MATEMÁTICA DISCRETA

(APUNTES)

UNED

MATEMÁTICAS

INGENIERÍA INFORMÁTICA

INGENIERÍA EN TECNOLOGÍAS DE LA INFORMACIÓN

Contenido

MATEMÁTICA DISCRETA
(APUNTES)

INTRODUCCIÓN

Estos apuntes son un resumen del texto oficial de la asignatura de Matemáticas discreta que se cursa en primero del Grado de Matemáticas de la UNED, así como optativa en cuarto de Ingeniería Informática y Ingeniería en Tecnologías de la Información de la misma universidad. En este resumen he incluido las definiciones y los teoremas, preposiciones y los corolarios sin las demostraciones. También he omitido los ejemplos, por lo que estos apuntes en ningún momento pueden sustituir al texto oficial, así que se deben tomar como un complemento o como un repaso a su estudio.

A lo largo del texto aparen unos recuadros grises con un texto de color morado, el contenido de los mismos no aparece en el texto oficial de la asignatura, sino en la bibliografía complementaria recomendada por el equipo docente que se encuentra al final de estos apuntes. Su inclusión me ha parecido interesante para reforzar cientos conceptos.

Todo texto en el que se emplean símbolos y notación matemática está expuesto a la aparición de erratas, así que se ruega que si alguno detecta alguna me lo haga saber.

Juan Miguel Suay Belenguer
jm_suay@hotmail.com
Curso 2016/17

1. Teoría Elemental de Números

1-1 Algoritmos de División y Euclides

1-1-1 La división de números enteros. Propiedades

Definición

Sean $\mathbf{a, b} \in \mathbb{Z}$.

1.- Llamaremos diferencia a - b de estos dos enteros a otro entero d que satisfaga la igualdad a = b + d.

2.- Si a ≠ 0 y b= a·q para algún q, diremos que a divide a b (a|b):

$$\forall \mathbf{a, b} \in \mathbb{Z}, \mathbf{a} \neq \mathbf{0}$$
$$\mathbf{a} \mid \mathbf{b} \Leftrightarrow \exists \mathbf{q} \in \mathbb{Z} \ / \ \mathbf{b} = \mathbf{a} \cdot \mathbf{q}$$

Otras expresiones equivalentes son a es un divisor o factor de b y b es múltiplo de a.

3.- Diremos que b es mayor que a (b > a), si existe un número natural n tal que b = a + n. Diremos que b ≥ a si b > a ó b = a.

Nota

(Z, +, ·) es un **anillo conmutativo**, que satisface las siguientes propiedades respecto a +:

1. ∀ a, b ∈ Z ⇒ a + b ∈ Z (operación cerrada)
2. ∀ a, b, c ∈ Z ⇒ (a + b) + c = a + (b + c) (asociativa)
3. ∀ a ∈ Z ∃ 0 / a + 0 = 0 + a = a (elemento neutro)
4. ∀ a ∈ Z ∃ b / a + b = 0 (elemento simétrico)
5. ∀ a, b ∈ Z ⇒ a + b = b + a (conmutativa)

y las siguientes respecto a ·

6. ∀ a, b ∈ Z ⇒ a · b ∈ Z (operación cerrada)
7. ∀ a, b, c ∈ Z ⇒ (a · b) · c = a · (b · c) (asociativa)
8. ∀ a ∈ Z ∃ 1 / a · 1 = 1 · a = a (elemento neutro)
9. ∀ a, b, c ∈ Z ⇒ a ·(b + c) = a · b + a · c (distributiva)

por lo que (Z, +, ·) es un anillo conmutativo con elemento unidad (el 1) y sin divisores del cero, es decir si ab = 0 entonces necesariamente a = 0 ó b = 0.

