Guía super chupi para no pencar discreta

Contents

Tema 1: Teoría de Conjuntos

Inducción

Ejemplo 1.4.- *Prueba por inducción que* $1+2+3+\cdots+n = \dfrac{n(n+1)}{2}$.

En primer lugar debemos verificar *la base de la inducción*, esto es, que la fórmula que debemos probar es cierta para $n=1$, es decir, cuando sólo hay un sumando. Pero esto es obvio, pues

$$1 = \frac{1\cdot(1+1)}{2} = 1.$$

Ahora tenemos que probar *el paso inductivo*, esto es, tenemos que ver que si la fórmula se cumple para $n=k$, también se cumple para $n=k+1$. En este caso, suponemos cierto que

$$1+2+\cdots+k = \frac{k(k+1)}{2}. \tag{1.1}$$

¿Se cumple entonces que $1+2+\cdots+k+(k+1) = \dfrac{(k+1)(k+1+1)}{2}$?

Teniendo en cuenta (1.1), resulta

$$1+2+\cdots+k+(k+1) = \frac{k(k+1)}{2}+(k+1).$$

Operando llegamos finalmente a

$$1+2+\cdots+k+(k+1) = \frac{(k+1)(k+2)}{2}.$$

Luego la fórmula también es cierta para $n=k+1$ y, por el principio de inducción matemática, es válida para cualquier $n\geq 1$. ■

Algoritmo de Euclides

Tabla 1.1: Cálculo del máximo común divisor de dos enteros a y b mediante el algoritmo de Euclides y esquema por el cual es posible expresar éste mediante una combinación entera de a y b.

$$\begin{array}{r|l} 1\,232 & 344 \\ \hline 200 & 3 \end{array} \qquad 8 = 7 \cdot 344 - 12 \cdot (1\,232 - 3 \cdot 344) = 43 \cdot 344 - 12 \cdot 1\,232$$

$$\begin{array}{r|l} 344 & 200 \\ \hline 144 & 1 \end{array} \qquad 8 = 7 \cdot (344 - 200) - 5 \cdot 200 = 7 \cdot 344 - 12 \cdot \overset{\uparrow}{\boxed{200}}$$

$$\begin{array}{r|l} 200 & 144 \\ \hline 56 & 1 \end{array} \qquad 8 = 2 \cdot 144 - 5 \cdot (200 - 144) = 7 \cdot \overset{\uparrow}{\boxed{144}} - 5 \cdot 200$$

$$\begin{array}{r|l} 144 & 56 \\ \hline 32 & 2 \end{array} \qquad 8 = 2 \cdot (144 - 56 \cdot 2) - 56 = 2 \cdot 144 - 5 \cdot \overset{\uparrow}{\boxed{56}}$$

$$\begin{array}{r|l} 56 & 32 \\ \hline 24 & 1 \end{array} \qquad 8 = 32 - (56 - 32) = 2 \cdot \overset{\uparrow}{\boxed{32}} - 56$$

$$\begin{array}{r|l} 32 & 24 \\ \hline 8 & 1 \end{array} \qquad 8 = 32 - \overset{\uparrow}{\boxed{24}}$$

$$\begin{array}{r|l} 24 & \boxed{8} \\ \hline 0 & 3 \end{array} \quad \longrightarrow \quad \overset{\uparrow}{8} = \text{m.c.d.}(1\,232, 344) \ \text{(último resto distinto de 0)}$$

Tabla 1.2: Método abreviado para calcular m.c.d.(a, b) mediante una combinación entera de a y b. En este caso $a = 1\,232$, $b = 344$ y m.c.d.$(1\,232, 344) = 8$, con $8 = -12 \cdot 1\,232 + 43 \cdot 344$.

r	m	n	q
1 232	1	0	
344	0	1	
200	1	-3	3
144	-1	4	1
56	2	-7	1
32	-5	18	2
24	7	-25	1
8	$\mathbf{-12}$	**43**	1

Para ponerlo en forma de tabla podemos representar en una columna los restos, en otra el coeficiente m en otra n y en una cuarta el cociente q. Partiendo de las dos ecuaciones triviales, los elementos m y n de la siguiente fila serán la resta de los de la fila dos posiciones por encima menos q por los de la fila anterior (véase la tabla 1.2). Por ejemplo, en la tabla 1.2, la tercera fila (en lo que atañe a los coeficientes m y n) es igual a la primera menos 3 veces la segunda, pues 3 es el cociente de la primera división del algoritmo de Euclides, y así sucesivamente.

Una aplicación inmediata de la identidad de Bézout es que si a y b son primos entre sí, entonces existen m y n tales que $m \cdot a + n \cdot b = 1$. Este hecho es importante y tiene algunas aplicaciones interesantes, como se ve en los siguientes ejemplos.

Tabla 1.2: Método abreviado para calcular m.c.d.(a, b) mediante una combinación entera de a y b. En este caso $a = 1\,232$, $b = 344$ y m.c.d.$(1\,232, 344) = 8$, con $8 = -12 \cdot 1\,232 + 43 \cdot 344$.

r	m	n	q
1 232	1	0	
344	0	1	
200	1	−3	3
144	−1	4	1
56	2	−7	1
32	−5	18	2
24	7	−25	1
8	**−12**	**43**	1

Para ponerlo en forma de tabla podemos representar en una columna los restos, en otra el coeficiente m en otra n y en una cuarta el cociente q. Partiendo de las dos ecuaciones triviales, los elementos m y n de la siguiente fila serán la resta de los de la fila dos posiciones por encima menos q por los de la fila anterior (véase la tabla 1.2). Por ejemplo, en la tabla 1.2, la tercera fila (en lo que atañe a los coeficientes m y n) es igual a la primera menos 3 veces la segunda, pues 3 es el cociente de la primera división del algoritmo de Euclides, y así sucesivamente.

Una aplicación inmediata de la identidad de Bézout es que si a y b son primos entre sí, entonces existen m y n tales que $m \cdot a + n \cdot b = 1$. Este hecho es importante y tiene algunas aplicaciones interesantes, como se ve en los siguientes ejemplos.

Ecuaciones Diofánticas

Paso 1.- Encontrar una solución particular de (1.5). Teniendo en cuenta la Identidad de Bézout (Teorema 1.5), existen m y n tales que $m \cdot a + n \cdot b = 1$. Multiplicando esta igualdad por c obtenemos una solución particular de la ecuación (1.5) de la forma:

$$x = c \cdot m, \qquad y = c \cdot n.$$

Paso 2.- Resolver la *ecuación homogénea asociada*:

$$a \cdot x + b \cdot y = 0. \tag{1.6}$$

Notemos que las soluciones enteras de esta ecuación se obtienen de manera sencilla si despejamos una de las incógnitas. Así,

$$x = -\frac{b}{a} y, \text{ con m.c.d.}(a, b) = 1.$$

Como m.c.d.$(a, b) = 1$, por el ejemplo 1.9, x es un número entero si a es un divisor de y. Por lo tanto, podemos poner $y = k \cdot a$ y las soluciones de (1.6) son de la forma

$$x = -k \cdot b, \qquad y = k \cdot a, \quad k \in \mathbb{Z}.$$

Paso 3.- Dar la solución general de la ecuación diofántica (1.5). Es evidente que si a una solución de (1.5) le sumamos una solución de (1.6) se obtiene una solución de (1.5) (basta con sumar las ecuaciones). En consecuencia, todas las posibles soluciones de (1.5) son de la forma

$$\left\{ \begin{array}{lcl} x & = & c \cdot m - k \cdot b \\ y & = & c \cdot n + k \cdot a \end{array} \right. \quad k \in \mathbb{Z}. \tag{1.7}$$

Ejemplo 1.14.- *Encuentra todas las soluciones enteras no negativas de la ecuación* $7 \cdot x + 13 \cdot y = 147$.

En primer lugar, como m.c.d.$(7, 13) = 1$, vemos que le ecuación se puede resolver. Además, por el algoritmo de Euclides, encontramos que

$$1 = 2 \cdot 7 - 1 \cdot 13.$$

Multiplicando por 147, se obtiene

$$147 = 294 \cdot 7 - 147 \cdot 13.$$

Así, una solución particular es $x = 294$, $y = -147$. Sin embargo, para obtener el total de soluciones hay que añadir las soluciones de la ecuación homogénea

$$7 \cdot x + 13 \cdot y = 0,$$

que son de la forma $x = -13 \cdot k$, $y = 7 \cdot k$. Finalmente, se tiene que la solución general es

$$x = 294 - 13 \cdot k, \qquad y = -147 + 7 \cdot k, \quad k \in \mathbb{Z}.$$

Como estamos interesados en las soluciones no negativas tiene que ser

$$294 - 13 \cdot k \geq 0 \Longrightarrow k \leq 294/13 = 22{,}615,$$
$$-147 + 7 \cdot k \geq 0 \Longrightarrow k \geq 147/7 = 21.$$

Por lo tanto $21 \leq k \leq 22{,}615$. Puesto que $k \in \mathbb{Z}$, los únicos valores posibles de k que hacen que la solución sea no negativa son $k = 21$ y $k = 22$. En estos casos la solución es:

$$\begin{array}{lll} k = 21, & x = 21, & y = 0. \\ k = 22, & x = 8, & y = 7. \quad \blacksquare \end{array}$$

Relaciones

R *es reflexiva si* aRa $\forall a \in A$.

R *es simétrica si* aRb *implica que* bRa.

