MATEMATICAS DISCRETAS

1. **Teoría de números**
   * + Principio de la buena ordenanza
       - Todo subconjunto no vacío de números enteros no negativos tiene un primer elemento (es decir, tiene un elemento que es menor que todos los demás)
   * **Algoritmo de división y**
     + Sean a y b dos enteros.
       - Llamaremos diferencia a – b de estos dos enteros a otros de que satisfagan la igualdad a = b + d
       - Si a 0 y b = a . q para algún q, diremos que a divide a b. otras expresiones equivalentes son a es un divisor de b, a es un factor de b, b es múltiplo de a. si a divide a b. escribimos a | b.
       - Diremos que b > a si existe un numero natural n tal que b = a + n. Diremos que b a si b > a o b = a
     + Propiedades: sean a, b, c números enteros:
       - 0 . a = 0
       - a ( -b ) = -a . b
       - si a 0 y ab = ac, entonces b = c
       - si a 0 y a | b, entonces a | bx para cada entero x
       - sean a 0 y b 0, si a | b y b | c entonces a | c
       - sean a 0. Si a | b y a | c , se verifica que a | (bx + cy ) para cualquier par de enteros x e y
       - sean a y b positivos. Si a | b entonces a b
       - sean a 0 y b 0. Si a | b y b | a, se tiene que a = b o a = -b
     + llamaremos valor absoluto a la aplicación | | : Z -> Z , definida por |n| = n si n 0 o |n| = -n si n < 0
       - obsérvese que la aplicación esta bien definida, es decir todo numero entero tiene imagen mediante | | y esta imagen es única.
     + Propiedad del valor absoluto
       - |n| N {0}
       - |n| = 0 si y solo si n = 0
       - |a . b| = |a|.|b|
       - |a + b| |a| +|b|
       - Si a 0 , b 0 y a|b entonces |a| |b|
     + Teorema (algoritmo de la división)
       - Sean a Z y b N. entonces existen números enteros q y r tales que a = bq + r con 0 r b. además q y r son únicos.
       - A los números a, b, y r del teorema anterior se les suele llamar dividendo, divisor, cociente y resto.
       - Dados dos enteros a y b con b 0 entonces existen q y r tales que a = bq + r donde 0 r < |b|. Además, q y r son únicos.
     + Sean a y b numeros enteros con b 0. Sea a = bq + r donde 0 r < |b|. definimos el operador madulo “MOD” por a MOD b = r
     + Propiedades del operador MOD
       - Sean a, b, c, d y m numero enteros con m 0 . si a MOD m = c MOD m y b MOD m = d MOD m entonces:
         * (a + b) MOD m = (c + d) MOD m
         * (ab) MOD m = (cd) MOD m.
     + sean a1, a 2, …, an, números enteros. Llamaremos máximo común divisor de a1, a2, …, an al bipartdivisor común d > 0 tal que cualquier otro divisor común de a1, a2, … , an divide también a d. se designara mediante m.c.d.(a1, … , an).
     + Sean a y b enteros distintos de 0. Entonces existe un único d máximo común divisor de a y b. Además, d es el entero positivo mas pequeño que puede expresarse en la forma ax + by donde x e y son números enteros.
     + Sean a y b enteros distintos de 0. Entonces m.c.d.(a,b) = 1 si y solo si existen enteros s y t tales que as + bt = 1
     + Dados dos números enteros a y b. con b 0
       - Los divisores comunes de a y b son divisores del resto r de la división de a por b
       - Los divisores de b y del resto r son divisores de a
     + el máximo común divisor del dividendo y del divisor de una división es el mismo que el máximo común divisor del divisor y del resto.
   * **Algoritmo de Euclides**
     + Del teorema anterior podemos obtener un algoritmo para el cálculo del m. c. d de dos numero a y b. como m.c.d(a,b) = m.c.d(|a|,|b|), podemos suponer sin pérdida de generalidad que a b > 0. Dividimos a por b a=bq1 + r1 con 0 r1 < d. si r1 = 0 es obvio que b = m.c.d (a,b). así pues supongamos que r 0 ; dividiendo b por r1 podemos escribir b = r1q2 + r2 con 0 r2 < r1. Si r2 = 0 entonces m.c.d(b,r1) = m.c.d(a,b) = r1 y hemos terminado. Si r2 0 efectuamos la división de r1 por r2. Vamos obteniendo así un conjunto de números r1>r2>…>r1>…, puesto que cada uno de los numero r1, r2,…, ri,… es mayor o igual que cero, este conjunto de números no puesde ser infinito. En algún momento llegaremos a un resto es cero. Sea dicho resto rn = 0 para algún n, entonces rn-1 = m.c.d.(rn-2,rn-1) = m.c.d.(rn-3,rn-2) = …= m.c.d(b,r1) = m.c.d.(a,b)
     + Si k> 0 entonces m.c.d.(ka, kb) = m.c.d.(a,b).
     + Para cada entero k 0 m.c.d.(ka,kb) = |k| m.c.d.(a,b).
   * **Números primos y teorema fundamental de la aritmética**
     + Dado un numero entero p>1, diremos que p es un numero primo (o simplemente primo), si 1 y p son los únicos divisores positivos de p. un entero a> 1 que es no primo le denominaremos número compuesto.
     + Sean a1,…,an una familia de números enteros. Diremos que los a1,…,an son primo entre si, si se tiene que m.c.d.(a1,…,an) = 1
     + Lema de Euclides
