NUMEROS ENTEROS

Cota inferior (definición): *Definición**

Un número n Es una cota inferior de un conjunto si es menor o igual que todos los elementos del conjunto. Todos los números $\leq n$ serán también cotas inferiores incluido n.
Ejemplo: $A = \{2, 5\}$, el 2 (y todos los números ≤ 2) son cotas inferiores del Conjunto$A$.

Mínimo (definición): *Definición**

Es el mayor de las cotas inferiores.
Ejemplo: $A = \{2, 5\}$, el 2 es la mayor cota inferior y pertenece a A entonces es el mínimo del conjunto.

Axiomas de ordenación:

Con a, b, c enteros arbitrarios:

- **(I8)** Ley de tricotomía:
  Vale una y solo una de las siguientes relaciones: $a < b, a = b, b < a$.
- **(I9)** Ley transitiva:
  Si $a < b$ y $b < c$, entonces $a < c$.
- **(I10)** Compatibilidad de la suma con el orden:
  Si $a < b$, entonces $a + c < b + c$.
- **(I11)** Compatibilidad de producto con el orden:
  Si $a < b$ y $0 < c$, entonces $ac < bc$.

Axioma de buena ordenación:

Si X es un subconjunto de Z que no es vacío y tiene cota inferior, entonces X tiene un mínimo.
Explicación: Dado un conjunto de números no enteros S, podemos decir que S tendrá cotas inferiores pero no mínimo, ya que si una cota inferior es 1, puedo elegir infinitamente números racionales cercanos a 1 sin llegar a 1.

Enunciado del principio de inducción (pág. 18): *Enunciado**

Sea $P(n)$ una propiedad para $n \in N$ tal que

a. $P(n_0)$ es verdadera. *(Caso Base)*

b. Para todo $k \in N$, $P(k)$ verdadera, implica $P(k + 1)$ verdadera *(Caso Inductivo)*
Entonces $P(n)$ es verdadera para todo $n \in N$

Enunciado del principio de inducción completa (pág. 20): *Enunciado**

Sea $n_0$un número y $P(n)$ una propiedad para $n \geq n_0$ tal que:

a. $P(n_0)$ es verdadera *(Caso Base).*

b. Si $P(n)$ es verdadera para todo h tal que $n_0 \leq h \leq k$ entonces $P(k + 1)$ es verdadera *(Caso Inductivo)*
Entonces $P(n)$ es verdadera para todo $n \geq n_0$.

Definiciones recursivas (pág. 15): *Definiciones**

Sea $n \in N$ y sea a_i una secuencia de números con $1 \leq i \leq n$

- Sumatoria:

$$\sum_{i=1}^{1} a_i = a_1, \quad \sum_{i=1}^{n} a_i = a_n + \sum_{i=1}^{n-1} a_i \qquad (n \geq 2)$$

- Productoria:

$$\prod_{i=1}^{1} a_i = a_1, \quad \prod_{i=1}^{n} a_i = a_n \cdot \prod_{i=1}^{n-1} a_i \text{ para } (n \geq 2)$$

- Factorial:

$$1! = 1, \qquad n! = n \cdot (n-1)! \text{ para } (n \geq 2)$$

- Potenciación:

$$x^0 = 1, \qquad x^1 = x, \qquad x^n = x \cdot x^{(n-1)} \qquad \text{para}(n \geq 2)$$

Propiedades de la potencia (pág 21): *Demostraciones**

- $x^n \cdot x^m = x^{n+m}$ (Demostracion por Induccion en m)
- $(x^n)^m = x^{n \cdot m}$ (Demostracion por Induccion en m)

CONTEO

Número combinatorio (pág. 32): *Definición**

Sean $n,\ m\ \in N_0$ tal que $m \leq n$. Definimos el número $\binom{n}{m}$ (número combinatorio) como la cantidad de subconjuntos de m elementos que tiene un conjunto de n elementos (cantidad de formas de elegir m elementos de un conjunto de n elementos). **No importa el orden!!**

- Fórmula: $\binom{n}{m} = \frac{n!}{(n-m)!\ m!}$
- Importante saber:
  - $\binom{n}{0} = \binom{0}{0} = 1$
  - $\binom{n}{1} = \binom{n}{n-1} = n$
  - $\binom{n}{m} = 0;$ para $m > n$