R *es antisimétrica si* aRa *y* bRa *implica que* $a = b$.

R *es transitiva si* aRb *y* bRc, *entonces que* aRc.

Tipos de aplicaciones

Se dice que f es *inyectiva* si para cada par de elementos $x, y \in A$ tales que $f(x) = f(y)$ se tiene que $x = y$. Es decir, no puede haber dos elementos distintos en A que tengan la misma imagen.

Se dice que f es *suprayectiva* si para todo $b \in B$ existe un elemento $a \in A$ tal que $f(a) = b$. Es decir, todo elemento en el conjunto B tiene una preimagen.

Se dice que f es *biyectiva* si es inyectiva y suprayectiva a la vez. En muchos textos, a las aplicaciones biyectivas también se les llama aplicaciones 1–1 (es decir, uno a uno).

Relación de orden parcial

Definición 7.9 *Una relación binaria* R *en un conjunto* A *se dice* relación de orden parcial *si cumple las propiedades reflexiva, antisimétrica y transitiva. En este caso* A *se dice* un conjunto parcialmente ordenado. *Para las relaciones de orden se usa la notación* $a \leq b$ *en lugar de* aRb *y* $a < b$ *si* aRb *y* $a \neq b$.

Relaciones de equivalencia

Definición 7.11 *Una relación binaria* R *en un conjunto* A *se dice* relación de equivalencia *si cumple las propiedades reflexiva, simétrica y transitiva. Dos elementos relacionados se dicen* equivalentes.

Tema 2: Aritmética modular

Congruencias

Definición 8.1 *Dados* $a, b \in \mathbb{Z}$, *decimos que* a *es* congruente *con* b *módulo* n *si* $a - b$ *es divisible por* n. *En este caso, denotamos*

$$a \equiv b\ (n) \quad \text{o} \quad a \equiv b \pmod{n}.$$

Algunas observaciones acerca de esta definición:

1. Existe un entero $k \in \mathbb{Z}$ tal que $a = kn + b$.
2. Podemos identificar una relación de congruencia módulo n como un reloj redondo de n posiciones. Por ejemplo, si $n = 5$, $a = 3$ y $b = 8$ coinciden en la misma posición.
3. Con las hora seguimos una aritmética modular ($n = 12$ o $n = 24$).

$$[a] = [b] \iff a \equiv b \pmod{n} \iff n \mid (b - a)$$

Elemento invertible

Un elemento es invertible si existe otro elemento ($\overline{x} \in \mathbb{Z}_n$) tal que $ax \equiv 1 \pmod{n}$. Si este inverso existe, es unico.

Un elemento solo pertenece al inverso si el mcd(a,n)=1.

Funcion de Euler

Numero de enteros positivos menores o iguales a n y coprimos con n.

$$\phi(n) = \operatorname{card}\left(\{a \mid 1 \leq a < n,\ m.c.d.(a, n) = 1\}\right) = |\mathbb{Z}_n^*|$$

ϕ (7) = 1,2,3,4,5,6

ϕ (4) = 1,3

Normalmente la ϕ (n) = n-1

a) Si $n = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}$ con $e_1, \ldots, e_r \geq 1$ entonces:

$$\phi(n) = p_1^{e_1 - 1}(p_1 - 1) \cdots p_r^{e_r - 1}(p_r - 1).$$

b) Si m.c.d.$(m, n) = 1$, $\phi(mn) = \phi(m)\phi(n)$.

Teorema de Euler-Fermat

Si m.c.d.$(a, n) = 1$, con $a \geq 2$, entonces $a^{\phi(n)} \equiv 1 \pmod{n}$

Pequeño teorema de Fermat

d) **Pequeño teorema de Fermat.** Si p es un primo que no divide a a entonces $a^{p-1} \equiv 1 \pmod{p}$

Veamos algunos ejemplos de cálculo:

1. $\phi(42) = \phi(2 \cdot 3 \cdot 7) = \phi(2)\phi(3)\phi(7) = 1 \cdot 2 \cdot 6 = 12$.
2. $\phi(72) = \phi(2^3 \cdot 3^2) = 2^2 \cdot 1 \cdot 3 \cdot 2 = 24$.

Ejemplo 8.1.- *¿En qué cifra termina* 7^{339}*?*

Para responder a esta pregunta, basta con calcular el resto de dividir 7^{339} entre 10, es decir calcular $7^{339} \pmod{10}$. Como m.c.d.$(7, 10) = 1$ y $\phi(10) = \phi(2)\phi(5) = 1 \cdot 4 = 4$, se tiene, por el pequeño teorema de Fermat, que $7^4 \equiv 1 \pmod{10}$.

Por otra parte, al dividir 339 entre 4, se tiene $339 = 4 \cdot 84 + 3$. Entonces, operando módulo 10:

$$7^{339} = (7^4)^{84} 7^3 \equiv 1^{84} 7^3 = 49 \cdot 7 \equiv 9 \cdot 7 = 63 \equiv 3 \pmod{10}.$$

Por lo tanto, 7^{339} acaba en 3. ∎

Teorema chino de los restos

Teorema 8.3 *Sean $n_1, \dots, n_r \geq 2$ primos entre sí. Sean $a_1, \dots, a_r \in \mathbb{Z}$. Existen soluciones $x \in \mathbb{Z}$ del sistema*

$$\left\{ \begin{array}{ccc} x & \equiv & a_1\,(n_1) \\ \vdots & \vdots & \vdots \\ x & \equiv & a_r\,(n_r). \end{array} \right.$$

Además si x_0 es una solución particular, el conjunto de soluciones es

$$\{x_0 + kn_1 \cdots n_r \mid k \in \mathbb{Z}\}.$$

La demostración del teorema nos da una técnica constructiva para calcular la solución particular x_0 que permite definir el conjunto de soluciones.

El teorema chino de los restos también sirve para simplificar expresiones en congruencias.

Ejercicios ejemplos

Encuentra las dos últimas cifras de 2011^{2011} y de 2011^{2012}.

Solución. Para encontrar las dos últimas cifras de un número, nos interesa trabajar módulo 100. Como $2011^{2011} \pmod{100} \equiv 11^{2011} \pmod{100}$, $11^{\phi(100)} \equiv 1 \pmod{100}$ y $2011 = 50 \times 40 + 11$, se tiene que

$$11^{2011} \pmod{100} \equiv 11^{11} \pmod{100} = 11^{2^3} 11^2 11 \pmod{100}$$

$$\equiv 81 \cdot 21 \cdot 11 \pmod{100} \equiv 11 \pmod{100},$$

las dos últimas cifras de 2011^{2011} son 11.

Análogamente, las dos últimas cifras de 2011^{2012} son 21 pues

$$2011^{2012} \pmod{100} \equiv 11^{12} \pmod{100} = 11^{2^3} 11^{2^2} \pmod{100}$$

$$\equiv 81 \cdot 41 \pmod{100} \equiv 21 \pmod{100}.$$

Demuestra que $n^2 + 1$ no es múltiplo de 19 para ningún $n \in \mathbb{N}$.

Solución. Razonamos por reducción al absurdo, suponiendo que 19 divide a $n^2 + 1$ para algún $n \in \mathbb{N}$. Entonces

$$n^2 + 1 \equiv 0 \pmod{19} \Rightarrow n^2 \equiv -1 \pmod{19} \Rightarrow n^2 \equiv 18 \pmod{19}.$$

Calculamos los posibles cuadrados en $\mathbb{Z}_{19}$: $1^2 \equiv 1 \pmod{19}$; $2^2 \equiv 4 \pmod{19}$; $3^2 \equiv 9 \pmod{19}$; $4^2 \equiv 16 \pmod{19}$; $5^2 \equiv 6 \pmod{19}$; $6^2 \equiv 17 \pmod{19}$; $7^2 \equiv 11 \pmod{19}$; $8^2 \equiv 7 \pmod{19}$; $9^2 \equiv 5 \pmod{19}$; $10^2 \equiv 5 \pmod{19}$; $11^2 \equiv 7 \pmod{19}$; $12^2 \equiv 11 \pmod{19}$; $13^2 \equiv 17 \pmod{19}$; $14^2 \equiv 6 \pmod{19}$; $1^2 \equiv 16 \pmod{19}$; $16^2 \equiv 9 \pmod{19}$; $17^2 \equiv 4 \pmod{19}$; $18^2 \equiv 1 \pmod{19}$.