       - Sean a,b y c números enteros. Supongamos que a y c son primos entres si y que c | ab. Entonces c| b.
     + Sea p un numero entero que 1. Las afirmaciones siguientes son equivalentes:
       - el numero p es primo
       - para cualquier par a y b de números enteros, si p | ab entonces p | a o p | b
     + sea p un numero primo. Si p|a1a2 … ar entonces p | ai para algún i
     + teorema fundamental de la aritmética
       - sea n un numero mayor que 1. Entonces existen números primos p1,…,pr tales que n=p1p2 … pr donde p1p2 … pr. Además, esta factorización es única en el siguiente sentido. Sean q1,…,q2 números primos con q1q2 … qs y tales que n=q1 … qs , entonces r=s y qi=pi para cada i = 1,2,…,r
     + sean n Z con |n| > 1. Entonces n tiene una factorización única de la forma n = … , donde t 1, los pi son primos distintos con p1 < p2 < … < pt y αi 1 para 1 t. esta factorización se llama factorización canónica de n.
     + el número de primos es infinito
     + si pn es el n-esimo numero primo entonces pn . Este resultado se demostrará en la sección 1.3 mediante el principio de inducción.
     + Existen infinitos numero de la forma 4n + 3
     + Sea un entero mayor que 1, entonces si para todo número primo p , p no divide al número a, se verifica que a es primo.
     + El numero es irracional.
     + Por cada entero n > 0, existen al menos n enteros compuestos consecutivos.
     + Sea a = , donde algunos se los y βi pueden ser cero. Entonces m.c.d.(a,b) =
     + Sean a y b dos números enteros. Llamaremos mínimo común múltiplo de a y b al menor positivo que sea múltiplo de ambos. Lo designaremos m.c.m.(a,b).
     + Sea a = , donde algunos se los y βi pueden ser cero. Entonces m.c.m.(a,b) =
     + Sean a1, a2,…, an números enteros. Llamaremos mínimo común múltiplo de estos números y lo designaremos por m.c.m (a1,a2,…,an) al entero positivo mas pequeño que sea múltiplo de todos ellos.
     + Sean a y b enteros n nulos, entonces |a.b| = [m.c.f.(a,b)].[m.c.m.(a,b)]
     + Test de primalidad
       - Determinísticos
       - Probabilísticos
     + números primos grandes
     + Sea p un primo impar. Entonces cualquier divisor primo q de M(p), si existe, es de la forma q = 2kp+1.
   * **El principio de inducción** 
     + en las matemáticas aparecen muchos problemas que tienen la siguiente forma general:
       - sea P(n) una determinada propiedad acerca de un numero natural n.
       - se trata de probar que P(n) es verdadero para todo n N.
     + sea S un conjunto de números naturales que satisface las dos condiciones siguientes:
       - el numero 1 S.
       - para cada número k 1 si k S entonces k + 1 S
       - entonces el conjunto S es igual N
     + pasos que debemos seguir:
       - paso 1: definir el conjunto S = {n N tale sque P(n) es verdadera}
       - paso 2: probar que 1 S
       - paso 3: suponer que k para k 1 arbitrario
       - paso 4: demostrar entonces que k + 1 S.
     + supongamos que P es una propiedad para la cual se tiene
       - P (1), es decir el 1 satisface la propiedad P.
       - para cada k N, P(k) -> P(k+1)
       - entonces P(n) se satisface para todo n
     + sea n0 Z y sea M = {n Z, nno}. Sea S un subconjunto de M tal que
       - n0 S
       - para cada k n0 arbitrario, si k S entonces k+1 S. entonces S = M
     + sea n0 Z y supongamos que P es una propiedad para la cual
       - P(n0) es cierta, es decir el numero n0 satisface P>
       - Para cada k n0 arbitrario se tiene que si P(k) e cierta entonces P (k+1) es cierta. Entonces P(n) se satisface para todo entero n n0.
     + Sea S un conjunto de enteros positivos tales que
       - 1 S.
       - Para cada entero n > 1, si k  S para todo entero k tal que 1 k < n entonces n S. entonces S = N
     + Supongamos que P es una propiedad que se verifica
       - P (1) es cierta
       - Para cada entero n0 > 1 si P(k) es cierta para cada entero k con 1 k < n0 entonces P(n0) es cierta. Entonces P(n) se satisface para todo n
     + Sena n0 Z, M = {n Z, n n0} y S un subconjunto de M tal que
       - n0 S
       - Para cada n > n0 si k para todo entero k tal que n0 k < n entonces n S. S = M
     + Sean n0 Z y supongamos que P es una propiedad tal que
       - P(n0) es cierta
       - Para cada n1 > n0, si es cierta P(k) para todo k con n0 ≤ k < n1 entonces P(n1) es cierta. Entonces P(n) se satisfacen para todo n n0
   * **Ecuaciones diofánticas** 
     + Sean a, b y n números enteros. La ecuación lineal ax + by = n tiene solución entera x0 e y0 si y solo si d = m.c.d.(a,b) divide a n
     + Algoritmo para encontrar una solución.
     + Supongamos que a, b y n son entero no nulos y d = m.c.d.(a,b) divide a n. entonces la solución general de la ecuación ax + by = n tiene la forma {