Propiedades

Sean $\mathbf{a,b,c} \in \mathbb{Z}$,

1.- 0·a = 0
2.- a(-b) = -a·b
3.- Si a ≠ 0 y ab = ac, entonces b = c
4.- Si a ≠ 0 y a|b, entonces a|bx para cada entero x
5.- Sean a ≠ 0 y b ≠ 0, si a|b y b|c entonces a|c
6.- Sea a ≠ 0. Si a|b y a|c, se verifica que a|(bx + cy) para cualquier par de enteros x e y
7.- Sean a y b positivos. Si a|b entonces a ≤ b
8.- Sean a ≠ 0 y b ≠ 0. Si a|b y b|a, se tiene que a = b ó a = -b

1-1-2 Definición de valor absoluto de un número entero. Propiedades.

Definición

Llamaremos valor absoluto a la aplicación:

$$|\ |: \mathbb{Z} \to \mathbb{Z}$$

Definida por |n| = n si n ≥ 0 ó |n| = -n si n < 0.
La aplicación está bien definida, es decir todo número entero tiene imagen mediante || y esta imagen es única.

Propiedades

1.- $|n| \in \mathbf{N} \cup \{0\}$
2.- |n|= 0 si y sólo si n=0
3.- |a·b|= |a|·|b|
4.- |a + b|≤|a|+|b|
5.- Si a ≠ 0, b ≠ 0 y a|b entonces |a| ≤ |b|

1-1-3 Algoritmo de la División

Teorema (Algoritmo de la División)

Sean a∈Z y b∈N. Entonces existen números enteros q y r tales que:

$$a = b \cdot q + r \quad 0 \leq r < b$$

Además, q y r son únicos. A los números a, b, q y r se denominan dividendo, divisor, cociente y resto.

Corolario

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.

1-1-4 El operador módulo: MOD

Definición

Sean a y b números enteros con b ≠ 0. Sea a = bq + r donde 0 ≤ r <|b|. Definimos el operador módulo "MOD" por

a MOD b = r.

Propiedades

Sean a, b, c, d y m números enteros con m = 0. Si

a MOD m = c MOD m y b MOD m= d MOD m

entonces:

1.- (a +b) MOD m = (c +d) MOD m.
2.- (ab) MOD m = (cd) MOD m.

1-1-5 Máximo común divisor (m.c.d.) de dos enteros

Definición

Sean a y b enteros. Un entero d ≠ 0 es un divisor común de a y b si d|a y d|b. Un divisor común de a y b se llama máximo común divisor de a y b, si d > 0 y cada común divisor de a y b divide también a d.

$$\mathbf{m.c.d.(a,b)=d} \Rightarrow \begin{cases} \mathbf{d \mid a,\ d \mid b} \\ \mathbf{\exists c / c \mid a,\ c \mid b \Rightarrow c \mid d \Rightarrow c \leq d} \end{cases}$$

Al máximo común divisor de a y b le designaremos por m.c.d.(a, b).

En el caso que a = b = 0 entonces m.c.d.(0, 0) = 0.

Nota

1. El m.c.d de dos números es siempre positivo, aunque a y b sean negativos, es decir:

   m.c.d.(-a, b) = m.c.d.(a, -b) = m.c.d.(-a, -b) = m.c.d.(a, b)

2. Como todos los números dividen a cero, si uno de ellos es nulo, b = 0, por ejemplo, entonces lod divisores comunes de a y b son los de a. Por lo tanto:

   m.c.d.(a, 0) = |a|

Definición

Sean $a_1, a_2, ..., a_n$, números enteros. Llamaremos máximo común divisor de $a_1, a_2, ..., a_n$ al divisor común d > 0 tal que cualquier otro divisor común de $a_1, a_2, ..., a_n$ divide también a d. Se designará mediante m.c.d.($a_1, a_2, ..., a_n$).

Teorema (Identidad de Bezout)

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 más pequeño que puede expresarse en la forma ax + by donde x e y son números enteros.

$$\text{m.c.d.}(a, b) = d = ax + by \qquad x,y \in Z$$

Corolario

Sean a y b enteros distintos de 0. Entonces m.c.d.(a, b) = 1 si y sólo si existen enteros s y t tales que as + bt = 1.

