Pontificia Universidad Católica de Chile
Departamento de Ciencia de la Computación
IIC1253 - Matemáticas Discretas

Apunte Discretas

1º semestre 2025 - Profesor P. Barceló

Rafael Lorca - rafael.lorca@uc.cl

---

1. Introducción

Este apunte va a ser una mezcla entre las soluciones de las ayudantías del semestre y algunos conceptos que yo considero que son importantes a la hora de responder las preguntas de prueba, eso sí siempre me han dicho que no se pueden mecanizar los ejercicios en este ramo, por lo que este apunte no debería ser su única fuente de ejercicios/conceptos.

Índice

2. Inducción

Inducción Simple

- Se utiliza para demostrar propiedades que dependen de los números naturales. Ej: $3n \geq 2n$ para todo n número natural.
- Se demuestra que "si $p(n)$ es verdadero entonces $p(n+1)$ es verdadero"
- Se divide en tres partes:
  1. **BI:** Se demuestra que la propiedad se cumple para el caso base. Demostrar que $p(0)$ es verdadero (a veces la propiedad por demostrar puede estar definida para los naturales n tales que $j \leq n$, en ese caso, el caso base sería $p(j)$).
  2. **HI:** Se supone que la propiedad se cumple para el número natural n. Asumir que $p(n)$ es verdadero.
  3. **TI:** Se demuestra que la propiedad se cumple para $n+1$. $p(n) \Rightarrow p(n+1)$.

Inducción Fuerte

- También se utiliza para los números naturales.
- Se demuestra que si $p(i)$ es verdadero para todos los $i \leq k$ entonces $p(k+1)$ es verdadero.
- Se divide en tres partes:
  1. **BI:** Se demuestra que la propiedad se cumple para el caso base. Demostrar que $p(0)$ es verdadero (a veces la propiedad por demostrar puede estar definida para los naturales n tales que $j \leq n$, en ese caso el caso base sería $p(j)$).
  2. **HI:** Se supone que la propiedad se cumple para todo número natural menor o igual a k. Asumir que $p(i)$ es verdadero para todo $i \leq k$.
  3. **TI:** Se demuestra que la propiedad se cumple para $k+1$. $(p(i) \forall i \leq k) \Rightarrow p(k+1)$.
- Cualquier problema de inducción simple se puede resolver con inducción fuerte.

Inducción Estructural:

Se utiliza cuando se quiere demostrar una propiedad en una estructura que está definida inductivamente (la inducción simple es un caso particular de inducción estructural). Un ejemplo de listas enlazadas, en árboles, grafos, etc. Se utiliza BI, HI y TI de la misma forma que en la inducción simple.

Preguntas

Pregunta 1

Demuestre, utilizando I.S, que para todo n° natural n la expresión:

$$n^2 + n$$

es par.

Sol:

- **C.B**: n=0 $\rightarrow 0^2 + 0 = 0$, es par.
- **H.I**: Suponga que existe un número natural "n"tq se cumple: $n^2 + n$, es par.
- **T.I**: Demostramos para k = n+1:

$$(n+1)^2 + (n+1) = n^2 + 3n + 2 = (n^2 + n) + 2(n+1)$$

El término de la derecha es par por estar multiplicado por 2 y el de la izq es par por H.I. Por I.S, queda demostrado.

Pregunta 1.b

Demuestre que a partir de cierto n° natural n la desigualdad:

$$2n + 3 \leq 2^n$$

, se cumple para todos los n° posteriores.

Sol: Nótese que el n° natural que satisface la desigualdad son $n \geq 4$, entonces:

- **C.B**: n=4 $\rightarrow 2 \times 4 + 3 \leq 2^4 = 11 \leq 16$.
- **H.I**: Suponga que existe un número natural $n \geq 4$ tq la desigualdad es verdadera.
- **T.I**: Demostramos para k = n+1, esta vez modificamos la propiedad a demostrar más que trabajar la T.I: Notamos que la siguiente desigualdad es cierta: $2 \leq 2^n$ para todo $n \geq 1$, más aún para $n \geq 4$. Sumamos esta desigualdad a la anterior y tenemos: $2n + 2 + 3 \leq 2^n + 2^n = 2(n+1) + 3 \leq 2^{n+1}$, que es la dessigualdad a demostrar.