Simetría del número combinatorio (pág. 33): *Enunciado**

Sean $n,\ m\ \in N_0$ tal que $m \leq n$. Entonces:

$$\binom{n}{n-m} = \binom{n}{m}$$

Demostración:

$$\binom{n}{n-m} = \frac{n!}{(n-(n-m))!\ (n-m)!} = \frac{n!}{m!\ (n-m)!} = \frac{n!}{(n-m)!\ m!} = \binom{n}{m}$$

Cálculo de número combinatorio por el triángulo de Pascal (pág. 34): *Enunciado**

Sean $n,\ m\ \in N_0$ tal que $m \leq n$. Entonces:

$$\binom{n+1}{m} = \binom{n}{m-1} + \binom{n}{m}$$

Demostración explicada en el apunte.

Teorema de Binomio (pág. 36): *Enunciado**

Sean n un entero positivo. El coeficiente de término $a^{n-r}b^r$ en el desarrollo de $(a\ +\ b)^n$ es el número binomial $\binom{n}{i}$. Explícitamente: $(a\ +\ b)^n = \sum_{i=0}^{n} \binom{n}{i} \cdot a^{n-i}b^i$

Ejemplo $\sum_{i=0}^{n} \binom{n}{i} = 2^n$ **(pág. 39):** *Demostración**

Demostración:

Observar que $2^n = (1\ +\ 1)^n$ y $1^n = 1$. Entonces, por teorema de binomio:

$$2^n = (1\ +\ 1)^n = \sum_{i=0}^{n} \binom{n}{i} 1^{n-i} \cdot 1^i = \sum_{i=0}^{n} \binom{n}{i} \cdot 1 \cdot 1 = \sum_{i=0}^{n} \binom{n}{i} = 2^n$$

DIVISIBILIDAD

Enunciado de algoritmo de división (pág. 41): *Enunciado**

Sean a y b números enteros cualesquiera, con $b \in N$, entonces existen enteros únicos q y r tales que $a = b \cdot q + r$ con $0 \leq r < b$.

Definición de "divide a" (pág. 45): *Definición**

Dados dos enteros x e y decimos que y es un divisor de x y lo escribimos como $x|y$, si y sólo si $x = y \cdot q$, con $q \in Z$ es decir que cuando aplicamos el algoritmo de división el resto (r) es igual a 0

Propiedades de "divide a" (pág. 45): *Demostración**

a. $1|a,$ $\quad a|0,$ $\quad a| \pm a.$

Se puede demostrar de la siguiente forma:

$a = 1 \cdot a,$ $\quad 0 = a \cdot 0,$ $\quad \pm a = a \cdot (\pm 1)$

b. Si $a|b$, entonces $a|(bc)$ para cualquier c

Si decimos que b es múltiplo de a, cuando multipliquemos a b por c seguirá siendo múltiplo, $b = aq$, si multiplicamos ambos miembros de la igualdad por c y aplicando asociatividad, obtenemos $bc = a(qc)$, lo cual implica que $a|(bc)$

c. Si $a|b$ y $a|c$, entonces $a|(b + c)$

Como $a|b$, entonces existe una k, tal que $b = ak$, y como $a|c$, entonces existe una k' tal que $c = ak$'. Entonces $(b + c) = (ak)(ak')$, aplicando factor común obtenemos $(b + c) = a(k + k')$, se sigue que $a|(b + c)$.

d. Si $a|b$ y $a|c$, entonces $a|(rb + sc)$ para cualquier $r, s \in Z$

Como $a|b$, entonces existe una k, tal que $b = ak$, multiplicando ambos términos por r obtenemos $rb = akr$. Como $a|c$, entonces existe una k' tal que $c = ak$', multiplicando ambos términos por s obtenemos $sc = ak's$. Entonces $(rb + sc) = (akr) + (ak's)$, aplicando factor común obtenemos $(rb + sc) = a(rk + sk')$, se sigue que $a|(rb + sc)$

