) | PIM(F)

Definición 3.3 **PIM(F)**

Sea $S \subseteq \mathbb{N}_{\geq k} = \{k, k+1, k+2, ...\}$ tal que

1. $k \in S$
2. Cada vez que $m \in S$, entonces $m + 1 \in S$ para $m \geq k$

Entonces $S = \mathbb{N}$