Proposición

Dados dos números enteros a y b, con b ≠ 0.
1.- Los divisores comunes de a y b son divisores del resto r de la división de a por b.

$$\left.\begin{array}{l} \forall a,b \in \mathbb{Z} \wedge b \neq 0 \\ \exists c / c \mid a \wedge c \mid b \\ a = b \cdot q + r \end{array}\right\} \Rightarrow c \mid r$$

2.- Los divisores comunes de b y del resto r son divisores de a.

$$\left.\begin{array}{l} \forall a,b \in \mathbb{Z} \wedge b \neq 0 \\ a = b \cdot q + r \\ \exists c / c \mid a \wedge c \mid r \end{array}\right\} \Rightarrow c \mid a$$

Teorema

El máximo común divisor del dividendo (a) y del divisor (b) de una división es el mismo que el máximo común divisor del divisor (b) y del resto (r).

$$\text{m.c.d.}(a,b) = \text{m.c.d.}(b, r)$$

1-1-6 Algoritmo de Euclides para el cálculo del m.c.d.

Existe algoritmo para el cálculo del m.c.d. de dos números a y b. Como se cumple:

$$m.c.d.(a,b) = m.c.d.(|a|, |b|),$$

podemos suponer sin pérdida de generalidad que $a \geq b > 0$. Dividimos a por b:

$$a=bq_1 + r_1 \text{ con } 0 \leq r_1 < b.$$

Si $r_1 = 0$ es obvio que b = m.c.d.(a, b). Así pues, supongamos que $r_1 \neq 0$; dividiendo b por r_1 podemos escribir:

$$b=r_1q_2+r_2 \text{ con } 0 \leq r_2 < r_1$$

Si $r_2 = 0$ entonces m.c.d.(b, r_1) = m.c.d.(a, b) = r_1 y hemos terminado. Si $r_2 \neq 0$ efectuamos la división de r_1 por r_2. Vamos obteniendo así un conjunto de números:

$$r_1 > r_2 > \ldots > r_i > \ldots$$

Puesto que cada uno de los números r_1, r_2, ..., r_i, ... es mayor o igual que cero, este conjunto de números no puede ser infinito. En algún momento llegaremos a que un resto es cero. Sea dicho resto $r_n = 0$ para algún n, entonces:

$$r_{n-1} = m.c.d.(r_{n-2}, r_{n-1}) = m.c.d.(r_{n-3}, r_{n-2}) = \ldots = m.c.d.(b, r_1) = m.c.d.(a, b)$$

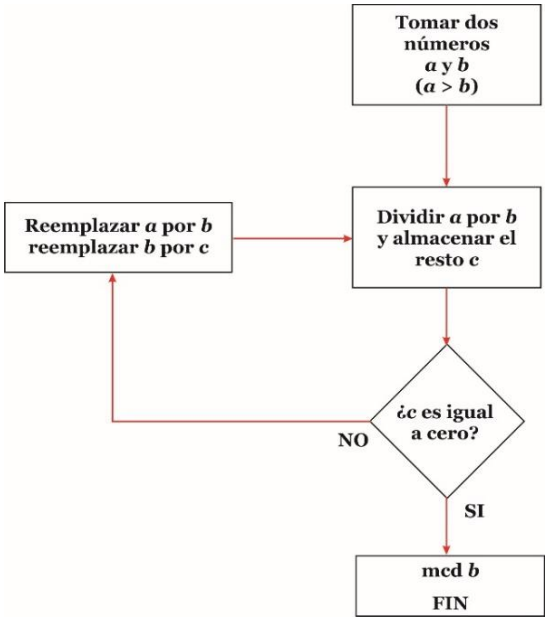


Fig. 1 Algoritmo de Euclides

Teorema

Si k > 0 entonces m.c.d.(ka, kb) = k·m.c.d.(a, b)

Corolario

Para cada entero $k \neq 0$ $m.c.d.(ka, kb) = |k| \cdot m.c.d.(a, b)$

1-2 NÚMEROS PRIMOS Y TEOREMA FUNDAMENTAL DE LA ARITMÉTICA

1-2-1 Definiciones de número primo, compuesto y números primos entre sí

Definición

Dado un número entero $p > 1$, diremos que p es un número 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.