Definición de máximo común divisor (pág. 46): *Definición**

Si a y b son enteros algunos de ellos no nulo, decimos que un entero no negativo d es un máximo común divisor o MCD de a y b si:

a. $d|a$ y $d|b$ (común divisor)
b. si $c|a$ y $c|b$ entonces $c|d$ (máximo divisor)

- **Proposición 3.3.4 (pág. 48):**

  Sean $a, b \in Z$ con alguno de ellos no nulo. Entonces existen $s, t \in Z$ tal que: $(a, b) = sa + tb$

- **Corolario 3.3.5 (pág. 48):** *Demostración**

  Sean a y b enteros, b no nulo, entonces: $(a, b) = 1 \Leftrightarrow$ existen $s, t \in Z$ tal que $1 = sa + tb$

  ($\Rightarrow$) Es consecuencia trivial de la proposición anterior.

  ($\Leftarrow$) Sea $d = (a, b)$, entonces $d|a$ y $d|b$ y por lo tanto, $d|(sa + tb)$para cualesquiera $s, t \in Z$. En particular, la hipótesis implica que $d|1$ y, en consecuencia $d = 1$(ver pág. 48)

Números coprimos (pág. 48): *Definición**

Si el $(a, b) = 1$ entonces decimos que a y $b$son coprimos.

Propiedades de MCD (pág. 48): *Demostración**

Sean a y b enteros, con $a \neq 0$, entonces:

a. $(a, b) = (b, a) = (\pm a, \pm b)$

b. si $a > 0$, $(a, 0) = a$ y $(a, a) = a$

Vemos que a cumple con las condiciones de MCD

i. $a|a$ y $a|0$ $\quad (0 = a \cdot 0)$

ii. Es el mayor divisor, dado a que no hay divisores comunes $> a$

c. $(1, b) = 1$

Vemos que 1 cumple con las condiciones de MCD

i. $1|1$ y $1|b$ $\quad (0 = a \cdot 0)$

ii. Es el mayor divisor, dado a que el 1 tiene un solo divisor, el mismo.

d. Si $a \neq 0$, $b \in Z$, entonces $(a, b) = (a, b - a)$

Sea $d = (a, b - a)$, luego

i. $d|a$ y $d|b - a$

ii. Si $c|a$ y $c|b - a$ entonces $c|d$

Ahora bien, como $d|a$ y $d|b - a$, entonces $d|a + (b - a)$ por lo tanto $d|b$. Por lo que ahora tenemos:

iii. $d|a$ y $d|b$

Si $c|a$ y $c|b - a$ entonces $c|a - b$, luego por **(ii)** tenemos que $c|d$, es decir

iv. Si $c|a$ y $c|b$ entonces $c|d$

Se sigue que d cumple la definición de MCD

Definición de mínimo común múltiplo (pág. 54): *Definición**

Si a y b son enteros, decimos que un entero no negativo m es un mínimo común múltiplo o MCM de a y b si:

a. $a|m$ y $b|m$ (común múltiplo)

b. si $a|n$ y $b|n$ entonces $m|n$ (múltiplo mínimo)

Enunciado de la relación entre MCM y DCM (pág. 55): *Enunciado**

Sean a y b enteros no nulos, entonces $m = \frac{ab}{(ab)}$, demostración en la pág. 55

Definición de número primo (pag. 56): *Definición**

Se dice que un entero positivo p es primo si $p \geq 2$ y los únicos enteros positivos que dividen p son 1 y p mismo.

Un entero $m \geq 2$ **no es un primo** si y sólo si $m = m_1 m_2$ donde m_1 y $m_2$son enteros estrictamente entre 1 y m ($1 < m_1, m_2 < m$)

Observación de números primos 3.4.3 (pag. 57): *Demostración**

Sea $a \in Z$ y p primo. Entonces:

a. Si $p \nmid a$, entonces $(a, p) = 1$
Por definición de número primo, tenemos que los únicos divisores de p son: 1 y p, sabiendo también que $p \nmid a$, el único divisor común de p y a es 1.

b. Si p y p' son primos y $p|p'$ entonces $p = p'$
Sabiendo que p' es primo, sabemos que sus únicos divisores son 1 y p'. Como $p \neq 1$, tenemos que $p = p'$.