3. Lógica Proposicional

¿Qué es la lógica proposicional?

Es un sistema que busca obtener conclusiones a partir de premisas. Los elementos más simples (letras 'p', 'q' u otras) representan proposiciones o enunciados. Los conectivas lógicas ($\neg$, $\wedge$, $\vee$ y $\rightarrow$), representan operaciones sobre proposiciones, capaces de formar otras proposiciones de mayor complejidad.

Semántica

Una valuación o asignación de verdad para las variables proposicionales en un conjunto P es una función $\sigma\colon P \rightarrow \{0,1\}$, donde '0' equivale a 'falso' y '1' a verdadero.

Tablas de verdad

Las fórmulas se pueden representar y analizar en una tabla de verdad, por ejemplo:

Cuadro 1: Bicondicional ($p \leftrightarrow q$)

p	q	$p \leftrightarrow q$
0	0	1
0	1	0
1	0	0
1	1	1

Si se tienen n variables proposicionales entonces existen 2^n valuaciones y 2^{2^n} tablas de verdad distintas.

Equivalencia Lógica $\equiv$

Dos fórmulas son lógicamente equivalentes (denotado como $\alpha \equiv \beta$) si para toda valuación σ se tiene que $\sigma(\alpha) = \sigma(\beta)$.

Leyes de Equivalencia

1. **Doble negación**:
$$\neg(\neg\alpha) \equiv \alpha$$
2. **De Morgan**:
$$\neg(\alpha \wedge \beta) \equiv (\neg\alpha) \vee (\neg\beta)$$
$$\neg(\alpha \vee \beta) \equiv (\neg\alpha) \wedge (\neg\beta)$$

3. **Conmutatividad**:

$$\alpha \wedge \beta \equiv \beta \wedge \alpha$$
$$\alpha \vee \beta \equiv \beta \vee \alpha$$

4. **Asociatividad**:

$$\alpha \wedge (\beta \wedge \gamma) \equiv (\alpha \wedge \beta) \wedge \gamma$$
$$\alpha \vee (\beta \vee \gamma) \equiv (\alpha \vee \beta) \vee \gamma$$

5. **Distributividad**:

$$\alpha \wedge (\beta \vee \gamma) \equiv (\alpha \wedge \beta) \vee (\alpha \wedge \gamma)$$
$$\alpha \vee (\beta \wedge \gamma) \equiv (\alpha \vee \beta) \wedge (\alpha \vee \gamma)$$

6. **Idempotencia**:

$$\alpha \wedge \alpha \equiv \alpha$$
$$\alpha \vee \alpha \equiv \alpha$$

7. **Absorción**:

$$\alpha \wedge (\alpha \vee \beta) \equiv \alpha$$
$$\alpha \vee (\alpha \wedge \beta) \equiv \alpha$$

8. **Implicación**:

$$\alpha \rightarrow \beta \equiv (\neg\alpha) \vee \beta$$

9. **Doble implicación**:

$$\alpha \leftrightarrow \beta \equiv (\alpha \rightarrow \beta) \wedge (\beta \rightarrow \alpha)$$

Conectivos Funcionalmente Completos

Un conjunto de conectivos lógicos se dice funcionalmente completo si toda fórmula en L(P) es lógicamente equivalente a una fórmula que sólo usa esos conectivos.