Donde t Z y {x0, y0} es una solución.

* + - La ecuación diofántica con n> 0, tiene solución si y solo si n se puede factorizar como producto de dos números de la misma paridad, es decir ambos pares o ambos impares. Si existen, las soluciones de esta ecuación tienen la forma x =

Donde a y b recorren todos los pares de números de la misma paridad y tales que n = a.b

* + - algoritmo de factorización de Fermat.
    - Las soluciones de la ecuación pitagórica que satisfacen las condiciones m.c.d.(x,y,z) = 1, 2|x, x,y,z > 0,

Viene dadas por las fórmulas:

X= 2st

V=

Z=

Para naturales s, t con s > t tales que m.c.d.(s,t) = 1 y s y t tiene distinta paridad.

* + - la ecuación no tiene solución para números x, y, z naturales.
    - la ecuación no tiene solución para números x, y, z naturales.
    - la ecuación , k > 0 no tiene solución para números x, y, z naturales
  + **Congruencias**
    - El conjunto de los números enteros 0,1,2,…. M-1 se denomina conjunto de menores residuos no negativos de modulo m.
      * En general dada una colección de enteros a1,a2,a3…, am se dice que es un conjunto completo de residuos (o también sistema completo de residuos) modulo m si cada número entero es congruente con modulo m con uno y solo uno de los ai 1m o lo que es equivalente, si cada uno de los ai es congruente modulo m a uno y solo uno de los números 0, 1 2, …. m-1
    - Sean a y b dos números enteros, entonces ab mod(m) si y solo si al dividir a y b por m el resto obtenido es el mismo
    - Sean a,b, c, d, h, m Z con h o y m > 0 entonces
      * A a mod(m)
      * Si ab mod(m) entonces ba mod(m)
      * Si ab mod(m) y bc mod(m) entonces ac mod(m)
      * Si ab mod(m) y cd mod(m) entonces acb + c mod(m), ac mod(m)
      * Si a mod(m) entonces hahb mod(m)
      * Si h|a, h|b, m.c.d. (h,m) = 1 y ab mod(m) entonces mod(m)
      * Supongamos que para 1 se tiene que aibi mod(m), entonces .
      * Sean a y b números enteros y m1, m2, …, mr, enteros positivos. Sea M= m.c.m(m1, m2, …, mr). Si ab mod(mi), para todo i = 1,…, r, entonces ab mod(M)
      * Aplicaciones de las congruencias a los dígitos de control
        + Cadena de bits
        + Dígitos de control de publicaciones
        + Código de barras
        + Número de identificación fiscal
      * La ecuación axb mod(m) tiene solución si y solo si d divide a b donde d es el m.c.d. (a, m ). Además, el número de soluciones no congruentes modulo m es exactamente d.
      * Aplicación a la generación de números pseudoaleatorios.
      * Teorema (teorema chino del resto)
      * El sistema de congruencias aix 1, 2,…,k, done m.c.d.(mi,mj) = 1 si ij y m.c.d.(ai,mi) = 1, i=1, 2,…,k, tiene una única solución en cada conjunto completo de residuos modulo m1,m2…mk.
      * Aplicación a la aritmética computacional con enteros grandes.
      * Dado un numero natural m, se designa por (m) al numero de enteros positivos r que no exceden a m y son primos con m. la función (m) se denomina función de Euler.
      * Un sistema reducido de residuos modulo m, es una colección maximal de enteros a1, a2, … ,ar, tal que cada ai es primo con m y cada par de enteros ai y aj tiene diferentes resto modulo m
        + En la colección anterior {49, -19, -5,15} es un sistema reducido de residuos de 8
        + Es claro que cualesquiera dos sistemas reducidos de residuos modulo m tienen el mismo número de elementos, es decir, (m) elementos.
      * Si m y n son dos numeros enteros primos entre si, entonces (mn) = (m)(n)
      * Sean n = entonces:
      * Teorema (Euler) sean a y m dos números enteros con m ; entonces si m.c.d.(a, m) = 1 se tiene que 1 mod(m)
      * Pequeño teorema de Fermat
        + Si p es un numero primo que no divide al número a entonces 1 mod(p).
      * Teorema (Wilson)
        + Si p es un numero primo entonces (p-1)!-1 mod(p)
      * Cifrado de mensajes. Criptografía
        + El sistema cesar
        + El sistema RSA
  + **Sistemas de numeración y criterios de divisibilidad**
    - Sea b 2 un numero natural (llamado base). Entonces número n N puede escribirse de manera única en base b de la forma n = ,

Para algún k 0, con 0 ai < b , i = 0, 1, … , k, y con ak 0.

* + - De ahora en adelante cuando tengamos un numero

n = ,

en base b, escribiremos simplemente

n = (.

* + - Criterios de divisibilidad por k.

1. **Teoría de grafos**
   * **Grafos, dígrafos y multígrafos**
     + Un grafo G consta de un conjunto V y un conjunto E de pares no ordenados de elementos distintos de V, el conjunto V se llama el conjunto de vértices siendo sus elementos los vértices. El conjunto E se llama conjunto de aristas (´edge´ en ingles) y sus elementos aristas.

Se escribe G = (V,E) para designar el grafo G con conjuntos de vértices V y conjuntos de aristas E o bien dado un grafo G se denota por V(G) el conjunto de vértices de G y por E(G) el conjunto de aristas.

Dado un gráfico G=(V,E) sean u, v dos vértices de G es decir u,v V, si e = {u,v} es arista de G, {u, v} E, se dice que los vértices u y v son adyacentes y designaremos la arista por uv simplemente. También llamaremos a los vértices u y v, extremos de la arista uv.