Enunciado de criterio de la raíz (pag. 58): *Enunciado**

Sea $n \geq 2$. Si para todo m tal que $1 < m \leq \sqrt{n}$ se cumple que $m \nmid n$, entonces n es primo.
Demostración en la pag. 58

Teorema 3.4.6 (pag. 59): *Demostración**

Sea p un número primo que cumpla con **a.** y **b.** entonces $p|x_i$ para algún x_i con $i \leq i \leq n$

a. Si $p|xy$ entonces $p|x$ o $p|y$.
Si $p|x$ ya está probado. Si $p \nmid x$entonces tenemos que $(p, x) = 1$ por proposición tenemos que $1 = rp + sx$, entonces tenemos $y = 1 \cdot y = (rp + sx)y = rpy + sxy$, sabiendo que $p|p$ y que $p|xy$ acomodamos como $(yr)p + s(xy)$, como p divide ambos términos se sigue que $p|y$

b. $x_1, x_2, \ldots, x_n$ son enteros tales que $p| x_1 x_2 \ldots x_n$
Demostración en la pag 59.

Teorema fundamental de la aritmética (pag. 59): *Enunciado**

La factorización en primos de un entero positivo $n \geq 2$ es única, salvo el orden de los factores primos.

Teorema de Euclides (pag. 60): *Demostración**

Existen infinitos números primos
La demostración de esta proposición, viene de la mano del Teorema fundamental de la aritmética (TFA). Suponemos que los números primos son finitos, entonces tendremos un conjunto de números primos $P = \{p_1, p_2, \ldots, p_r\}$. Sea $n = p_1 p_2 \ldots p_{r-1} p_r + 1$, notamos que ninguno de los elementos de P divide a n, ya que a dividirlo por cualquier p_i el resto es 1 por lo que n no tiene factorización en primos.
Esto es una contradicción al TFA. El absurdo viene de suponer que el conjunto P es finito.

CONGRUENCIA

Definición de congruencia (pag. 65): *Definición**

Sean a y b enteros y m un entero positivo. Diremos que a es congruente a b módulo m y escribimos $a \equiv b\ (m)$ si $a - b$ es divisible por m

Observar que $a \equiv 0\ (m)$ si y sólo si $m|a$ y que $a \equiv b\ (m)$ si y sólo si $a - b \equiv 0\ (m)$

Observar también que $a \equiv b\ (m)$ si y sólo si, a y b tienen el mismo resto en la división por m

Propiedades (pag. 66): *Demostración**

a. Reflexiva, $x \equiv x\ (mod\ m)$
   Debido a que $x - x = 0$, por lo tanto es divisible por m, otro forma de verlo es que ambos términos de la congruencia tienen el mismo resto a dividirse por m

b. Simétrica, si $x \equiv y\ (mod\ m)$ entonces $y \equiv x\ (mod\ m)$
   Si $x - y = km$, entonces $y - x = (-k)m$

c. Transitiva, si $x \equiv y\ (mod\ m)$ y $y \equiv z\ (mod\ m)$ entonces $x \equiv z\ (mod\ m)$
   Si $x - y = mk$ y $y - z = mh$, entonces $x - z = (x - y) + (y - z) = mk + mh = m(k + h)$, notar que el m divide a $x - z$ por lo tanto $x \equiv z\ (mod\ m)$.

Compatibilidad con las operaciones (pag. 66): *Demostración**

Sea m un entero positivo y sean x_1, x_2, y_1, y_2 enteros tales que $x_1 \equiv x_2\ (mod\ m)$ y $y_1 \equiv y_2\ (mod\ m)$.

Entonces:

a. $x_1 + y_1 \equiv x_2 + y_2\ (mod\ m)$
b. $x_1 y_1 \equiv x_2 y_2\ (mod\ m)$
c. Si $x \equiv y\ (mod\ m)$ y $k \in N$, entonces $x^k \equiv y^k\ (mod\ m)$
   Demostraciones en el libro (pag. 66 y 67)

Teorema 4.2.1 (pag. 70): *Enunciado**

Sean $a,\ b$ números enteros y m un entero positivo, denotamos $d = (a, m)$, como la ecuación $ax \equiv b\ (mod\ m)$. Esta ecuación admite solución si y sólo si $d|b$, y en este caso, dada x_0 una solución, todas las soluciones son de la forma $x = x_0 + kn$, con $k \in Z$ y $n = \frac{m}{d}$.