Ejemplos: $\{\neg, \wedge, \vee\}$,$\{\neg, \wedge\}$,$\{\neg, \vee\}$,$\{\neg, \rightarrow\}$

Conceptos importantes de lógica proposicional

- **Tautología**: Una fórmula es una tautología si su valor de verdad es siempre 1, para cualquier valuación.
- **Contradicción**: Una fórmula es una contradicción si su valor de verdad es siempre 0, para cualquier valuación.
- **Forma normal conjuntiva (CNF)**: Una fórmula está en forma normal conjuntiva si es una conjunción de disyunciones de literales. Es decir, es de la forma

$$C_1 \wedge C_2 \wedge \ldots \wedge C_k$$

  donde cada C_i es una disyunción de literales, es decir,

$$C_i = (l_{i1} \vee \ldots \vee l_{ik}).$$

- **Forma normal disyuntiva (DNF)**: Una fórmula está en forma normal disyuntiva si es una disyunción de conjunciones de literales. Es decir, es de la forma

$$B_1 \vee B_2 \vee \ldots \vee B_k$$

  donde cada B_i es una conjunción de literales, es decir,

$$B_i = (l_{i1} \wedge \ldots \wedge l_{ik}).$$

- **Satisfacibilidad**: Un conjunto de fórmulas Σ es satisfacible si existe una valuación σ tal que $\sigma(\Sigma) = 1$. En caso contrario, Σ es inconsistente.
  ¿Como saber si un conjunto es insatisfacible?
  - Tabla de verdad: Si en una tabla de verdad, para las valuaciones de las variables proposicionales no hay una fila con 1 (una fórmula no es verdadera), entonces es insatisfacible.
  - Resolución: Pasar todas las fórmulas del conjunto a CNF y aplicar la regla de resolución hasta llegar a la cláusula vacía $\square$.
  - Por contradicción: Σ es insatisfacible si $\Sigma \vDash F$, algo falso es consecuencia lógica del conjunto de fórmulas, por ejemplo:

$$\Sigma = \{p \to q, p, \neg q\}$$

Consecuencia Lógica ($\Gamma \vDash \phi$)	**Satisfacibilidad** ($\mathcal{M} \vDash \phi$)
Universal: ϕ es verdadera en **todos** los modelos donde Γ es verdadero.	Existencial: ϕ es verdadera en **al menos un modelo** $\mathcal{M}$.
Ejemplo:	**Ejemplo**:
"Todos los humanos son mortales, Sócrates es humano"$= \Gamma$: Predicados	Fórmula ϕ: Existe un dia soleado para pasear al perro. Modelo $\mathcal{M}$: "Hoy está soleado"
$\therefore \Gamma \vDash$ Sócrates es humano	$\mathcal{M} \vDash \phi \rightarrow$ pasear al perro
$\{\forall x P(x) \vDash P(a)\}$	Basta que **hoy** esté soleado para pasear al perro (no necesita ser siempre).

4. Relaciones

Una relación binaria es un conjunto de pares ordenados que establece una conexión o asociación entre elementos de dos conjuntos distintos.

Propiedades de una relación binaria

- **Refleja**
  R es refleja si para todo elemento x en el conjunto, el par (x, x) está en R.

$$\forall x \in A, (x, x) \in R$$

- **Irrefleja**
  R es irrefleja si ningun par (x, x) está en R para cualquier x en el conjunto.

$$\forall x \in A, (x, x) \notin R$$

- **Simétrica**
  R es simétrica si para cada par (x, y) en R, también los está el par (y, x).

$$\forall x, y \in A, (x, y) \in R \rightarrow (y, x) \in R$$

- **Antisimétrica**
  R es antisimétrica si para cada par (x, y) en R, si $x \neq y$, entonces $(y, x) \notin R$

$$\forall x, y \in A, (x, y) \in R \wedge (y, x) \in R \rightarrow x = y$$

- **Transitiva**
  R es transitiva si para cada par (x, y) y (y, z) en R el par (x, z) también está en R.

$$\forall x, y, z \in A, (x, y) \in R \wedge (y, z) \in R \rightarrow (x, z) \in R$$

- **Conexa**
  R es conexa si para cada par de elementos x,y podemos encontrar a (x, y) en R o a (y, x) en R.

$$\forall x, y \in A, (x, y) \in R \vee (y, x) \in R$$

Relación de equivalencia

Una relación binaria R sobre A es de equivalencia si es **refleja**, **simétrica** y **transitiva**. Se denota como $x \sim y$.