Por lo tanto, ninguno de ellos cumple que $n^2 \equiv 18 \pmod{19}$ y, en consecuencia, $n^2 + 1$ no puede ser múltiplo de 19 para ningún $n \in \mathbb{N}$. ■

Tema 3: Combinatoria

Tipos de aplicaciones

- *Se dice que f es* inyectiva *si para cada par de elementos $x, y \in A$ tales que $f(x) = f(y)$ se tiene que $x = y$. Es decir, no puede haber dos elementos distintos en A que tengan la misma imagen.*
- *Se dice que f es* suprayectiva *si para todo $b \in B$ existe un elemento $a \in A$ tal que $f(a) = b$. Es decir, todo elemento en el conjunto B tiene una preimagen.*
- *Se dice que f es* biyectiva *si es inyectiva y suprayectiva a la vez. En muchos textos, a las aplicaciones biyectivas también se les llama aplicaciones 1–1 (es decir, uno a uno).*

Principio de adición

Teorema 2.3.- (Principio de adición) *Sean A y B dos conjuntos finitos tales que $A \cap B = \emptyset$, entonces $|A \cup B| = |A| + |B|$.*

Este principio se generaliza por inducción. Así, si $A_1, A_2, \ldots, A_n$ es una colección de conjuntos disjuntos dos a dos, es decir $A_i \cap A_j = \emptyset$ si $i \neq j$, entonces

$$|A_1 \cup A_2 \cup \cdots \cup A_n| = |A_1| + |A_2| + \cdots + |A_n|.$$

Notemos que el principio del palomar es una consecuencia del principio generalizado de la adición. Así, si las cajas las denominamos $A_1, A_2, \ldots, A_n$ y cada caja contiene menos de r elementos, entonces, por el principio de adición,

$$|A_1 \cup A_2 \cup \cdots \cup A_n| \leq nr < m.$$

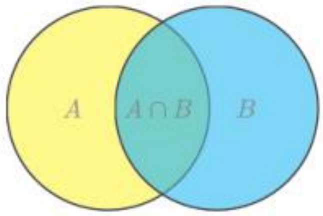
Es decir, el total de elementos que hay en todas las cajas, es inferior al número de objetos que hemos repartido m.

También consecuencia del principio de adición es el *principio de inclusión-exclusión*.

Principio de Inclusión - Exclusión

Teorema 2.4.- (Principio de inclusión-exclusión) *Sean A y B dos conjuntos finitos, entonces*

$$|A \cup B| = |A| + |B| - |A \cap B|.$$



Variaciones con repetición

El número de *variaciones con repetición* de n elementos tomados de k en k es:

$$VR(n, k) = n^k.$$

Este número es lo mismo que:

- El número de aplicaciones de $\mathbb{N}_k$ en $\mathbb{N}_n$, o en general, el número de aplicaciones $f : X \longrightarrow Y$ entre un conjunto X con cardinal k y otro conjunto Y con cardinal n.
- El número de palabras de k letras en un alfabeto de n letras.
- El número de selecciones ordenadas de k elementos (admitiendo repeticiones) de un conjunto de n elementos.

Variaciones

El número de *variaciones* de n elementos tomados de k en k es:

$$V(n,k) = \frac{n!}{(n-k)!}, \text{ si } 0 \leq k \leq n.$$

Este número es lo mismo que:

- El número de aplicaciones inyectivas de $\mathbb{N}_k$ en $\mathbb{N}_n$, o en general, el número de aplicaciones inyectivas $f: X \longrightarrow Y$ entre un conjunto X con cardinal k y otro conjunto Y con cardinal n.
- El número de palabras de k letras en un alfabeto de n letras que no tienen ninguna letra repetida.
- El número de selecciones ordenadas de k elementos (sin repeticiones) de un conjunto de n elementos.

Permutaciones

El número de *permutaciones* de un conjunto de n elementos es:

$$P(n) = n!.$$

Este número es lo mismo que:

- El número de aplicaciones biyectivas de $\mathbb{N}_n$ en $\mathbb{N}_n$, o en general, el número de aplicaciones biyectivas $f: X \longrightarrow Y$ entre dos conjuntos X e Y con el mismo cardinal n.
- El número de ordenaciones distintas de un conjunto de n elementos.
- El número variaciones de n elementos tomados de n en n.

Permutaciones con repetición

El número de *permutaciones con repetición* de un conjunto de k elementos $\{a_1, \ldots, a_k\}$ en el que cada elemento a_i se repite α_i veces, con $\alpha_1 + \cdots + \alpha_k = n$, $\alpha_i \geq 1$, es:

$$PR(n; \alpha_1, \ldots, \alpha_k) = \binom{n}{\alpha_1 \alpha_2 \ldots \alpha_k} = \frac{n!}{\alpha_1! \alpha_2! \cdots \alpha_k!}.$$

Este número es lo mismo que:

- Dar una lista ordenada de longitud n donde el elemento a_1 se repite α_1 veces, el a_2, α_2 veces y, en general, el a_i, α_i veces ($\alpha_1 + \alpha_2 + \cdots + \alpha_k = n$ y $\alpha_i \geq 1$).
- Distribuir n objetos diferentes en k cajas, de modo que la caja i-ésima recibe α_i objetos.
- El número de aplicaciones de un conjunto de n elementos en otro conjunto de k elementos tales que envían α_1 elementos a a_1, ..., α_k elementos a a_k.

Combinaciones

El número de *combinaciones* de un conjunto de n elementos tomados de k en k es:

$$C(n,k) = \binom{n}{k} = \frac{n!}{k!(n-k)!}, \quad 0 \leq k \leq n.$$

Este número es lo mismo que:

- El número de subconjuntos de k elementos que podemos formar a partir de un conjunto de n elementos.
- El número de selecciones no ordenadas de k elementos que se pueden hacer a partir de un conjunto de n elementos.

Combinaciones con repetición

El número de *combinaciones con repetición* de n elementos tomados de k en k es:

$$CR(n,k) = \binom{n+k-1}{k} = \frac{(n+k-1)!}{k!(n-1)!}.$$

Este número es lo mismo que:

- El número de selecciones no ordenadas (con elementos repetidos) de k elementos que se pueden hacer a partir de un conjunto de n elementos.
- El número de soluciones enteras no negativas de la ecuación

$$x_1 + x_2 + x_3 + \cdots + x_n = k.$$

- Formas de distribuir k objetos idénticos en n cajas etiquetadas.

Particiones

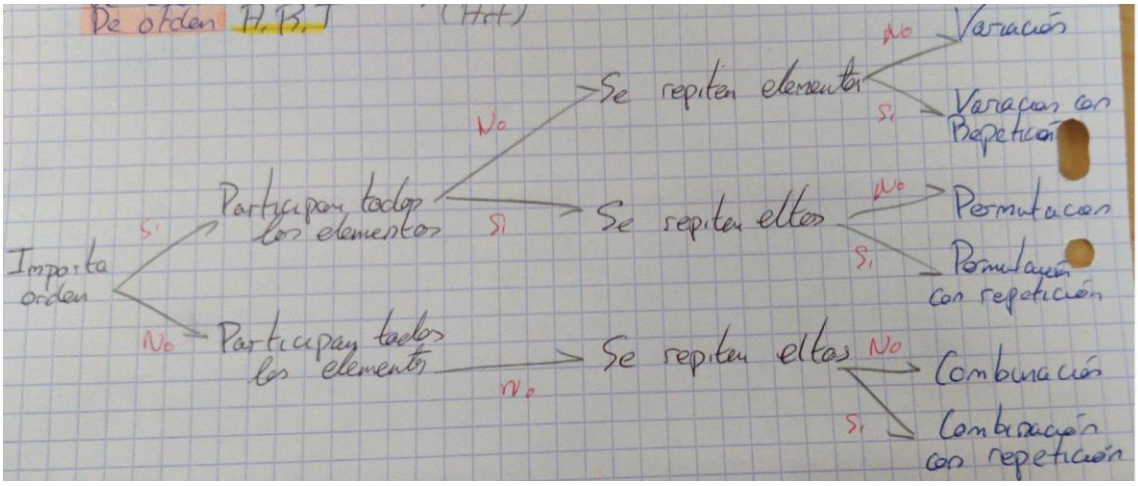
Una *partición* de un conjunto A de n elementos en k partes es una familia de k subconjuntos disjuntos no vacíos de A tales que su unión es el propio conjunto A. De esta forma si A_1, A_2, $\ldots$, A_k son los subconjuntos de la partición, entonces

1.- A_j no vacío.

2.- $A_i \cap A_j = \emptyset$ si $i \neq j$.

3.- $A_1 \cup A_2 \cup \cdots \cup A_k = A$.

Cuando usar cada uno



Tema 4: Funciones Generadoras

Función generadora:

Definición 3.1.- *Sea $a_0, a_1, a_2, \ldots$ una sucesión de números reales. Llamamos función generadora de la sucesión $\{a_n\}_{n\geq 0}$ a una función $G(x)$ tal que*

$$G(x) = \sum_{n\geq 0} a_n x^n = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n + \cdots.$$

La función generadora de la sucesión $\{a_n\}_{n\geq 0}$ debe entenderse como una forma alternativa de representarla. En este sentido, no debemos preocuparnos por la convergencia de la serie.

Adición:

Adición. Si $G_1(x)$ es la función generadora de $a_0, a_1, \ldots$ y $G_2(x)$ es la función generadora de $b_0, b_1, \ldots$, entonces $\alpha G_1(x) + \beta G_2(x)$ es la función generadora de $\alpha a_0 + \beta b_0, \alpha a_1 + \beta b_1, \ldots$. Basta tener en cuenta que las series se suman como si fueran polinomios.

Desplazamiento:

Desplazamiento. Si $G(x)$ es la función generadora de $a_0, a_1, \ldots$, entonces $x^n G(x)$ es la función generadora de

$$\overbrace{0, \ldots, 0}^{n \text{ ceros}}, a_0, a_1, \ldots.$$

Análogamente,

$$(G(x) - a_0 - a_1 x - \ldots - a_{n-1}x^{n-1})/x^n$$

es la función generadora de $a_n, a_{n+1}, \ldots$.