Demostración en la pag 70.

Teorema de Fermat (pag. 74): *Enunciado**

Sea p un número primo y a un número entero. Entonces $a^p \equiv a\ (mod\ p)$
Demostración en la pag. 70

GRAFOS

Definición de grafo (pag. 83): *Definición**

Un grafo G consiste de un conjunto finito V, cuyos miembros son llamados vértices, y un conjunto de 2-subconjuntos de V, cuyos miembros son llamados aristas. $G = (V, E)$
Ejemplo: $G = (V, E)$ con $V = \{a, b, c, d, z\}$ y $E = \{\{a, b\}, \{a, d\}, \{b, z\}, \{c, d\}, \{d, z\}\}$

Valencia de un vértice (pag. 89): *Definición**

La valencia o grado de un vértice v en un grafo $G = (V, E)$ es el número de aristas de G que contienen a v. Formalmente $\delta(v) = |D_v|$, donde $D_v = \{e \in E | \, v \in e\}$

Teorema 5.3.1 (pag. 89): *Demostración**

La suma de los valores de las valencias $\delta(v)$, tomados sobre todos los vértices v de grafo $G = (V, E)$, es igual a dos veces el número de aristas:

Fórmula: $\sum_{v \in V} \delta(v) = 2|E|$.

Demostración: La valencia de un vértice v indica la cantidad de "extremos" de aristas que "tocan" a v. Es claro que hay $2|E|$ extremos de aristas, luego la suma total de las valencias de los vértices es $2|E|$

Teorema 5.3.2 (pag. 89): *Demostración**

El número de vértices impares es par
Demostración: Denotemos como V_i y V_p los conjuntos de vértices impares y pares respectivamente, luego $V = V_i \cup V_p$ por teorema 5.3.1, obtenemos

$$\sum_{v \in V_i} \delta(v) + \sum_{v \in V_p} \delta(v) = 2|E|.$$

Ahora cada término de la segunda sumatoria es par, por ende, el resultado es par. Dado que el lado derecho es par, tenemos que la primera sumatoria es par, sabiendo que la suma de números impares es par solo cuando la cantidad de sumandos es par, tenemos que la cantidad de vértices impares es par.

Caminata y camino (pag. 91): *Definición**

Una **caminata** en un grafo G es una secuencia de vértices $(v_1, v_2, v_3, \ldots, v_k)$, tal que v_i y v_{i+1}son adyacentes $(1 \leq i \leq (k - 1))$. Si todos los vértices son distintos, una caminata es llamada un **camino**.

Ciclo (pag. 91): *Definición**

Llamaremos ciclo a una caminata $v_1, v_2, v_3, \ldots, v_{r+1}$ con $r \geq 3$ y cuyos vértices son distintos exceptuando los extremos. En otras palabras es un camino de a menos tres vértices con $v_1 = v_{r+1}$

Ciclo Hamiltoniano (pag. 94): *Definición**

Un grafo G es un ciclo que contiene a todos los vértices del grafo.

Caminata y circuito euleriano(pag. 95): *Definición**

Una caminata euleriana en un grafo G es una caminata que usa todas las aristas de G exactamente una vez. Se le llama circuito euleriano a una caminata euleriana que comienza y termina en el mismo vértice.

Existencia de caminatas eulerianas (pág. 95): *Enunciado**

Un grafo conexo con más de un vértice posee una caminata euleriana de v a w, con $v \neq w$ si y sólo si v y w son los únicos vértices con valencias impares.

Un grafo conexo con más de un vértice tiene un circuito euleriano si y sólo si todos los vértices tienen grado par.

Definición de árbol (pag. 98): *Definición**

Diremos que un grafo G es un árbol si es conexo y no hay ciclos en G

Grafos conexos (pag. 92):

Un grafo G es conexo si para cualesquiera dos vértices x, y existe una caminata de x a y. Es decir $x \sim y$.