Clases de equivalencia

Dado $x \in A$, la clase de equivalencia de x bajo $\sim$ es el conjunto

$$[x]_\sim = \{y \in A | x \sim y\}$$

Conjunto cuociente

Sea $\sim$ una relación de equivalencia sobre un conjunto A. El conjunto cuociente de A con respecto a $\sim$ es el conjunto de todas las clases de equivalencia de $\sim$:

$$A/\sim = \{[x] \mid x \in A\}$$

Son equivalentes las siguientes proposiciones:

1. $a \sim b$
2. $[a]_\sim = [b]_\sim$
3. $[a]_\sim \cap [b]_\sim \neq \emptyset$

Relación de orden

Orden Parcial

Una relación R sobre un conjunto A es un orden parcial si es **refleja**, **antisimétrica** y **transitiva**. Se denota como $x \preceq y$. El par $(A, \preceq)$ es un orden parcial.

Orden total

Una relación $\preceq$ sobre A es un orden total si es un orden parcial u además es **conexa**.

Elementos extremos

Mínimo y máximo

Sean $(A, \preceq)$, un orden parcial, $S \subseteq A$ y $x \in A$. Diremos que:

1. x es una **cota inferior** de S si para todo $y \in S$ se cumple que $x \preceq y$.
2. x es un **elemento minimal** de S si $x \in S$ y para todo $y \in S$ se cumple que $y \preceq xy = x$.
3. x es un **mínimo** en S si $x \in S$ y es cota inferior de S.

Las definiciones de **cota superior**, **elemento maximal** y **máximo** son análogas.

Ínfimo y supremo

Sea $(A, \preceq)$ un orden parcial y $S \subseteq A$. Diremos que s es un ínfimo de S si es cota inferior, y para cualquier otra cota inferior $s' \preceq s$. Es decir, el ínfimo es la mayor cota inferior. Análogamente se define el supremo de un conjunto.

El orden parcial $(A, \preceq)$ es **superiormente completo**, si $S \subseteq A$ es un conjunto no vacío que tiene cota superior y también tiene supremo. Análogamente **inferiormente completo**.

Teorema: $(A, \preceq)$ es superiormente completo $\leftrightarrow$ $(A, \preceq)$ es inferiormente completo.

Demostración: Supongamos $(A, \preceq)$ es superiormente completo. Tomemos $S \subseteq A$ que tiene cota inf y $S \neq \emptyset$.
Defina $S_{c.i} = \{a \in A | \text{a es cota inf de S}\}$. Luego $S_{c.i}$ es no vacio $\rightarrow \forall x \in S_{c.i}\ \forall y \in S : x \preceq y$.
Esto quiere decir que $S_{c.i}$ tiene como cota superior a los elementos de S. $\therefore$ $S_{c.i}$ tiene supremo $\sup(S_{c.i})$ por lo que $(A, \preceq)$ es superiormente completo.
Luego, $\forall y \in S : \sup(S_{c.i}) \preceq y$ (todos los elementos de S son $c.s$ de $S_{c.i}$).
$\therefore \sup(S_{c.i})$ es c.i de S. Pero además, $\forall y \in S_{c.i} : y \preceq \sup(S_{c.i}) \implies \sup(S_{c.i}) = \text{ínf}(S)$.
$\square$

Concepto	¿Debe estar en A?	¿Es único?	¿Puede no existir?	Descripción
Mínimo	Sí	Sí	Sí	El menor de todos los
Cota inferior	No	No	Sí	Un elemento menor o
Elemento minimal	Sí	No	Sí	No hay otro elemento
Ínfimo	No	Sí	Sí	Mayor entre todas las

Cuadro 2: Comparación entre mínimo, cota inferior, elemento minimal e ínfimo

Ejemplo

Sea $P = \mathcal{P}(\{1, 2, 3\})$ y $A = \{\{1\}, \{2\}, \{3\}\}$ con el orden parcial dado por la inclusión: $X \leq Y \iff X \subseteq Y$.

- No hay **mínimo** en A, ya que ningún conjunto está contenido en los otros.
- Todos los elementos de A son **minimales**: no hay subconjuntos estrictamente más pequeños dentro de A.
- Una **cota inferior** de A es $\emptyset$, ya que $\emptyset \subseteq \{1\}, \{2\}, \{3\}$.
- ínf $A = \emptyset$, porque es la mayor de las cotas inferiores (y única, en este caso).
- Observa que el **ínfimo** no está en A, pero sí en el conjunto total P.