Multiplicación:

Multiplicación. Si $G_1(x)$ es la función generadora de $a_0, a_1, \ldots$ y $G_2(x)$ es la función generadora de $b_0, b_1, \ldots$, entonces

$$\begin{aligned} G_1(x)G_2(x) &= (a_0 + a_1 x + a_2 x^2 + \cdots)(b_0 + b_1 x + b_2 x^2 + \cdots) \\ &= (a_0 b_0) + (a_0 b_1 + a_1 b_0)x + (a_0 b_2 + a_1 b_1 + a_2 b_0)x^2 + \cdots \end{aligned}$$

es la función generadora de la sucesión $s_0, s_1, \ldots$, donde

$$s_n = \sum_{0\leq k\leq n} a_k b_{n-k}.$$

En términos de series de potencias, a la serie

$$\sum_{k\geq 0} s_k x^k$$

se le llama producto de Cauchy de las series definidas por $G_1(x)$ y $G_2(x)$.

Un caso importante es cuando $\{b_n\}$ es la sucesión constante 1. En esta situación tenemos

$$\frac{1}{1-x} G(x) = a_0 + (a_0 + a_1)x + (a_0 + a_1 + a_2)x^2 + \cdots$$

que es la función generadora de la sucesión de sumas parciales de la sucesión $\{a_n\}_{n\geq 0}$.

Cambio de Variable

Cambio de variable. Si $G(x)$ es la función generadora de la sucesión $a_0, a_1, \ldots$, entonces $G(cx)$ es la función generadora de la sucesión

$$a_0, ca_1, c^2a_2, \ldots .$$

En particular, la función generadora de la sucesión $1, c, c^2, c^3, \ldots$ es $1/(1-cx)$.

Además de estas propiedades algebraicas las técnicas de cálculo nos proporcionan nuevas operaciones, como la derivación y la integración. Así, si $G(x)$ es la función generadora de la sucesión $a_0, a_1, \ldots$, entonces $xG'(x)$ es la función generadora de $\{na_n\}$. Análogamente

$$\frac{1}{x}\int_0^x G(s)\,ds = a_0 + \frac{1}{2}a_1x + \frac{1}{3}a_2x^2 + \cdots$$

es la función generadora de $\{a_n/(n+1)\}$.

Las funciones generadoras tienen múltiples aplicaciones y el poder determinarlas, para una sucesión dada, resulta de gran utilidad, especialmente si la sucesión está relacionada con la solución general de un cierto problema combinatorio. En cualquier caso, no existen métodos generales para determinar una función generadora, aunque en cierto tipo de problemas es posible dar unas reglas más o menos generales. En este sentido nos será de utilidad el Teorema del binomio generalizado.

Teorema del binomio generalizado:

Teorema 3.1.- (Teorema del binomio generalizado) *Si definimos*

$$\binom{\alpha}{k} = \frac{\alpha(\alpha-1)(\alpha-2)\cdots(\alpha-k+1)}{k!}$$

con $\alpha \in \mathbb{R}$, entonces

$$(1+x)^\alpha = \sum_{k=0}^{\infty} \binom{\alpha}{k} x^k.$$

Corolario 3.2.- *Si $\alpha = -n$, con $n \in \mathbb{N}$, entonces*

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

Además,

$$\frac{1}{(1-x)^n} = \sum_{k=0}^{\infty} CR(n,k)x^k.$$

Funciones generadoras exponenciales

Se usan, por ejemplo, para problemas de distribución de objetos diferentes en cajas diferentes.

Definición 3.2.- *Una función generadora exponencial para la sucesión de números* $\{a_n\}_{n\geq 0}$ *es una función* $G(x)$ *que admite el siguiente desarrollo en serie:*

$$G(x) = a_0 + a_1 x + a_2 \frac{x^2}{2!} + a_3 \frac{x^3}{3!} + \cdots + a_n \frac{x^n}{n!} + \cdots .$$

Para analizar la relación entre las funciones generadoras exponenciales y los problemas de distribución en los que importa el orden, recordemos lo que nos dice el Teorema del binomio:

$$(1+x)^n = \binom{n}{0} + \binom{n}{1}x + \binom{n}{2}x^2 + \cdots + \binom{n}{n}x^n$$

$$= C(n,0) + C(n,1)x + C(n,2)x^2 + \cdots + C(n,n)x^n, \quad n = 0,1,2,3\ldots$$

Tengamos en cuenta ahora que

$$C(n,j) = \frac{n!}{j!(n-j)!} = \frac{V(n,j)}{j!},$$

donde $V(n,j)$ es el número de variaciones de n elementos tomados de j en j. En consecuencia, para $n = 0,1,2,3\ldots$,

$$(1+x)^n = V(n,0) + V(n,1)x + V(n,2)\frac{x^2}{2!} + V(n,3)\frac{x^3}{3!} + \cdots + V(n,n)\frac{x^n}{n!}.$$

Por lo tanto, si nos fijamos en el coeficiente de $x^j/j!$ en el desarrollo de $(1+x)^n$, obtenemos $V(n,j)$.

Observemos que el desarrollo en serie de Taylor de la función exponencial e^x es:

$$e^x = 1 + \frac{x}{1!} + \frac{x^2}{2!} + \frac{x^3}{3!} + \cdots + \frac{x^n}{n!} + \cdots = \sum_{j=0}^{\infty} \frac{x^j}{j!}.$$

Por lo tanto e^x es la función generadora exponencial de la sucesión $\{1,1,1,\ldots\}$ y la función generadora ordinaria de la sucesión $\{1, 1/1!, 1/2!, 1/3!, \ldots\}$.

Tema 5: Sucesiones recurrentes lineales

Sucesión recurrente:

Aquella sucesión en la que los términos de la misma imagen vienen dados en función de los anteriores.

Sucesión recurrente lineal:

En las que los términos de la sucesión se obtienen a partir de combinaciones lineales de los términos anteriores.

Definición 4.1.- *Dada una sucesión* (a_n), *si existe un número natural* k *y unos números reales* c_1, c_2, $\ldots$, c_k *tales que a partir de un cierto* m *se tiene*

$$a_{n+k} = c_1 a_{n+k-1} + c_2 a_{n+k-2} + \cdots + c_k a_n + f(n), \tag{4.6}$$

con $n \geq m \geq 1$, *diremos que* (a_n) *es una* sucesión recurrente lineal de orden k. *A la relación (4.6) la denominaremos* ecuación recurrente lineal de orden k.

Supongamos que (4.6) es válida para $n = 1$ (lo que significa $m = 1$ en la definición), entonces

$$a_{k+1} = c_1 a_k + c_2 a_{k-1} + \cdots + c_k a_1 + f(1),$$

por lo que para determinar a_{k+1} es necesario conocer a_1, a_2, $\ldots$, a_k. Es decir, para que una recurrencia lineal de orden k esté completamente determinada, además de la ecuación (4.6) que la define, es preciso conocer los k primeros términos de la misma.

Recurrencias lineales homogéneas y no homogéneas:

Definición 4.2.- *Las recurrencias lineales se clasifican en* homogéneas *y* no homogéneas, *según sea el término independiente* $f(n)$. *Así, si en la ecuación (4.6)* $f(n) = 0$, *es decir,* $f(n)$ *es la función constante igual a cero, diremos que la recurrencia es* homogénea. *En caso contrario, diremos que la recurrencia es* no homogénea.

En muchas ocasiones una recurrencia no homogénea puede transformarse en otra que sí lo es. Por ejemplo, la recurrencia dada para el problema de las Torres de Hanoi (ejemplo 4.1), $T_n = 2T_{n-1} + 1$, es una recurencia de orden uno no homogénea. Sin embargo, escribamos la recurrencia para $n + 1$ y restemos las expresiones correspondientes a T_{n+1} y T_n

$$T_{n+1} = 2T_n + 1, \qquad T_n = 2T_{n-1} + 1$$
$$T_{n+1} - T_n = 2T_n - 2T_{n-1}$$
$$T_{n+1} = 3T_n - 2T_{n-1}.$$

Observamos que los términos de T_n satisfacen una recurrencia lineal homogénea de orden dos.

Análogamente, la recurrencia para el caso de las regiones en que queda dividido el plano por n rectas (ejemplo 4.2) puede transformarse en otra homogénea por un procedimiento similar. En este caso en la recurrencia no homogénea $R_n = R_{n-1} + n$, consideramos los términos R_n y R_{n+1}. Restándolos se obtiene

$$R_{n+1} - R_n = R_n - R_{n-1} + 1,$$

es decir

$$R_{n+1} = 2R_n - R_{n-1} + 1.$$

Considerando ahora R_{n+2} y volviendo a restar se obtiene finalmente

$$R_{n+2} = 3R_{n+1} - 3R_n + R_{n-1},$$

que es una recurrencia lineal homogénea de orden 3.

Como se ve, el precio que hay que pagar para convertir una recurrencia no homogénea en otra homogénea es el aumento en el orden de la misma. Sin embargo, para la resolución de las recurrencias homogéneas existe un método general que consideraremos a continuación.

Resolución de recurrencias lineales homogéneas:

Empecemos resolviendo una recurrencia lineal de primer orden homogénea. Esto es, una recurrencia dada por la ecuación

$$a_{n+1} = q a_n, \qquad n \geq 1. \tag{4.7}$$

Observemos que cualquier progresión geométrica de razón q cumple esta ecuación. De hecho, aplicando sucesivamente la relación (4.7) se obtiene

$$a_{n+1} = a_1 q^n, \qquad n \geq 0. \tag{4.8}$$

En este caso, la sucesión queda determinada de manera única por el primer término de la misma y por el coeficiente q. Una fórmula explícita para los términos de la sucesión está dada por (4.8).