* + - Existen algunas variaciones de la idea de grafo que son muy útiles y frecuentemente usadas. Así, un multígrafo es un grafo con (posiblemente) varias aristas entre dos vértices, por tanto en la definición formal de multígrafo, el conjunto de aristas puede contener algunas aristas distintas con el mismo par de extremos.
    - Otra variación del concepto de grafo es pseudografo. Al contrario que en un grafo en un pseudografo están permitidas aristas cuyos extremos coinciden. Tales aristas se denominan lazos
    - Otro concepto útil es el de disgrafo. Un disgrafo es un grafo donde a cada arista se le asigna un orden de sus extremos. El orden se indica en el dibujo del grafo con una flecha. Se llama origen al primer vértice de una arista y fin al segundo.
    - Por supuesto pueden aparecer multitud de variaciones de los conceptos anteriores como multidisgrafos o pseudomultigrafos.
    - Los matemáticos usan el termino isomorfismo para expresar que dos objetos son ” fundamentalmente iguales” o bien que su estructura matemática coincide mientras que posiblemente existen aspectos no esenciales como nombres de sus partes que son diferentes. En la siguiente definición se refleja con precisión lo que se entiende por isomorfia de grafos:
    - sean = (V, E) y G´ = (V’,E’) dos grafos y sea f: V -> V’ una biyeccion entre dos conjuntos de vértices tal que uv E si y solo si f(u)f(v) E’. la biyeccion f se denomina isomorfia de G a G’. se dice entonces que los grafos G y G’ son isomorfos.
    - Sea G un grafo y u un vértice de G. se llama grado de u en G. gr(u), al número de aristas de G que tiene al vértice u por extremo.
    - Sean G y G’ son dos grafos y f un isomorfismo entre G y G. si u es un vértice de G entonces gr(u) = gr(f(u))
    - Sean G = (V, E) un grafo, V = {v1,…, vp} el conjunto de vértices y #E el número de aristas entonces:

Por tanto todo grafo contiene un número par (o cero) de vértices de grado impar)

* + - Sea G = (V ,E) un grafo. Un subgrafo de G es cualquier grafo H = (V(H)), (E(H)) de modo que V(H) este contenido en V y E(H) está contenido en E.
      * Loa subgrafos de G se obtiene borrando o eliminado algunas aristas y vértices de G, de modo que si suprimimos un vértice hemos de borras todas las aristas que tiene tal vértice como extremo.
    - Un grafo se dice regular si todos sus vértices tienes el mismo grado. Si dicho grado es k entones el grafo se llama k-regular.
    - Un grafo para el que cualquiera par de vértices esa formado por los extremos de una arista se llama grafo completo.
    - Dos grafos completos con el mismo número de vértices son isomorfos.
    - Un autómata finito es un quinteto M = (Q, S, d, v, F), donde:
      * Q es un conjunto finito de posibles estados de M (es decir un conjunto finito cualquiera)
      * S es un alfabeto (otro conjunto finito cualquiera),
      * D es una aplicación de Q x S en Q que se llama función de transición, es en realidad el mecanismo de la máquina,
      * q Q es el estado inicial
      * F Q es el conjunto de estados finales.
  + **Grafos eulerianos y hamiltonianos**
    - sea G un grafo o un multígrafo. Un camino en G es una sucesión (finita) en la que aparecen alternadamente vértices y aristas de G:

donde cada arista tiene por extremos los vértices adyacentes en la sucesión.

* + - a los vértices v0 y vn se les denomina extremos del camino, también se dices que el camino conecta v0 con vn o que va de v0 a vn.
    - La longitud del camino es el numero n de aristas que contiene.
    - Un camino se dice que es cerrado si sus extremos coinciden, es decir v0 = vn.
    - En un grafo (pero no en un multígrafo) un camino puede ser especificado simplemente por la sucesión de los vértices: (v0,…, vn).
    - Un camino se dice que es simple si en la sucesión de vértices no hay ninguno repetido.
    - Un ciclo es un camino cerrado donde los únicos vértices repetidos son el primero y el ultimo, además, en el caso de caminos de longitud dos, solo consideramos ciclos a aquellos caminos cerrados en multígrafos que no repiten aristas.
    - Un circuito es un camino cerrado que no repite aristas.
    - En un grafo G si existe un camino que conecta dos vértices distintos x e y de Entonces un camino simple con extremos x e y.
    - Un grafo G es conexo si para cada par de vértices u, v existen un camino cuyos extremos son u y v. en caso contrario decimos que G es desconexo.
    - Sea G un grafo. Un camino (circuito) **euleriano** es un camino (Rep. Circuito) que contiene todas las aristas apareciendo cada una de ellas exactamente una vez. Un grafo que admite un circuito euleriano se denomina grafo euleriano.
      * El problema que resolvió Euler fie entonces más general pues encontró una caracterización de los grafos eulerianos.
      * Otro modo de entender que es un grafo euleriano es un camino en un grafo G es un modo de dibujar el camino sin levantar el lápiz del papel y sin pintar dos veces la misma arista.
    - Sea G un grafo. Si G es euleriano todo vértice de G tiene grado par.
    - Sea G un grafo. Si G tiene un camino euleriano entonces o bien todo vértice de G tiene grado par o bien exactamente dos de los vértices tiene grado impar.
    - Un grafo conexo es euleriano si y solo si cada vértice tiene grado par.
    - Sea H un grafo tal que todo vértice de H tiene grado par. Si u y v son dos vértices de H que son adyacentes entonces existe un circuito g que contiene la arista uv.
    - Un grafo conexo admite un camino euleriano no cerrado si y solo si exactamente dos vértices tienen grado impar.
    - sea G un grafo. Un camino simple en G que contiene todos los vértices de G se denomina camino **hamiltoniano**, un ciclo que a su vez es un camino hamiltoniano se denomina ciclo hamiltoniano, un grafo que contiene un ciclo hamiltoniano se denomina grafo hamiltoniano.
    - Sea G un grafo y u, v dos vértices de G. se dice que u y v están conectados en G si existe un camino de u a v.
    - En un grafo G la relación en el conjunto de vértices dada por “estar conectado con” es una relación de equivalencia.
    - Las clases de equivalencia que define la relación “estar conectado con” en un grafo G se denomina componentes conexas de G.
    - Sea G = (V ,E) un grafo tal que #V 3. Si G es hamiltoniano, entonces, para cada subconjunto U de V, el subgrafo de G cuyos vértices son los de V -U y sus aristas son todas las de G que tiene extremos en V -U, tiene a lo más #U componentes.
    - Sea G = (V, E) un grafo con #V = n > 2. Si para todo vértice v V se verifica que gr(v) , entonces G es hamiltoniano.
    - Sea G = (V, E) un grafo con #V = n. si gr(v) + gr(w) n-1 para todo v, w V, v w, entonces G tiene un camino hamiltoniano.
    - Sea G = (V, E) un grafo con #V = n> 1. Si para todo vértice v entonces G tiene un camino hamiltoniano.
  + **Exploración de grafos**
    - Sea G = (V, E) un grafo con V = {v1,…,vp}. Se denomina matriz adyacente a la matriz M = (mij) de orden pxp cuyas entradas son unos o ceros siguiendo la siguiente ley: mij = 1 si vi vj E Mij = 0 si vi vj E
    - para el caso de disgrafo se define la matriz adyacente del siguiente modo:
    - sea G = (V, E) un disgrafo con V = {v1,…,vp}. La matriz de adyacencia de G es la matriz M (mij) de orden pxp y con entradas unos y ceros definida por:
      * mij = 1 si vi vj y la orientación de tal arista es vi -> vj, (es decir el origen es vi y el fin es vj),
      * mij = 0 si vi vj E o bien vi vj E y la orientación de tal arista es G es vj -> vi
    - sean G y G’ dos grafos con la misma matriz adyacente, entonces G y G’ son isomorfos.
    - Sea G un disgrafo. Un camino en G es una sucesión (finita) en la que aparecen alternativamente vértices y aristas de G:

Donde cada arista vi vi+1 tiene por origen a vi y por fin a vi+1. A los vértices v0 y vn se les denomina origen y fin del camino respectivamente. El número de aristas del camino se denomina longitud.

* + - Seda M la matriz adyacente de un grafo(disgrafo) G con p vértices, p>1. Entonces la entrada (i, j) de la matriz Mn = M x ..n.. x M es el número de caminos de longitud n con extremos vi y vj (en el caso de disgrafo es el número de caminos de longitud n con origen vi y fin vj).
    - Sea M la matriz adyacente de un grafo G con p vértices, v1 ,…,vp, con p>1. Sea C = Mp-1 + Mp-2 +…+ M. existe un camino entre vi y vj si y solo si la entrada en el lugar (i, j) de la matriz C es no nula.
    - Sea M la matriz de adyacencia de un grafo con p vértices, p>2. Sea C Mp-1 + Mp-2 +…+ M. el grafo de G es conexo si y solo si todas las entradas de C son no nulas.
    - Un árbol es un grafo conexo sin ciclos
    - Un grafo T es un árbol, si y solo si, cada dos vértices distintos de T se conectan por un único camino simple.
    - Sea G un grafo conexo. Existe un árbol T que es un subgrafo de G de modo que el conjunto de vértices de G coincide con el de T. Un árbol T con la propiedad anterior de denomina subárbol conectan o subárbol máximo máxima de G.
    - Un árbol con raíz es un par (T, r) donde T es un árbol y r es un vértice de T que se llama raíz.

Un árbol con raíz define de modo natural una relación de orden (parcial) entre los vértices del árbol, de forma rápida, un vértice v será mayor que otro w si está más cerca que” w de la raíz r. es una relación de orden parcial porque en general no siempre se puede comparar dos vértices del árbol.