5. Funciones

Sea $f \subseteq A \times B$ diremos que f es una función de A en B si dado cualquier elemento $\forall a \in A \; \exists b$ tal que:

$$afb \wedge afc \implies a = c$$

Sea: $f : a \to B$. Diremos que f es:

- **Inyectiva** si la función es uno a uno, esto es $\forall x, y \in A$ se tiene que $f(x) = f(y) \implies x = y$.
- **Sobreyectiva** si $\forall b \in B . \exists a \in A$ ta que $b = f(a)$.
- **Biyectiva** si es inyectiva y sobreyectiva a la vez.

Función invertible

Dada una función f de A en B, diremos que f es invertible si su relación inversa f^{-1} es una función de B en A.

Composición de funciones

Dadas relaciones R de A en B y S de B en C, la composición de R y S es una relación de A en C definida como

$$S \; o \; R = \{(a, c) \in A \times \; | \; \exists b \in B \text{ tal que } aRb \wedge bSc\}$$

Principio del palomar

Si se tiene una función $f : \mathbb{N}_m \to \mathbb{N}_n$ con $m > n$, la función f no puede ser inyectiva. Es decir, necesariamente existirán $x, y \in \mathbb{N}_m$ tales que $x \neq y$, pero $f(x) = f(y)$.

- Si $m > n, f$ no puede ser inyectiva.
- $m < n, f$ no puede ser sobreyectiva.
- Si f es biyectiva, entonces $m = n$. (No necesariamente al revés).

6. Cardinalidad

Dos conjuntos A y B son equinumerados si eiste una biyección $A \to B$. Se denota como $A \approx B$.

Cardinalidad $= |A| = [A]_{\approx}$ Conjunto de todos los conjuntos equinumerosos.

Si un conjunto es **numerable** o **contable** si $|A| \leq |\mathbb{N}|$. Contrario a esto se tienen conjuntos no contables como $(0, 1) \in \mathbb{R}$. Para demostrar no numerabilidad:

- Asumimos que tenemos una lista que numera y llegar a una contradicción → diagonalización de Cantor.
- Legamos a una biyección con un conjunto no numerable.
- Demostramos que un subconjunto de este no es numerable.

Teorema de Cantor

- $(0, 1) \subseteq \mathbb{R}$ no es numerable.
- $(0, 1) \approx \mathbb{R} \approx P(\mathbb{N})$.
- $A < P(A)$ no es numerable.

En general el teorema de Cantor-Schröder-Bernstein (nombre completo) sirve para demostrar que dos conjuntos A y B son equinumerosos. Si existe $f_1 : A \to B$ y $f_2 : B \to A$, ambas inyectivas, entonces $|A| = |B|$.

7. Conteo

- Regla del producto: $|A \times B| = |A| * |B|$
- Regla de la suma: $|A \cup B| = |A \cap B|$

Permutaciones y combinaciones

Dado $|A| = n$

- Permutación: arreglo ordenado de r elementos. $P(n, r) = \frac{n!}{(n-r)!}$
- Combinación: subconjunto de tamaño r. ¿De cuantas formas podemos elegir r objetos entre n objetos? $C(n, r) = \frac{P(n,r)}{P(r,r)} = \frac{n!}{(n-r)!r!}$

Observaciones:

- $\binom{n}{k} = \binom{n}{n-k}$ → Dejar n-k objetos afuera.
- $\sum_{k=0}^{n} \binom{n}{k}$ = número de subconjuntos de n elementos $= 2^n$

Demuestre utilizando conteo las siguientes proposiciones:

- $\binom{n+1}{k} = \binom{n}{k} + \binom{n}{k-1}$.