Consideremos ahora el caso de una recurrencia lineal homogénea de orden k dada por la relación

$$a_{n+k} = c_1 a_{n+k-1} + c_2 a_{n+k-2} + \cdots + c_k a_n, \qquad n \geq 1. \tag{4.9}$$

Esta ecuación es satisfecha por infinitas sucesiones, al igual que la ecuación (4.7) era satisfecha por cualquier progresión geométrica de razón q. En este caso la sucesión quedará determinada de manera única una vez que se conozcan los k primeros términos de la misma.

Por ejemplo, no es complicado comprobar que las sucesiones de la forma $a_n = A + B2^n$, con A y B dos números reales cualesquiera, satisfacen la recurrencia $a_{n+1} = 3a_n - 2a_{n-1}$, $n \geq 1$. Ahora bien, si fijamos los dos primeros términos de la sucesión (a_n), ésta queda determinada de forma única. En efecto, si $a_0 = a_1 = 1$ entonces $a_n = 1$ para todo $n \geq 0$. Sin embargo, si $a_0 = 1/2$ y $a_1 = 1$ entonces $a_n = 2^{n-1}$ para todo $n \geq 0$. En general, dados los dos primeros términos a_0 y a_1, los coeficientes A y B son la única solución del sistema de ecuaciones

$$\left\{ \begin{array}{ccccc} A & + & B & = & a_0 \\ A & + & 2B & = & a_1. \end{array} \right.$$

Teorema 4.1 *Si (x_n) e (y_n) son dos sucesiones que satisfacen la ecuación (4.9), entonces la sucesión (z_n) tal que $z_n = Ax_n + By_n$, con $A, B \in \mathbb{R}$, también satisface (4.9).*

Este resultado nos dice que cualquier combinación lineal de sucesiones que satisfacen (4.9) también satisface (4.9). A partir de aquí, no es difícil probar que cualquier sucesión que satisface (4.9) se puede poner como combinación lineal de una base de k sucesiones independientes que también satisfacen (4.9). En efecto, sean (x_n^m), con $m = 1, \ldots, k$, las k sucesiones independientes. Entonces la sucesión (a_n) cuyos k primeros términos son a_1, a_2, …, a_k se podrá obtener como combinación lineal de (x_n^m) siempre que el sistema de ecuaciones

$$\left\{ \begin{array}{l} A_1 x_1^1 + A_2 x_1^2 + \cdots + A_k x_1^k = a_1, \\ A_1 x_2^1 + A_2 x_2^2 + \cdots + A_k x_2^k = a_2, \\ \qquad\qquad\vdots \\ A_1 x_k^1 + A_2 x_k^2 + \cdots + A_k x_k^k = a_k, \end{array} \right.$$

tenga solución única. En este caso tiene que ser

$$\begin{vmatrix} x_1^1 & x_1^2 & \cdots & x_1^k \\ x_2^1 & x_2^2 & \cdots & x_2^k \\ \vdots & \vdots & \vdots & \vdots \\ x_k^1 & x_k^2 & \cdots & x_k^k \end{vmatrix} \neq 0,$$

que es la condición de independencia de las sucesiones (x_n^m).

Por lo tanto, el problema de encontrar la sucesión que satisface (4.9) y cuyos k primeros términos son a_1, a_2, …, a_k pasa por encontrar k sucesiones independientes que cumplan (4.9).

A la vista de que una recurrencia de orden uno es satisfecha por progresiones geométricas, podemos buscar si existen progresiones geométricas

$$a_n = \lambda^n, \tag{4.10}$$

que satisfacen (4.9). En este caso se tiene que cumplir

$$\lambda^{n+k} = c_1\,\lambda^{n+k-1} + c_2\,\lambda^{n+k-2} + \cdots + c_k\,\lambda^n.$$

Dividiendo por λ^n, obtenemos una ecuación polinómica de orden k:

$$\lambda^k - c_1\lambda^{k-1} - c_2\lambda^{k-2} - \cdots - c_k = 0. \tag{4.11}$$

Esta ecuación se llama ecuación característica asociada a la ecuación recurrente homogénea.

Por lo tanto, para que la progresión geométrica (4.10) sea solución de (4.9), λ tiene que ser solución de la ecuación característica (4.11). De este modo, por cada raíz de (4.11) obtendremos una solución de la recurrencia de la forma (4.10). Además, no es difícil ver que dos raíces distintas dan lugar a soluciones independientes. En consecuencia se nos pueden presentar las siguientes situaciones:

1. La ecuación característica (4.11) tiene raíces reales y distintas.
2. La ecuación característica (4.11) tiene raíces reales múltiples.
3. La ecuación característica (4.11) tiene raíces complejas distintas.
4. La ecuación característica (4.11) tiene raíces complejas múltiples.

A continuación, explicamos cómo obtener la solución general de una recurrencia lineal homogénea (4.9) en cada una de estas situaciones.

Case de raíces reales distintas:

Si la ecuación característica (4.11) tiene k raíces reales distintas, entonces tenemos las k sucesiones independientes que necesitamos para encontrar la solución del problema. En este caso la solución general de la recurrencia es de la forma

$$a_n = \alpha_1 \lambda_1^n + \alpha_2 \lambda_2^n + \cdots + \alpha_k \lambda_k^n,$$

donde $\lambda_1, \lambda_2, \ldots, \lambda_k$ son las k soluciones diferentes de la ecuación característica.

Está claro que si todas las raíces de la ecuación característica son reales y distintas es posible encontrar un conjunto de k sucesiones independientes que nos permiten dar con la solución de la recurrencia (4.9). Sin embargo, si alguna de las raíces tiene multiplicidad mayor que uno, el total de sucesiones de la forma (4.10) será menor que k y necesitaremos encontrar otras sucesiones que nos completen la base para generar la solución general.

Supongamos, en primer lugar, que λ_1 es una raíz de multiplicidad 2, es decir $(\lambda - \lambda_1)^2$ es un factor del polinomio

$$\lambda^k - c_1\lambda^{k-1} - c_2\lambda^{k-2} - \cdots - c_k.$$

En este caso, λ_1 es además raíz de la derivada, por lo que se cumple

$$k\lambda_1^{k-1} - c_1(k-1)\lambda_1^{k-2} - c_2(k-2)\lambda_1^{k-3} - \cdots - c_{k-1} - c_k(k-k) = 0.$$

Multiplicando por λ_1 resulta

$$k\lambda_1^{k} - c_1(k-1)\lambda_1^{k-1} - c_2(k-2)\lambda_1^{k-2} - \cdots - c_{k-1}\lambda_1 - c_k(k-k) = 0,$$

que podemos escribir como

$$k\lambda_1^k - \sum_{n=1}^{k} (k-n)\, c_k\, \lambda_1^{k-n},$$

lo que nos dice que $n\lambda_1^n$ también es solución de la recurrencia.

A esta conclusión también se puede llegar haciendo uso del Teorema 4.1. En efecto, si λ_1 y λ_2 son dos raíces distintas de la ecuación característica, las sucesiones (λ_1^n) y (λ_2^n) son soluciones de (4.9), pero también cualquier combinación lineal de ellas, en particular

$$\lambda_1 \frac{\lambda_2^n - \lambda_1^n}{\lambda_2 - \lambda_1}.$$

Si hacemos ahora que λ_2 se acerque a λ_1, tomando límites tenemos que

$$n\lambda_1^n$$

es solución, pero ahora λ_1 es una raíz de multiplicidad 2 de la ecuación característica.

En general, se puede demostrar que si λ_1 (o cualquier otra raíz de (4.11)) tiene multiplicidad m, entonces son solución de la recurrencia (4.9) las sucesiones de término general

$$\lambda_1^n, \quad n\lambda_1^n, \quad n^2\lambda_1^n, \quad \ldots, \quad n^{m-1}\lambda_1^n.$$

De este modo es posible encontrar el conjunto de k sucesiones independientes que dan lugar a la solución general de (4.9).

Caso de raíces complejas distintas:

Si la ecuación característica (4.11) tiene raíces complejas conjugadas se puede proceder igual que si fueran reales, con la única particularidad de que ahora los coeficientes que finalmente determinan la recurrencia pueden ser también números complejos. No obstante, dado que las sucesiones que vamos a tratar son de números reales, es preferible evitar la aparición de números complejos en la expresión explícita de los términos de la sucesión. Para ello, supongamos que $\alpha \pm i\beta$ son dos raíces complejas conjugadas de la ecuación característica. Si r y θ son, respectivamente, el módulo y el argumento (véase la figura 4.3) de un número complejo $\alpha + i\beta$, entonces

$$\alpha + i\beta = r(\cos\theta + i \operatorname{sen}\theta), \quad \alpha - i\beta = r(\cos\theta - i \operatorname{sen}\theta).$$

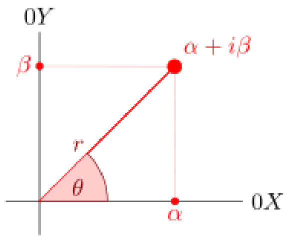


Figura 4.3: Módulo r y argumento θ de un número complejo $\alpha + i\beta$: $r = \sqrt{\alpha^2 + \beta^2}$, $\theta = \operatorname{arc\,tg}(\beta/\alpha)$.