* + - Sea (T, r) un árbol con raíz y v, w dos vértices de T. se dice que v w si el camino simple que une r con w pasa por el vértice v.
    - La relación entre los vértices de un árbol con raíz (T, r) es una relación de orden. Es decir verifica las propiedades:
      * Reflexiva: v v para cada vértice de T
      * Antisimétrica: si v w y w v, entonces v = w
      * Transitiva: si u, v, w son tres vértices de T tales que u v y v w, entonces u w.
    - Un grafo o disgrafo G se dice que es un grafo etiquetado si sus aristas tienen asignado un número. Es decir si existen una aplicación d: E(G) -> C, donde C es un conjunto finito de números. A la etiqueta de una arista a de G se le suele designar longitud de a. dado un camino en G cuyas aristas son a1,…,ar, se denomina longitud de tal camino a d(a1) +…+ d(ar).
      * Obsérvese que si todas las etiquetas son 1 la definición de longitud en un grafo o disgrafo etiquetado coincide con la de longitud de un camino en un grafo o disgrafo. Dados dos vértices de un grafo etiquetado se denomina distancia entre tales vértices a la longitud del camino de longitud mínima entre dichos vértices.
    - Algoritmo de Dijkstra: sea G = (V,E) un disgrafo etiquetado, es decir tenemos d: E -> C donde C es un subconjunto finito de los números reales positivos ( y no nulos ). Sean x, y dos vértices de G. el siguiente algoritmo dará la distancia entre x e y:
      * Paso 1. Considérese la aplicación L V => R{} (donde R es el conjunto de los números reales), dad por L(x) = 0 y L(v) = para todo vértice de G, v, diferente de x. sea T = V. la aplicación L y el conjunto T irán transformándose en el curso del algoritmo.
      * Paso 2. Encuéntrese el vértice v T con etiqueta L(v) mínima
      * Paso 3. Si v = y la distancia entre x e y es L(y) y el algoritmo acaba.
      * Paso 4. Para todo w T tal que existe una arista vw con origen en v y fin en w, si L(w) > L(v) + d(vw) entonces redefínase el valor de L sobre w por L(w) = L(v) + d(vw)
      * Paso 5. Elimínese en el conjunto T el vértice v y volvamos al paso 2.
  + **Mapas y coloraciones**
    - Un grafo (multígrafo) se dice que es plano si admite una representación gráfica en el plano de modo que cada arista corta únicamente a otra arista en un vértice que sea extremo de ambas.
    - Sea G un grafo(multígrafo) plano, una representación del grafo en el plano en las condiciones … de denomina mapa. Diremos que el mapa es conexo si el grafo representa es conexo. Un mapa divide al plano en varias “parte” que se denomina regiones y su número lo representamos por #R.
    - Se denomina grado de una región a la longitud del camino que la bordea.
      * Así en el ejemplo … la región sombreada tiene grado 8
      * Existen un teorema análogo al primer teorema de la teoría de grafos para mapas:
    - La suma de los grados de las regiones de un mapa es al doble del número de aristas de un grafo que representa.
    - Teorema (formula de Euler) sea M un mapa conexo con #R regiones que represente el grafo G = (V, E), entonces: #V - #E + #R =2
    - Sea G = (V, E) un grafo plano conexo, con #V > 2. Entonces: #E 3 #V -6 .
    - Sea G = (V, E) un grafo plano, conexo, con #V > 2. Supongamos que en G no existe ningún subgrafo isomorfo a k3, entonces: #E 2#V – 4
    - Sea G = (V, E) un grafo u, v V y uv E. una subdivisión elemental del grafo G es un grafo G’=(V {w}, (E – {uv}) {uw, wv}) donde w V. es decir se trata de sustituir una arista uv de G’ por un nuevo vértice w unido con los extremos de la arista suprimida por dos nuevas aristas. en un mapa se trata simplemente de añadir un vértice sobre el interior de una arista existente ya. Una subdivisión de un grafo G es el grafo obtenido efectuando un numero finito (puede ser cero) de subdivisiones sucesivas.
    - Teorema de Kuratowski
      * Un grafo G es plano si y solo si no contiene ningún subgrafo que sea isomorfo a una subdivisión de k5 o k3,3.
    - Sea M un mapa que representa un grafo G, diremos que dos regiones diferentes de M son adyacentes si los caminos que bordean tales regiones tienen alguna artista en común. El pseudimultigrafo dual Gm de M se define como un pseudomultigrafo construido del siguiente modo: tomamos como conjunto de vértices las regiones de M y a cada artista e de G le asociamos una arista e\* de Gm de modo que si e separa las regiones adyacentes s, t de M (podría ser s=t) entonces e\* es un lazo)

El pseudomultigrafo dual Gm de un mapa M es un pseudomultigrafo plano pues se puede conseguir un mapa que represente Gm del siguiente modo:

* + - * cada vértice de Gm se representa por un punto en la región correspondiente de M, para representar cada arista de Gm dibujaremos un arco que una los dos puntos que representan las regiones de M adyacentes pasando sobre cada arista común de los caminos que bordean tales regiones.
    - Se H = (V,E) un grafo y C = {1,2,…,k} un conjunto de k colores. Una coloración con k colores del grafo G es una aplicación : V -> C, de modo que si u, v V y uv E entonces .
    - Todo grafo plano admite una coloración con cuatro colores.
    - Un grafo G = (V,E) se dice que es bipartito si existe una coloración con dos colores, : V->{0,1}. Normalmente se consideran los colores blanco y negro en lugar de 0 y 1.
    - Un grafo bipartito si y solo si no tiene ciclos con longitud impar.
    - Un clique en un grafo es un conjunto de vértices tal que para cada par de vértices de tal conjunto hay una arista en el grafo que los une, es decir, es el conjunto de vértices de un subgrafo que es un grafo completo,

el siguiente problema de teoría de grafos tiene una complejidad NP:

* + - * Dado un grafo finito G = (V, E) y un entero positivo m menor o igual al número de vértices, el grafo G tiene un clique con m vértices?

1. **Combinatoria**
   * **Técnicas básicas**
     + Teorema (principio de adición): sean A1, A2,…,An conjuntos finitos tales que Ai Aj = para cada i j, i, j {1, 2, …, n} entonces |A1A2An|=|a1|+…+|An|.
     + Teorema (principio de multiplicación): sean A1, A2,…,An conjuntos finitos no vacíos entonces, |A1A2An|=|A1||A2|…|An|.
       - Supongamos que un experimento consiste en seleccionar n objeto de manera que la primera elección consiste en elegir un elemento de un subconjunto de m1, objetos, la segunda elección consiste en elegir otro elemento de un subconjunto de m2 objetos y así sucesivamente. Para la elección n-esima se dispone de mn objetos. Entonces, la selección se puede realizar de m1m2…mn formas diferentes.
     + Teorema (principio de distribución): sean m,n y p números naturales. Si se distribuyen np+m objetos en n cajas entonces alguna caja deberá contener, al menos, p+1 objetos.
     + Dados n números enteros positivos m1, m2,…, mn tal que > p, entonces para algún 1 n se tiene que mi >p.
   * **Permutaciones, variaciones y combinaciones** 
     + Sea A un conjunto finito no vacío. Una permutación de A es una biyeccion de A en A. diremos que dos permutaciones son diferentes si las biyecciones son diferentes.
     + Sea 1 y dos permutaciones del conjunto A. llamaremos producto de 1 y y escribiremos 1., a la permutacon de A tal que: (a) = 2((a)) para todo a A.
     + El conjunto de todas las permutaciones de un conjunto A con la operación de producto tiene de estructura algebraica de grupo y se denomina grupo simétrico de A. se designa habitualmente por Sa.