De la definición de primo, es claro que un entero $p > 1$ es primo si y solo si es imposible expresar $p = a \cdot b$, donde a y b son enteros, y ambos $1 < a < p$ y $1 < b < p$.

Nota

En lo que sigue p designará un número primo mayor que 1. En el conjunto de los diez primeros números naturales 2, 3, 5 y 7 son primos, mientras que 4, 6, 8, 9 y 10 son números compuestos. Observemos que el número 2 es el único primo par.

Definición

Sean $a_1, ..., a_n$ una familia de números enteros. Diremos que los $a_1, ..., a_n$ son primos entre sí, si se tiene que $m.c.d.(a_1, ... ,a_n) = 1$.

1-2-2 El Lema de Euclides

Sean a, b y c números enteros. Supongamos que a y c son primos entre sí y que $c|ab$. Entonces $c|b$.

Corolario

Sea p un número entero mayor que 1. Las afirmaciones siguientes son equivalentes:

a) El número p es primo.
b) Para cualquier par a y b de números enteros, si $p|ab$ entonces $p|a$ ó $p|b$.

Corolario

Sea p un número primo. Si $p|a_1a_2 ... a_r$ entonces $p|a_i$ para algún i.

1-2-3 Factorización de un número en producto de primos: El Teorema Fundamental de la Aritmética

Sea n un número mayor que 1. Entonces existen números primos $p_1, \ldots, p_r$ tales que:

$$n = p_1p_2 \cdots p_r \text{ donde } p_1 \leq p_2 \leq \cdots \leq p_r$$

Además, esta factorización es única en el siguiente sentido. Sean q_1, q_2, ..., q_s números primos con $q_1 \leq q_2 \leq \cdots \leq q_s$ y tales que $n = q_1 q_2 \cdots q_s$ entonces $r = s$ y $q_i = p_i$ para cada $i = 1,2, \ldots, r$.

Corolario

Sea $n \in Z$ con $|n| > 1$. Entonces n tiene una factorización única de la forma:

$$n = \pm p_1^{\alpha_1} \cdots p_t^{\alpha_t}$$

donde $t \geq 1$, los p_i son primos distintos con pi < p2 < < pi y $\alpha_i \geq 1$ para $1 \geq i \geq t$. Esta factorización se llama factorización canónica de n.

1-2-4 Existencia de infinitos primos

Teorema

El número de primos es infinito.

El resultado anterior que garantiza la existencia de infinitos números primos nos plantea la cuestión sobre su distribución dentro del conjunto de los números naturales.

1-2-5 Cota superior para los divisores primos de un número

Sean p_1, p_2, ..., p_n el primero, el segundo, ..., el n-ésimo número primo. Observemos que

$$P_{n+1} \leq (P_1 \cdot P_2 \cdots P_n) + 1,$$

donde p_{n+i} es el n+1-ésimo número primo, puesto que por el teorema anterior si designamos por q al número $(P_1 \cdot P_2 \cdots P_n) + 1$, tenemos que si q es primo, como $p_n < q$, entonces $p_{n+1} \leq q$ y si q no es primo entonces hemos visto que tiene factores primos diferentes de $p_1 \cdot p_2 \cdots p_n$ ya que ninguno de los p_i puede dividir a q. En particular se tiene que si q_1 es el menor factor primo de q entonces $p_n < q_1$ y así $p_{n+1} < q_1 < q$.

En el siguiente Teorema vamos a ver una cota superior para el n-ésimo número primo en función de n.

Teorema

Si p_n es el n-ésimo número primo entonces $p_n \leq 2^{2^{n-1}}$

En el próximo Teorema veremos que existen familias particulares de números primos que también son infinitas.

Teorema

Existen infinitos números primos de la forma 4n + 3.