Según hemos visto, las sucesiones $(\alpha \pm i\beta)^n$ son soluciones de (4.9), pero por la fórmula de de Moivre se tiene que

$$(\alpha \pm i\beta)^n = r^n(\cos n\theta \pm i \operatorname{sen} n\theta)$$

son soluciones. Aplicando ahora el Teorema 4.1, permitiendo combinaciones lineales complejas, son soluciones de (4.9) las sucesiones

$$(r^n \cos n\theta), \qquad (r^n \operatorname{sen} n\theta).$$

Ahora bien, estas dos sucesiones son de términos reales y nos valen para formar la base de sucesiones necesarias para obtener la solución general.

Caso de raíces complejas múltiples:

Si $\lambda = \alpha + i\beta$ es una raíz de multiplicidad m de la ecuación característica, entonces las siguientes sucesiones son soluciones de la recurrencia (4.9):

$$\lambda^n,\ n\lambda^n,\ n^2\lambda^n, \ldots,\ n^{m-1}\lambda^n.$$

Nótese que de igual modo se obtendría una familia de soluciones para la raíz conjugada $\bar{\lambda} = \alpha - i\beta$:

$$\bar{\lambda}^n,\ n\bar{\lambda}^n,\ n^2\bar{\lambda}^n, \ldots,\ n^{m-1}\bar{\lambda}^n.$$

Al igual que ocurría en el caso anterior, los coeficientes que determinan la recurrencia podrían ser números complejos. Si se quiere evitar la aparición de números complejos en la expresión explícita de los términos de la sucesión, se deberían combinar dos soluciones complejas y así, junto con la fórmula de de Moivre, obtener soluciones reales.

Resolución de recurrencias lineales no homogéneas:

Consideremos ahora el caso de una recurrencia lineal no homogénea dada por la ecuación (4.6)

$$a_{n+k} = c_1 a_{n+k-1} + c_2 a_{n+k-2} + \cdots + c_k a_n + f(n),$$

donde $f(n)$ es una función conocida de n, distinta de la función nula, $f(n) = 0$.

Puede verse que la solución general de la ecuación anterior depende de k constantes arbitrarias y su estructura es de la forma

$$a_n = a_n^h + a_n^p,$$

siendo a_n^h la solución general de la recurrencia lineal homogénea a la que da lugar la ecuación anterior (haciendo $f(n) = 0$) y a_n^p una solución particular de la misma. Puesto que la resolución de las recurrencias homogéneas ya se ha discutido en el apartado anterior, el problema se reduce a encontrar una solución particular.

Vamos a presentar un método para encontrar una solución particular en el caso en que $f(n)$ sea de la forma

$$\sum_{j=i}^{m} p_j(n) r_j^n,$$

con $p_j(n)$ polinomios en n y $r_j \in \mathbb{R}$. El método se denomina de *coeficientes indeterminados* y consiste en buscar una solución de la forma

$$\sum_{j=i}^{m} q_j(n) r_j^n,$$

donde, en general, los polinomios p_j y q_j son del mismo grado y los coeficientes de los q_j deben ser determinados. Sin pérdida de generalidad, supondremos que $f(n)$ se compone de un sólo sumando, es decir

$$f(n) = p(n) r^n,$$

donde $p(n)$ es un polinomio de grado conocido. Distinguimos dos situaciones, dependiendo de que r sea solución de la ecuación característica de la recurrencia homogénea o no.

1. Si r no es solución de la ecuación característica de la recurrencia homogénea, tomamos como solución particular una de la forma

   $$a_n^p = q(n) r^n,$$

   siendo $q(n)$ un polinomio del mismo grado que $p(n)$.

2. Si, por el contrario, r es raíz de la ecuación característica de multiplicidad m, entonces

   $$a_n^p = n^m q(n) r^n,$$

   siendo $q(n)$ y $p(n)$ polinomios del mismo grado.

Ecuación característica generalizada:

Una recurrencia lineal no homogénea puede resolverse, también, asociando a la misma una ecuación característica que denominaremos generalizada. Esto puede hacerse siempre que el término no homogéneo sea de la forma

$$\sum_{j=1}^{m} p_j(n) r_j^n,$$

es decir, de la forma estudiada previamente.

Definición 4.4.-*Dada la recurrencia lineal no homogénea*

$$a_{n+k} = c_1 a_{n+k-1} + c_2 a_{n+k-2} + \cdots + c_k a_n + f(n),$$

donde $f(n) = \sum_{j=1}^{m} p_j(n) r_j^n$ *y* $p_j(n)$ *es un polinomio en* n *de grado* g_j*, decimos que la* ecuación característica generalizada de la recurrencia *es*

$$(\lambda^k - c_1\lambda^{k-1} - \cdots - c_k) \prod_{j=1}^{m} (\lambda - r_j)^{g_j+1} = 0.$$

Es importante hacer notar que esta ecuación se obtiene a partir de la ecuación característica de la recurrencia lineal homogénea multiplicando por factores de la forma $(\lambda - r_j)$. De esta forma podemos considerar la ecuación característica generalizada como la correspondiente a una recurrencia lineal homogénea, sólo que ahora el grado se ha incrementado de k a $k + \sum_{j=1}^{m}(g_j + 1)$. De hecho, se puede probar que esta ecuación corresponde a la de la recurrencia lineal homogénea que resulta al eliminar $f(n)$ mediante manipulaciones convenientes, como ya se hizo para el caso de los Ejemplos 4.1 y 4.2.

Sean λ_1, λ_2, ..., λ_s las raíces de la ecuación característica generalizada con multiplicidades α_1, α_2, ..., α_s respectivamente. Entonces la solución de la recurrencia se expresa de la forma

$$a_n = \sum_{j=1}^{s} q_j(n)\lambda_j^n,$$

donde $q_j(n)$ es un polinomio en n de grado $\alpha_j - 1$. Los coeficientes de estos polinomios se determinan una vez se conocen los $k + \sum_{j=1}^{m}(g_j + 1)$ primeros términos de la recurrencia.

Nótese que, como la recurrencia original es de orden k, basta con conocer los k primeros términos de la misma. Los términos extra que se necesitan, debido a la ecuación característica generalizada, pueden obtenerse a partir de la propia fórmula de recurrencia.

Funciones generadoras y recurrencias lineales:

Las funciones generadoras pueden usarse también para encontrar una fórmula explícita que nos dé el término general de una recurrencia lineal. Así, si (a_n) son los términos de la recurrencia, buscamos la función generadora

$$F(x) = \sum_{n=1}^{\infty} a_n x^n.$$

La expresión de $F(x)$ podrá determinarse gracias a la relación de recurrencia, lo que dará lugar a una fórmula para el cálculo de los términos a_n de la sucesión.

Tema 6: Teoría de grafos

Grafo y tipos de grafos

Definición 5.1.- *Un* grafo $G = (V, E)$ *consiste en un conjunto finito* V, *cuyos elementos reciben el nombre de* vértices, *y un conjunto* E *de pares de elementos de* V, *cuyos elementos se conocen como* aristas. *Si* $\{u, v\}$ *es una arista de* G, *se dice que los vértices* u *y* v *son* adyacentes *y llamaremos a* u *y* v extremos *de la arista.*

Existen algunas variaciones de la idea de grafo (véase la figura 5.2), como las siguientes:

- *Multigrafos*, grafos con, posiblemente, varias aristas entre dos vértices.
- *Pseudografos*, grafos en donde se permiten aristas cuyos extremos coinciden (*lazos*).
- *Digrafos* o *grafos dirigidos*, grafos en los que se asigna un orden a los extremos de cada arista. En este caso, las aristas dirigidas se denotan de la forma (a, b) y se ha de entender que el orden es importante ($(a, b) \neq (b, a)$). En el caso de una arista dirigida (a, b), al vértice a se le llama *origen* o *fuente* de la arista y al vértice b se le llama *término* o *vértice terminal* de la arista.

Nos referiremos a un *grafo simple* cuando se trate de un grafo no dirigido que además no es multigrafo ni psedografo. En este texto nos dedicaremos fundamentalmente al estudio de los grafos simples, aunque muchos resultados puedan ser extendidos a multigrafos, pseudografos y digrafos.

Grado de un vértice:

Definición 5.2.- *El* grado *de un vértice* v, *que denotaremos por* $\delta(v)$, *de un grafo* $G = (V, E)$ *es el número de aristas de* G *que confluyen en* v. *En el caso de los pseudografos, cada lazo contribuye dos veces al grado del vértice correspondiente. Además, diremos que un grafo* $G = (V, E)$, *con* $|V| = n$, *es* regular *(de grado* r*) si* $\delta(x) = \delta(y) = r < n$ *para todo* $x, y \in V$.

Grafo completo:

Definición 5.3.- *Un grafo en el que cada uno de sus vértices está unido con los demás vértices se llama* grafo completo *(véase la figura 5.3). Se denota* K_n *al grafo completo con* n *vértices. Es sencillo comprobar que el número de aristas de* K_n *es* $C(n, 2) = n(n-1)/2$.

Grafo bipartido

Definición 5.4.- *Un grafo* $G = (V, E)$ *se denomina* bipartido *si* $V = V_1 \cup V_2$ *con* $V_1 \cap V_2 = \emptyset$ *y cada arista de* G *es de la forma* $\{x, y\}$ *con* $x \in V_1$ *e* $y \in V_2$. *Si cada vértice de* V_1 *está unido con todo vértice de* V_2 *y viceversa, se tiene un grafo* bipartido completo*; si* $|V_1| = m$ *y* $|V_2| = n$, *el grafo se denota por* $K_{m,n}$. *Evidentemente,* $K_{m,n} = K_{n,m}$.