Si A = {1,2,…,n} N, enotces denotaremos a Sa por Sn.

* + - Las permutaciones aparecen en una amplia variedad de contextos en matemáticas y en la construcción de modelos de los fenómenos físicos; especialmente cuando los datos que describen los acontecimientos se pueden situar en n casillas distintas que determinan la colección de n objetos. Si las localizaciones se numeran de a n, al proceso que mueve un objeto del lugar i al lugar j, se le puede asociar a una permutación de Sn tal que (i) = j.
    - Sean A y B conjuntos con n elementos cada uno. El número de biyecciones distintas se A a B es n.(n-1).(n-2)…2.1
      * El número de biyecciones distintas de A y B, que hemos visto que es igual al producto de los n primeros números naturales, se denota por n! (que se lee factorial de n)
      * Por convenio tomaremos 0! = 1
      * Cuando A = B las biyecciones son permutaciones de A. así pues se tiene el siguiente corolario:
    - El número de permutaciones de un conjunto de n, elementos que designaremos por P(n), es n!. Así |Sn|=n!.
    - Sean A un conjunto finito con n elementos (n>0) y r un numero natural rn. una variación de orden r de A es una lista ordenada (a1, a2, a3, …, ar) de elementos de A distintos. Diremos que dos variaciones son diferentes si algún elemento de una de las dos listas contiene los mismos elementos en distinto orden.
      * Designaremos el número de variaciones de orden r del conjunto A con n elementos por V(n,r). en ocasiones se utilizara la frase: V(n,r) es el número de variaciones de n elementos tomados de r en r.
    - Sean A y B dos conjuntos no vacíos con |A| = r,|B| = n y r n. entonces el nuemro de aplicaciones inyectivas de A a B es: N(N-1)…(n-r+1)=
    - Sean A un conjunto finito con n elementos (n>0) y r un numero natural r n . entonces el número de variaciones de orden r de A es V(n,r) =
    - Sean A un conjunto finito con n elementos (n>0) y r un numero natural. Una variación con repetición de orden r, de A es una lista ordenada (a1,a2,a3,…,ar) de elementos de A, en donde los elementos de pueden ser iguales. Diremos que dos variaciones con repetición diferentes si algún elemento de una las dos listas no se encuentran en la otras, o bien si las dos listas contienen los mismos elementos en distinto orden.
      * Designaremos el numero de variaciones con repetición de orden r del conjunto A con n elementos por VR(n,r). en ocasiones se utiliza la frase: VR(n,r) es el número de variaciones con repetición de n elementos tomados de r en r.
    - Sean A y B dos conjuntos no vacíos con |A| = r,|B|=n, entonces el número de aplicaciones de A a B es .
    - Sean A un conjunto finito con n elementos (n>0) y r un numero natural. Entonces el numero de variaciones con repetición de orden r de A es VR(n,r) =
    - Sean A un conjunto finito con n elementos (n>0) y r un numero natural r n. una combinación de orden r de A es una lista (a1, a2, a3, …, ar) de elementos de A distintos. Diremos que dos combinaciones son diferentes si algún elemento de una lista no se encuentra en la otra.
      * Designaremos el número de combinaciones de r elementos de A por C(n,r) o también por (esta notación fue introducida por Euler).

Llamaremos a numero combinatorio. En ocasiones se utiliza la frase: C(n,r) es el número de combinaciones de n elementos tomados de r en r.

* + - Para todo n N y para todo r, 1 n, V(n,r) = r!C(n,r) por lo tanto C(n,r) = .
    - Sean A un conjunto finito con n elementos (n>0) y r un numero natural. Una combinación con repeticiones de orden r de A es una lista (a1,a2,a3,…,ar) de elementos de A, donde los elementos pueden ser iguales. Diremos que dis combinaciones con repetición son diferentes si algún elemento de una la dos listas no se encuentra en la otra.
      * Designaremos el numero de combinaciones con repeticiones de orden r del conjunto A(|A|=n) por CR(n,r). en ocasiones se utiliza la frase: CR(n,r) es el número de combinaciones con repetición de n elementos tomados de r en r.
    - Sean k y n enteros positivos. El numero de soluciones enteras no negativas de la ecuación x1+x2+…+xn=k, es C(n+k-1nk).
    - El numero de combinaciones con repetición de orden k de un conjunto A de n elementos es CR(n,k) = C(n+k-1,k).
    - Una permutación circular de n objetos distintos de orden r, rn, es una colocación ordenada de r de los n objetos en r posiciones igualmente espaciados sobre una circunferencia.

Consideramos dos permutaciones iguales si una puede ser obtenida de la otra mediante una rotación apropiada de la circunferencia alrededor de su centro.