Nos piden demostrar que se cumple lo anterior, sin expandir términos $\binom{n+1}{k}$ nos dice que tenemos que contar de cuántas formas se puede elegir un subconjunto de k elementos de un conjunto de $n+1$ elementos. Separamos a los subconjuntos en casos:

1. Subconjuntos que NO contienen a $n+1$. Tenemos que elegir k elementos de un grupo de n (ya que no se tiene al $n+1$, por conteo sabemos que esto equivale a $\binom{n}{k}$.
2. Subconjuntos que contienen a $n+1$. Tenemos que elegir $k-1$ elementos (ya que tenemos al $n+1$ de n elementos restantes, esto equivale a $\binom{n}{k-1}$.

Finalmente por principio de la suma: $\binom{n+1}{k} = \binom{n}{k} + \binom{n}{k-1}$ $\square$

8. Algoritmos y notación asintótica

Un algoritmo es correcto si:

- Termina en un número finito de pasos para cualquier entrada válida.
- Entrega una salida correcta, es decir, cumple con la especificación del problema.

Para demostrar la correctitud se utiliza (normalmente):

- Invariante
- Inducción matemática

Análisis temporal

Para modelar la complejidad de una algoritmo es útil definir:

$T(n) =$ numero de operaciones que ejecuta el algoritmo en funcion del tamaño de entrada n

Luego se puede clasificar estas funciones según notación asintótica y obtener su complejidad.

Notación asintótica

$$g \in \mathcal{O}(f) \leftrightarrow (\exists c > 0)(\exists n_0)(\forall n > n_0) g(n) \leq c \cdot f(n)$$
$$g \in \Omega(f) \leftrightarrow (\exists c > 0)(\exists n_0)(\forall n > n_0) g(n) \geq c \cdot f(n)$$
$$g \in \Theta(f) \leftrightarrow g \in \mathcal{O}(f) \ \wedge g \in \Omega(f)$$

Propiedades de las Sumatorias

Sumatorias Básicas

$$\sum_{k=0}^{n} k = \frac{n(n+1)}{2} \qquad \text{(Suma de los primeros } n \text{ enteros)}$$

$$\sum_{k=1}^{n} k = \frac{n(n+1)}{2} \qquad \text{(Misma suma, índice desde 1)}$$

$$\sum_{k=1}^{n-1} k = \frac{(n-1)n}{2} \qquad \text{(Suma hasta } n-1\text{)}$$

$$\sum_{k=1}^{n} k^2 = \frac{n(n+1)(2n+1)}{6} \qquad \text{(Suma de cuadrados)}$$

$$\sum_{k=1}^{n} k^3 = \left(\frac{n(n+1)}{2}\right)^2 \qquad \text{(Suma de cubos)}$$

$$\sum_{k=0}^{n} r^k = \frac{1-r^{n+1}}{1-r} \qquad \text{(Serie geométrica, } r \neq 1\text{)}$$

Propiedades Generales

$$\sum_{k=1}^{n}(a_k + b_k) = \sum_{k=1}^{n} a_k + \sum_{k=1}^{n} b_k \qquad \text{(Linealidad)}$$

$$\sum_{k=1}^{n} c \cdot a_k = c \cdot \sum_{k=1}^{n} a_k \qquad \text{(Homogeneidad)}$$

$$\sum_{k=m}^{n} a_k = \sum_{k=m+p}^{n+p} a_{k-p} \qquad \text{(Cambio de índice)}$$

$$\sum_{k=1}^{n} a_k = \sum_{k=1}^{m} a_k + \sum_{k=m+1}^{n} a_k \qquad \text{(Aditividad en rangos)}$$

Sumatorias Notables

$$\sum_{k=1}^{n} \frac{1}{k} \approx \ln n + \gamma \qquad \text{(Serie armónica, } \gamma \approx 0{,}5772\text{)}$$

$$\sum_{k=0}^{\infty} r^k = \frac{1}{1-r} \qquad \text{(Serie geométrica infinita, } |r| < 1\text{)}$$