Ciclo

Definición 5.5.- *Si los vértices de un grafo son* $V = \{v_1, \ldots, v_n\}$ *y las aristas son* $E = \{\{v_1, v_2\}, \{v_2, v_3\}, \ldots, \{v_{n-1}, v_n\}, \{v$ *al grafo correspondiente se le llama* ciclo *de* n *vértices y se le denota por* C_n *(véase la figura 5.5).*

Matriz de adyacencia

Definición 5.8.- *Dado un grafo $G = (V, E)$ con $V = \{v_1, v_2, \ldots, v_p\}$, se denomina* matriz de adyacencia *a la matriz $M = (m_{ij})$ de orden $p \times p$ verificando*

$$\begin{array}{ll} m_{ij} = 1 & \{v_i, v_j\} \in E, \\ m_{ij} = 0 & \{v_i, v_j\} \notin E. \end{array}$$

Por ejemplo, las matrices de adyacencia del grafo completo K_5 y del grafo bipartido $K_{4,4}$ son:

$$K_5 = \begin{pmatrix} 0 & 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 1 & 1 \\ 1 & 1 & 0 & 1 & 1 \\ 1 & 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 1 & 0 \end{pmatrix} \qquad K_{4,4} = \begin{pmatrix} 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \end{pmatrix}$$

Obsérvese que la matriz de adyacencia de un grafo simple es simétrica ($m_{ij} = m_{ji}$ para todo i, j) y además los elementos de la diagonal principal son cero, $a_{ii} = 0$ para todo i.

También se puede definir la matriz de adyacencia para pseudografos (aparece un 1 en la posición a_{ii} si en el vértice v_i hay un lazo), multigrafos (indicando en la posición a_{ij} el número de aristas que unen los vértices v_i y v_j) y grafos dirigidos (en este caso, la matriz puede dejar de ser simétrica).

Finalizamos esta sección con algunos resultados generales sobre grafos. El primero de ellos relaciona los grados de los vértices con el número de aristas y constituye una aplicación de los principios básicos de conteo.

Cálculo del número de aristas:

Teorema 5.1.- *La suma de los grados $\delta(v)$ para todos los vértices v de un grafo $G = (V, E)$ es igual al doble del número de aristas:*

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

Un grafo es impar si el grado es impar, y un grafo es par entonces es que el grado de este es impar.

Isomorfismos

Definición 5.9.- *Dos grafos $G_1 = (V_1, E_1)$ y $G_2 = (V_2, E_2)$ son* isomorfos *si existe una aplicación biyectiva α entre V_1 y V_2 tal que $\{x, y\} \in E_1$ si y sólo si $\{\alpha(x), \alpha(y)\} \in E_2$. A la biyección α se le denomina* isomorfismo.

Subgrafo

Grafo formado por un subconjunto de vértices y aristas de un grafo G = (V, E)

Propiedades de grados:

1. Grado de un vértice es una propiedad que se conserva con el isomorfismo.
2. Si dos grados son isomorfos, también lo son los correspondientes subgrafos
3. Dos grafos G1 y G2 son isomorfos si, y solo si, sus complementarios son isomorfos.

Matriz de permutación:

Matriz cuadrada formada por ceros y unos de modo que solo hay un 1 en cada fila y columna.

Por ejemplo, las siguientes matrices son de permutación:

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}.$$

Teorema 5.4.- *Sean G_1 y G_2 dos grafos tales que sus correspondientes matrices de adyacencia son M_1 y M_2. Entonces G_1 y G_2 son isomorfos si y sólo si existe una matriz de permutación P tal que $M_2 = P^{-1}M_1P$.*

Grafos eulerianos

Definición 5.13.- *Un recorrido en un grafo $G = (V, E)$ es una sucesión de vértices de G*

$$v_0, v_1, v_2, \ldots, v_n,$$

tales que v_i y v_{i+1} son adyacentes $(0 \leq i < n)$.

Grafo conexo:

Grafos que tienen una única componente, es decir, que dos vértices se pueden unir por un camino.

Teorema 5.5.- *Sea $M = (m_{ij})$ la matriz de adyacencia de un grafo G. Entonces, el elemento ij de la matriz M^k nos da el número de recorridos de longitud k entre los vértices v_i y v_j.*

Una consecuencia de este resultado es el siguiente:

Corolario 5.6.- *Sea $M = (m_{ij})$ la matriz de adyacencia de un grafo conexo G. Entonces la distancia entre los vértices v_i y v_j es igual a k si y sólo si k es el menor entero no negativo que cumple que el elemento ij de la matriz M^k es distinto de cero.*

Recorrido euleriano:

Recorrido que contiene todas las aristas del grafo una sola vez. Si el recorrido es cerrado, se denomina circuito euleriano. Todos los vertices de un grafo euleriano tiene grado par. Si G es un grafo conexo y todos sus vertices tienen grado par, entonces admite un circuito euleriano.

Grafos hamiltonianos:

Se dice que un grafo G = (V, E) tiene un ciclo hamiltoniano si existe un ciclo de G que contiene a todos los vértices de V. Un camino hamiltoniano es un camino de G que contiene todos los vértices. Un grafo que contiene un ciclo hamiltoniano se llama grafo hamiltoniano.

Teorema 5.9.- (Condición suficiente) *Sea $G = (V, E)$ un grafo conexo con $|V| = n \geq 3$. Si $\delta(x) + \delta(y) \geq n - 1$ para todo x e y de V, con $x \neq y$, entonces G tiene un camino hamiltoniano. Como consecuencia de esto, si $\delta(v) \geq (n-1)/2$ para todo $v \in V$, entonces G tiene un camino hamiltoniano. Además si $\delta(v) \geq n/2$ para todo $v \in V$, entonces G es hamiltoniano.*

La condición que asegura que G es hamiltoniano si $\delta(v) \geq n/2$ para todo $v \in V$, se conoce como Teorema de Dirac. Una aplicación inmediata de este resultado permite comprobar que los grafos completos K_n son hamiltonianos para $n \geq 3$. En efecto, como $\delta(v) = n - 1$ para todo $v \in V$, se tiene que $n - 1 \geq n/2$.

Teorema 5.10.- (Condición necesaria) *Sea un grafo hamiltoniano $G = (V, E)$ con $|V| \geq 3$. Entonces para cada subconjunto U de V, el subgrafo de G cuyos vértices son los de $V \setminus U$ y cuyas aristas son las que tienen extremos en $V \setminus U$, tiene a lo sumo $|U|$ componentes.*

Un caso particular de este resultado, más sencillo de aplicar en la práctica, nos proporciona un criterio para determinar cuándo un grafo no es hamiltoniano.

Se llama punto de corte en un grafo a un vértice v tal que al eliminar v y las aristas que lo tienen por extremo, el grafo resultante resulta disconexo. Entonces un grafo hamiltoniano no tiene puntos de corte. Puede haber grafos sin puntos de corte que no sean hamiltonianos.

Reglas para saber si un grafo es o no hamiltoniano:

1. Si G tiene un ciclo hamiltoniano, entonces para todo $v \in V$, $\delta(v) \geq 2$.

2. Si $v \in V$ y $\delta(v) = 2$, entonces las dos aristas incidentes en v pertenecen a cualquier posible ciclo hamiltoniano.

3. Si $v \in V$ y $\delta(v) > 2$, entonces cuando se intenta construir un ciclo hamiltoniano, una vez que se pase por v, las aristas no utilizadas incidentes en v dejan de tenerse en cuenta.

4. Construyendo un ciclo hamiltoniano no puede obtenerse un ciclo para un subgrafo, a menos que contenga a todos los vértices.

Grafo completo de n vértices, hay $\frac{(n-1)!}{2}$ ciclos hamiltonianos.

Grafos planos:

Un grafo plano es un grafo que se puede dibujar intersecándose solo en los vértices de G. Un mapa es una representación geométrica de un grafo en la que las aristas solo se cortan en los vértices. Los mapas dividen al plano en varias regiones, Un no acotada que se llama región exterior. El grado de la región R es la longitud del camino cerrado que la bordea.

Teorema 5.12.- *Sean $R_1, R_2, \ldots, R_n$ las regiones de un mapa conexo. Entonces*

$$\delta(R_1) + \cdots + \delta(R_n) = 2|E|,$$

siendo $|E|$ el número de aristas del grafo.

Formula de Euler:

Para todo polihedro regular se cumple la siguiente relacion:

c + v = e + 2

Siendo c el numero de caras, v el numero de vertices y e el numero de aristas del poliedro.

Teorema 5.14 *Sea $G = (V, E)$ un grafo plano conexo con más de 3 vértices. Entonces,*

$$|E| \leq 3(|V| - 2).$$

Teorema 5.15 *Sea $G = (V, E)$ un grafo plano conexo con más de 3 vértices y tal que no contiene a ningún subgrafo isomorfo a K_3 (es decir, no contiene triángulos). Entonces*

$$|E| \leq 2(|V| - 2).$$

Grafos homeomorfos:

Definición 5.19.- *Dos grafos G_1 y G_2 se dice que son* homeomorfos *si G_2 se puede obtener de G_1 por la inserción o eliminación de vértices de grado 2.*

Una subdivisión elemental *de un grafo G es un nuevo grafo que se obtiene al insertar vértices de grado 2 en las aristas de G.*

Teorema 5.16.- (Teorema de Kuratowski) *Un grafo es plano si, y sólo si, no contiene ningún subgrafo homeomorfo a K_5 o a $K_{3,3}$.*

Un enunciado equivalente es el siguiente: Un grafo es plano si, y sólo si, no contiene ningún subgrafo que es una subdivisión elemental de K_5 o de $K_{3,3}$.