La distribución de números primos es un problema muy difícil y del que se conocen sólo resultados parciales. Eratóstenes en el siglo III a. C. estableció un método para la obtención de números primos llamado en su honor la Criba de Eratóstenes y que es una consecuencia del próximo Teorema cuya primera demostración rigurosa se debe a Fermat

Teorema

Sea a un entero mayor que 1, entonces si para todo número primo $\mathbf{p} \leq \sqrt{\mathbf{a}}$, no divide al número a, se verifica que a es primo.

Como una consecuencia del Teorema Fundamental de la Aritmética se puede establecer el carácter irracional de $\sqrt{2}$. Euclides en los Elementos otorga a Pitágoras este resultado.

Teorema

El número $\sqrt{2}$ es irracional.

1-2-6 Distribución de los números primos

Hemos visto que existen infinitos primos y hemos discutido la abundancia de primos. Ahora vamos a estudiar cómo se distribuyen los números primos entre los enteros positivos. La primera proposición nos permite ver que existen cadenas de longitud arbitraria de enteros positivos que no contienen números primos.

Proposición

Por cada entero n > 0, existen al menos n enteros compuestos consecutivos

La proposición anterior demuestra que la secuencia de enteros compuestos entre primos es arbitrariamente tan larga como se quiera. Los dos únicos primos consecutivos son el 2 y el 3, porque el dos es el único par primo. Sin embargo, existen muchos pares de primos cuya diferencia es 2. Estos primos son llamados primos gemelos. Ejemplos de estos primos son 5 y 7, 11 y 13, 101 y 103, 1.003.619 y 1.003.621.

1-2-7 Algunas conjeturas sobre números primos

Existen multitud de conjeturas concernientes a números primos:

1) Existen infinitos primos gemelos.
2) Conjetura de Goldbach (1742): cualquier número par más grande que 2 es suma de dos números primos. Algunos ejemplos: 4 = 2 + 2, 6 = 3 + 3, 8 = 5 + 3, 10 = 7 + 3, 12 = 7 + 5, 14 = 11 + 3, 16 = 13 + 3, 18 = 13 + 5, 20 = 17 + 3.

Esta conjetura ha sido verificada hasta $4 \cdot 10^{14}$, pero aún no se ha encontrado un argumento matemático que demuestre que es cierta para todo número par. Se han demostrado algunos resultados ya muy "cercanos" a la conjetura: Se sabe que cualquier número par es suma de 6 o menos números primos (Ramaré, 1995). Se sabe también, demostrado por Chen en 1966, que cualquier número par "suficientemente grande" es suma de un numero primo más el producto de dos números primos.

Obsérvese que, si la conjetura de Goldbach es cierta, entonces cualquier número impar mayor que 5 ha de ser suma de 3 o menos números primos, llamada la conjetura de Goldbach impar.

3) Dirichlet probó que, en cualquier progresión aritmética, o sea de la forma:

$$\{a + bn \mid n \in N\},$$

con a, b primos entre sí, existen infinitos números primos. Posteriormente Chevotarev demostró que, fijado b, y si denominamos

$$\phi(b) := \#\{a, 0 < a < b \text{ y a primo con b}\}$$

tenemos que, para cada a, el número de primos de la forma a + bn es $1/\phi(b)$ el número de primos totales. Por ejemplo, el número de primos que en forma decimal acaban en 1 (o en 3, o en 7, o en 9) es una cuarta parte del total.

¿Existe siempre un número primo entre n2 y (n + 1)2? Se sabe que siempre hay un primo entre n y 2n, con n > 1. Este resultado lo conjeturó Bertrand, y lo probó Chebichev.

4) Un primo de Fermat es un número primo de la forma $2^{2^n}+1$. Se conocen los cuatro primeros: $2^1 + 1 = 3$, $2^2 + 1 = 5$, $2^4 + 1 = 17$, $2^8 + 1 = 257$. ¿Hay infinitos primos de Fermat? Aún más, ¿hay algún primo de Fermat además de los cuatro primeros?