* + - El número de permutaciones circulares de n objetos distintos de orden r, rn es C(n,r).(r-1)!
    - Una permutación circular de n objetos distintos de orden n se denominará permutación circular de n objetos.
    - Reunimos a continuación un cuadro el contenido de esta sección.

|  |  |  |
| --- | --- | --- |
| Se elijen k objeto de un conjunto de n | Numero de selecciones ordenadas | Numero de selecciones no ordenadas |
| No están permitidas las repeticiones |  |  |
| Están permitidas las repeticiones |  |  |

* + **Teorema del binomio**
    - La generalización de este resultado para , conocido como el teorema del binomio, se demostrará tras una serie de resultados previos sobre números combinatorios.
    - Sean k y n números enteros tales que 0 entonces
    - Corolario (formula de pascal) si n y k son enteros tales que 1n-1, enotences .
    - Triangulo de pascal: la fórmula de pascal da un método para el cálculo de los coeficientes binomicos, dado el valor inicial para todo n0. Los coeficientes de las sucesivas potencias de se pueden distribuir en una figura como sigue, se conoce como el triángulo de pascal.

Desarrollando los números combinatorios se tiene

1

1 1

1 2 1

2 3 3 1

1 4 6 4 1

1 5 10 10 5 1

En el triangulo de pascal se tiene que:

* + - * El primer y ultimo elemento de cada fila es 1
      * Cualquier otro numero del triangulo de pascal se puede obtener sumando los dos números que aparecen encima de él.
    - Para cada n N y para cada par de números de elementos x, y R.
    - En el teorema anterior haciendo y = 1 obtenemos el siguiente corolario
      * Para cada n N y para cada elemento de x R.
    - Para cada elemento m, k m se tiene la siguiente igualdad:
    - Sean n, n1, n2,…, nk números enteros no negativos, con n = o negativos, con n = .Se define el coeficiente multinomico P(n, n1, n2,…,nk) como que también se escribe
    - Dados n objeto de k tipos, con ni objetos del tipo i, para 1 y con entonces hay , diferentes ordenaciones de estos n objetos. En donde consideramos que dos operaciones son iguales si para cada i, 1 , los objetos que ocupan el lugar i son del mismo tipo.
    - Formula de Leibnitz: los coeficientes multinoimicos surgen, al igual que los binomicos, de la consideración de expresiones algebraicas del tipo donde los xi son elementos del un cuerpo y n es un número natural.
  + **Principio de inclusión-exclusión**
    - El principio de inclusión-exclusión, a pesar de su apariencia de simplicidad, es una potente herramienta del análisis combinatorio; nos dice que si sabemos contar elementos de intersecciones de conjuntos, entonces podemos determinar el tamaño de la unión de dichos conjuntos. En su forma más simple, la relación entre el número de elementos de la unión de dos conjuntos A y B, el número de elementos de dichos conjuntos y el de la intersección es: |AB|=|A|+|B|-|AB|
    - Teorema (principio de inclusión-exclusión)

**|**

Donde para 2las sumas se extiende a todas las combinaciones de orden k, {i1,i2,…,ik},{1,2,…,n}.

* + - El número de elementos de S que satisfacen al menos una de las propiedades P1,P2,…,Pn es….
  + **Recursividad y relaciones recurrentes**
    - Un conjunto de objetos está definido recursivamente siempre que
      * 1.Se especifiquen de forma explícita algunos elementos del conjunto.
      * 2.Los demás elementos del conjunto se definan en términos de los elementos dados en 1
      * En el caso particular de funciones matemáticas definidas de N de R de tiene la siguiente definición.
    - Un función f: N -> R se dice que esta definida recursivamente, si para algún n0 N ,se verifica:
      * Los valores de f(1),f(2),…,f(n0) son conocidos
      * Para n>n0, f(n) esta definida en términos de f(1),f(2),…,f(n-1)
    - Los f(1)… se llaman valores o condiciones iniciales de f y nos referimos a la ecuación que describe f(n) en términos de f(1),f(2)….f(n-1) como una relación de recurrencia para f.
    - Una relación de recurrencia de la forma r(n) = a1 r(n-1) + a2 r(n-2)+…+ at r(n-t) + k(n), donde n t + 1 y a1, a2,…,at son constantes, se llama relación de recurrencia lineal con coeficientes constantes. Cuando k(n) = 0, diremos que la relación es lineal homogénea.
      * Se denomina lineal puesto que no aparecen productos de la función r(n), tales como (n-t).r(n-s),1
      * Un ejemplo de la relación de recurrencia que satisface la definición anterior es r(n)=6r(n-1)+8r(n-2)-4r(n-3)+3r(n-4)+. Para n 5 es lineal con coeficientes constantes.
    - Se denomina sucesión de Fibonacci a la sucesión obtenida a partir de la relación de recurrencia:
      * Fib(n) = fib(n-1)+fib(n-2) para n 3, Con condiciones iniciales fib(1)=1, fib(22) =2.
    - Sea r(n) – a1r(n-1) – a2r(n-2)- …- str(n-t)=0, con n>t+1, una relación de recurrencia lineal y homogénea de coeficientes constantes. Se denomina ecuación característica asociada a la ecuación recurrente a la expresión:
    - Sea r(n) – a1r(n-1)-a2r(n-2)-…-atr(n-t)=0, donde n > t+1, una relación de recurrencia lineal y homogénea de coeficientes constantes. Entonces r(n) = es una solución si y solo si b es una raíz de la ecuación característica.
    - La función fib(n), solución de la relación de recurrencia de Fibonacci: fib(n) = fib(n-1) + fib(n-2), para n 3,

Fib(1) = 1, fib(2) = 2, viene dada por fib(n)= (n 1)