$$\sum_{k=1}^{n} \binom{n}{k} = 2^n - 1 \qquad \text{(Suma de combinaciones)}$$

9. Grafos y árboles

Grafos

- **Grafo:** Un grafo $G = (V, E)$ es un par donde V es in conjunto cuyos elementos llamaremos nodos y E es una relación binaria sobre V (es decir, $E \subseteq V \times V$), cuyos elementos llamaremos aristas.
- **Subgrafos:**
  - Ciclo: es una caminata cerrada en la que no se repiten aristas.
  - Clique: es un subgrafo en el que cada vértice está conectado a todos los demás vértices del subgrafo.
- **Tipos de grafos:**
  - Grafo no dirigido: Un grafo es no dirigido si toda arista tiene una arista paralela.
  - Grafo isomorfo: Dos grafos son isomorfos si existe una función biyectiva $f : V_1 \to V_2$ tal que $(x, y) \in E_1$ si y solo si $(f(x), f(y)) \in E_2$.
  - Grafo completo: todos los pares de vértices son adyacentes (están conectados por una arista).
  - Grafo conexo: Son aquellos grafos tal que todo par de vértices está conectado por un camino.
  - Grafo bipartito: es un grafo tal que su conjunto de vérices puede particionarse en dos conjuntos independientes.
  - Multigrafo $G = (V, E, f)$: es un trío ordenado donde $f : E \to S$ es una función que asigna dos conjuntos independientes.
- **Grado de un vértice:** El grado de v ($\delta(v)$) es la cantidad de aristas que inciden en v.

- **Teorema de los saludos**: $\sum_{v \in V} \delta_g(v) = 2|E|$.
- **Tipos de ciclos:**
  - Ciclo hamiltoniano: es un ciclo que contiene a todos los vértices del grafo una única vez (excepto por el inicio y el final).
  - Ciclo euleriano: es un ciclo que contiene a todas las aristas y vértices del grafo.

Arboles

- Un grafo $T = (V, E)$ es un árbol si y solo si es conexo y acíclico.
  - Un grafo $T = (V, E)$ es un árbol si y solo si todas sus aristas son de corte (arista que si se elimina aumentan las componentes conexas).
  - Un grafo $T = (V, E)$ es un árbol si y solo si tiene exactamente $n - 1$ aristas.
- **Bosque**: Un grafo $T = (V, E)$ es un bosque si para cada par de vértices $x, y \in V$ si existe un camino entre ellos, este es único.
- **Árbol binario**: Un árbol con raiz se dice binario si todo vértice tiene grado a lo más 3 o equivalentemente si todo vértice tiene a lo más dos hijos.

10. Teoría de números

División y módulo

- **Relación de división**: Si x divide a b, se denota $x|b$ y es una relación sobre $\mathbb{Z}\backslash 0$ tal que $\exists k \in \mathbb{Z} : b = x \cdot k$.
- **Módulo n**: $\equiv_n$ es una relación sobre $\mathbb{Z}$ tal que $a \equiv_n b$ si y solo si $n|(b - a)$. Esta relación es de equivalencia.
- **Operación módulo**: La operación módulo n entrega el resto de la división por n, se denota $a \mod (n)$

Teoremas:

$$a \equiv_n b \leftrightarrow a \mod n = b \mod n$$

$$(a + b)\ mod\ n = ((a\ mod\ n) + (b\ mod\ n))\ mod\ n$$

$$(a \cdot b)\ mod\ n = ((a\ mod\ n)(b\ mod\ n))mod\ n$$

Pequeño teorema de Fermat

- Si p es primo:
$$a^p \equiv_p a$$
- Si p es primo y no divide a a:
$$a^{n-1} \equiv_p 1$$

Máximo común divisor

- **GCD:** Dados a y b diremos que su máximo común divisor, denotado como $gcd(a, b)$ es el mácimo natural n tal que $n|a \ \wedge \ n|b$,
- **Algoritmo de euclides**: Si $a > b$:
$$gcd(a, b) = gcd(r, b) \quad \text{con} a \ mod \ b = r < b$$
Siguiendo recursivamente llegamos a $gcd(n, 0) = n$
- **Identidad de Bezout**: Esta identidad enuncia que si $a, b \in \mathbb{Z}$ son distintos de 0 y $gcd(a, b) = d$, entonces existen $x, y \in \mathbb{Z}$ tales que:
$$a \cdot x + b \cdot y = d$$