1-2-8 Cálculo del m.c.d. y m.c.m. de dos enteros (a partir de su factorización)

Teorema

Sean a y b dos enteros, entonces existen números primos $p_1 \ldots, p_t$ y enteros $\alpha_i \geq 0$ y $\beta_i \geq 0$ para $1 \leq i \leq t$ tales que:

$$a = \pm p_1^{\alpha_1} \cdots p_t^{\alpha_t}$$
$$b = \pm p_1^{\beta_1} \cdots p_t^{\beta_t}$$

Estas factorizaciones se consiguen a partir de la factorización canónica de a y de b. Si existe algún factor primo de a que no es factor de b se introduce en la factorización de éste con exponente cero y se procede análogamente con los factores de b que no lo son de a. Se demuestra que:

Sea $a = \pm p_1^{\alpha_1} \cdots p_t^{\alpha_t}$ y $b = \pm p_1^{\beta_1} \cdots p_t^{\beta_t}$, donde algunos de los α_i y β_i pueden ser cero.

Entonces:

$$\mathbf{m.c.d.(a,b) = p_1^{\min(\alpha_1,\beta_1)} \cdots p_t^{\min(\alpha_t,\beta_t)}}$$

Definición

Sean a y b dos números enteros. Llamaremos mínimo común múltiplo de a y b al menor entero positivo que sea múltiplo de ambos. Lo designaremos m.c.m.(a, b).

Teorema

Sea $\mathbf{a = \pm p_1^{\alpha_1} \cdots p_t^{\alpha_t}}$ y $\mathbf{b = \pm p_1^{\beta_1} \cdots p_t^{\beta_t}}$, donde algunos de los α_i y β_i pueden ser cero. Entonces:

$$\mathbf{m.c.m.(a,b) = p_1^{\max(\alpha_1,\beta_1)} \cdots p_t^{\max(\alpha_t,\beta_t)}}$$

Es decir, para hallar el mcm de dos números a y b se hallan los factores primos de los números y se toma el producto de todos los factores primos elevados al mayor exponente que aparezca en a ó en b.

Definición

Sean a_1, a_2, …, a_n números enteros. Llamaremos mínimo común múltiplo de estos números y lo designaremos por m.c.m.(a_1, a_2, …, a_n) al entero positivo más pequeño que sea múltiplo de todos ellos.

Teorema

Sean a y b enteros no nulos, entonces:

$$|ab| = [\text{m.c.d.(a, b)}].[\text{m.c.m.(a, b)}].$$

1-2-9 Test de primalidad

Hasta ahora, en todos los ejemplos vistos de números compuestos hemos dado su factorización. Esto ha sido posible ya que los números eran pequeños. En general, no es posible dar la factorización si el número tiene muchas cifras. ¿Cómo saber si un número es primo, sin necesidad de conocer ninguno de sus factores? Vemos, por tanto, que hay dos problemas distintos: uno es saber si un número es primo o no y el otro conocer sus factores, en el caso de ser un número compuesto. Para resolver el primer problema se utilizan los tests de primalidad y para el segundo métodos de factorización.

Los tests de primalidad pueden ser de dos clases: determinísticos y probabilísticos. Los primeros determinan con absoluta certeza si un número es primo o no. En los segundos puede ocurrir que se identifique falsamente a un número compuesto como primo, pero la posibilidad de que esto suceda es bajísima. Nunca identificarán un número primo

como compuesto. Son, en general, mucho más rápidos que los determinísticos y son los que suelen estar implementados en programas de ordenador.

Los primos de la forma $M(p)= 2^p — 1$, donde p es primo, se denominan primos de Mersenne y, en general, los números de la forma $M(n) = 2^n — 1$, se llaman números de Mersenne.

Teorema

Sea p un primo impar. Entonces cualquier divisor primo q de M(p), si existe, es de la forma $q = 2kp + 1$.

1-3 El Principio de Inducción

En las Matemáticas aparecen muchos problemas que tienen la siguiente forma general:

1.- Sea P(n) una determinada propiedad acerca de un número natural n.
2.- Se trata de probar que P(n) es verdadero para todo $n \in N$.