Coloración de grafos:

Definición 5.20.- *Una* coloración de vértices *de un grafo $G = (V, E)$ es una función $c : V \longrightarrow \mathbb{N}$ tal que $c(x) \neq c(y)$ siempre que $\{x, y\} \in E$. El* número cromático *de G, que denotaremos por $\chi(G)$, se define como el menor entero k tal que existe una coloración de vértices de G con k colores. En otras palabras, $\chi(G) = k$ si, y sólo si, existe una función de coloración c de V en $\mathbb{N}_k = \{1, 2, \ldots, k\}$ y k es el menor entero con esa propiedad.*

Polinomio cromático:

Definición 5.21.- *El polinomio cromático P_G de un grafo G es un polinomio tal que, para cada entero positivo k, $P_G(k)$ indica el número de k-coloraciones diferentes de G.*

El siguiente resultado nos permite encontrar el número cromático $\chi(G)$ de un grafo con la ayuda del polinomio cromático.

Numero cromático:

Teorema 5.17.- *El número cromático $\chi(G)$ de un grafo es el menor entero positivo, k, que hace que*

$$P_G(k) > 0.$$

En los siguientes ejemplos mostramos cómo encontrar el número cromático $\chi(G)$ a partir del polinomio cromático para algunos casos sencillos.

Relación de recurrencia para el polinomio cromático.

Teorema 5.18.- (Relación de recurrencia para el polinomio cromático) *Sean x e y dos vértices no adyacentes de un grafo conexo $G = (V, E)$. Definimos G^+_{xy} como el grafo que se obtiene al añadir la arista $\{x, y\}$ a G. Definimos G^-_{xy} como el grafo que se obtiene al hacer coincidir x e y en un sólo vértice que es adyacente a todos los vértices que eran adyacentes a x o a y en G. Entonces,*

$$P_G(k) = P_{G^+_{xy}}(k) + P_{G^-_{xy}}(k).$$

Descomposición del polinomio cromático.

Corolario 5.19.- (Descomposición del polinomio cromático) *Si x e y son dos vértices adyacentes de un grafo conexo $H = (V, E)$ y denotamos por H^1_{xy} al grafo que se obtiene al eliminar la arista $\{x, y\}$ en H, H^2_{xy} al grafo que se obtiene al hacer coincidir x e y en un sólo vértice que es adyacente a todos los vértices que eran adyacentes a x o a y en H. Entonces,*

$$P_H(k) = P_{H^1_{xy}}(k) - P_{H^2_{xy}}(k).$$

Teorema 5.21.- *Son equivalentes las siguientes afirmaciones:*

i) *G es un grafo bipartido.*

ii) $\chi(G) = 2$.

iii) *G no contiene ciclos de longitud impar.*

Teorema de Brooks:

Teorema 5.22.- (Teorema de Brook) *Sea G un grafo, con $G \neq C_{2n+1}$ (G no es un ciclo de longitud impar) y $G \neq K_n$ (G no es un grafo completo). Entonces $\chi(G) \leq d$ donde d es el máximo de los grados de los vértices de G.*

Emparejamiento:

Definición 5.22.- *Un emparejamiento en un grafo bipartido $G = (X \cup Y, E)$ es un subconjunto M de E con la propiedad de que dos aristas de M nunca tienen un vértice en común. Diremos que M es un emparejamiento máximo si ningún otro emparejamiento tiene cardinal mayor. Si $|M| = |X|$ diremos que M es un emparejamiento completo.*

Deficiencia de un grafo bipartido:

$$d = \max_{A \subseteq X}\{|A| - |T(A)|\}.$$

Tema 7: Arboles

Árbol:

Grafo T conexo sin ciclos. Un árbol con raíz es un par (T, v*) donde T es un árbol y v* es un vértice de T que recibe el nombre de raíz. Una hoja es un vértice de grado 1 que no sea la raíz; cualquier otro vértice se denomina interno o de decisión. La raíz es un vértice interno.

Propiedades de los árboles:

Teorema 6.1.- (Propiedades de los árboles) *Si $T = (V, E)$ es un árbol con $|V| \geq 2$, entonces:*

1. *Para cada par de vértices x e y, existe un único camino de x a y en T.*
2. *El grafo que se obtiene de T al eliminar cualquier arista tiene dos componentes conexas, cada una de los cuales es un árbol.*
3. *Si añadimos una arista cualquiera a T, se forma un ciclo.*
4. $|E| = |V| - 1$.
5. $\sum_{v \in V} \delta(v) = 2|V| - 2$.

Sea (T, v*) un árbol con raíz, el nivel de un vértice x de T a la longitud del único camino entre v* y x. La altura h de T es el máximo de los niveles de los vértices. Si todas las hojas del árbol se encuentran en los niveles h y h-1, diremos que el árbol es equilibrado.

Si T es un árbol m-ario con n vértices e i vértices internos, entonces n =mi+1.

Fórmulas para calcular el número de vértices, vértices internos y hojas

Corolario 6.3.- *Si T es un árbol m-ario con n vértices, de los cuales i vértices son internos y l son hojas, se tiene que*

(a) *Dado i, entonces* $l = (m-1)i + 1$ *y* $n = mi + 1$.

(b) *Dado l, entonces* $i = (l-1)/(m-1)$ *y* $n = (ml-1)/(m-1)$.

(c) *Dado n, entonces* $i = (n-1)/m$ *y* $l = [(m-1)n + 1]/m$.

Teorema 6.4.- *Si T es un árbol m-ario de altura h, entonces:*

(a) $l \leq m^h$, *y si todas las hojas del árbol están en el nivel h,* $l = m^h$.

(b) $h \geq \lceil \log_m l \rceil = \lceil \ln l / \ln m \rceil$. *Además, si el árbol es equilibrado, se tiene que*

$$h = \lceil \log_m l \rceil = \lceil \ln l / \ln m \rceil,$$

donde $\lceil r \rceil$ es el «redondeo por exceso» de un número real $r \in \mathbb{R}$, es decir, $\lceil r \rceil$ es el menor entero p que satisface $r \leq p$.

Arboles generadores y algoritmos de búsqueda:

Árbol generador o árbol maximal T de un grafo G es un subgrafo de G que es un árbol y contiene a todos los vértices de G.

Procedimiento de búsqueda en profundidad (pila) o DFS:

1. Vértice inicial x+ v*
2. Si el vértice activo x tiene nuevos adyacentes se elije uno de ellos (y) y se añade {x, y} a W
3. Sustituir x por y como nuevo vértice activo
4. Si no hay vértices adyacentes a x, se retrocede al vértice que te llevo hasta x

5. En algún momento del proceso nos hallaremos de nuevo en v* sin poder hallar un nuevo vértice.
6. W=T

Toda arista de T se recorre dos veces, 1 avanza y otra retrocede.

Proceso de búsqueda en anchura (Cola) o BFS:

Árbol con raíz (T, v*), se sale de la raíz v* del árbol, se genera el árbol W con el siguiente algoritmo:

1. Vértice inicial, x=v*
2. Si x tiene vértices adyacentes, se escoge una de ellas (y) y se añade la arista {x, y} a W
3. Cuando no haya nuevos adyacentes, se pasa el siguiente vértice en orden de aparición.
4. Cuando el vértice no tiene nuevos adyacentes y no existe vértice siguiente, W=T

Este algoritmo se usa para encontrar el camino mas corto entre dos vértices dados.

Algoritmos para arboles generadores minimales:

Algoritmo de Krustal:

Dado un conjunto k vacío, con n-aristas:

1. Se añade a k la arista menor peso que no forma un ciclo con las aristas que ya están en k.
2. Se repite el paso 1 hasta que haya n-1 aristas.

Algoritmo de Prim:

Dado un árbol T, con n-aristas.

1. Añadir a T la arista con menor peso entre un vértice de T y uno que no está en T.
2. Se repite el paso 1 hasta que haya n-1 aristas
   El árbol inicial es el de las aristas de menor peso.

Algoritmo de Dijkstra:

Supongamos que hemos comprobado que el camino mas corte de un vértice v a un vértice p tiene longitud f(p).

Supongamos que y es adyacente a p y que solo conocemos una estimación l(y) de la longitud del camino más corto de v a y.

La ruta mas corta de v a y, a través de p, tiene longitud l(p) + w ({p, y}) y, si esta es menor que l(y), podemos mejorar la estimación asignando a l(y) un nuevo valor igual a

min { l(y), l(p) + w({p, y}) }

Algoritmo del vecino más próximo

Dado un grafo completo de n vértices ponderado construiremos un ciclo hamiltoniano.

1. Elegimos cualquier vértice como principio del ciclo C1 que es de un solo vértice
2. Dado el ciclo de k vértices Ck con k ≥1, buscamos el vértice yk que no esta en Ck y que este mas cerca de Ck (lo llamamos Xk)
3. Sea C(k+1) el ciclo de k+1 vértices que se obtiene insertando yk inmediatamente antes de xk en Ck.
4. Repetir 2) y 3) hasta obtener un ciclo hamiltoniano.