1-3-1 El principio de la Buena Ordenación

En la demostración del Principio de Inducción juega un papel fundamental el Principio de la Buena Ordenación, cuyo enunciado es el siguiente:

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. Este primer elemento, m, puede sustituir al "1" en el Principio de Inducción, para demostrar que una propiedad P(n) se cumple para todo natural $n \geq m$.

1-3-2 El Principio de Inducción

Teorema (Principio de Inducción)

Sea S un conjunto de números naturales que satisface las dos condiciones (hipótesis) siguientes:

1) El número $1 \in S$. (Arranque de la inducción)
2) Para cada número $k \geq 1$ si $k \in S$ entonces $k + 1 \in S$. (Motor de la inducción)

Entonces el conjunto S es igual a N.

El Principio de Inducción es una técnica muy potente que se utiliza para demostrar que cierta propiedad P se satisface para todo número natural n. Los pasos que debemos seguir son los siguientes:

Paso 1: Definir el conjunto $S= \{n \in N$ tales que P(n) es verdadera$\}$.
Paso 2: Probar que $1 \in S$.
Paso 3: Suponer que $k \in S$ para $k \leq 1$ arbitrario.
Paso 4: Demostrar entonces que $k + 1 \in S$.

Del Principio de Inducción se sigue que S es igual a N y así la propiedad P(n) se satisface para todo $n \in N$.

Corolario

Supongamos que P es una propiedad para la cual se tiene

1) P(1), es decir el 1 satisface la propiedad P. (Arranque de la inducción)
2) Para cada $k \in N$, $P(k) = P(k + 1)$. (Motor de la inducción)

Entonces P(n) se satisface para todo n.

Corolario

Sea $n_o \in Z$ y sea $M = \{n \in Z, n \geq n_o\}$. Sea S un subconjunto de M tal que:

1) $n_o \in S$. (Arranque de la inducción)
2) Para cada k no arbitrario, si $k \in S$ entonces $k + 1 \in S$. (Motor de la inducción)

Entonces S = M.

Corolario

Sea $n_o \in Z$ y supongamos que P es una propiedad para la cual

1) $P(n_o)$ es cierta, es decir el número n_o satisface P. (Arranque de la inducción)
2) Para cada k no arbitrario se tiene que si P(k) es cierta entonces P(k + 1) es cierta. (Motor de la inducción)

Entonces P(n) se satisface para todo entero n no.

1-3-3 El Principio Fuerte de Inducción

Teorema (Principio Fuerte de Inducción)

En ocasiones al argumentar por inducción necesitaremos más condiciones que la vista hasta ahora: P(k) implica P(k + 1). Por este motivo introduciremos a continuación el llamado Principio Fuerte de Inducción:

Sea S un conjunto de enteros positivos tales que

1) $1 \in S$. (Arranque de la inducción)
2) Para cada entero $n > 1$, si $k \in S$ para todo entero k tal que $1 \leq k < n$ entonces $n \in S$. (Motor de la inducción)

Entonces S = N.

Corolario

Supongamos que P es una propiedad para la que se verifica.

1) P(1) es cierta. (Arranque de la inducción)
2) Para cada entero $n_o > 1$ si P(k) es cierta para cada entero k con $1 \leq k < n_o$ entonces $P(n_o)$ es cierta. (Motor de la inducción)

Entonces P(n) se satisface para todo n.

Corolario

Sean $n_o \in Z$, $M = \{n \in Z, n \geq n_o\}$ y S un subconjunto de M tal que

1) $n_o \in S$. (Arranque de la inducción)
2) Para cada $n > n_o$ si $k \in S$ para todo entero k tal que $n_o \leq k < n$ entonces $n \in S$. (Motor de la inducción)

Entonces S = M.

Corolario

Sean $n_o \in Z$ y supongamos que P es una propiedad tal que

1) $P(n_o)$ es cierta. (Arranque de la inducción)
2) Para cada $n_1 > n_o$, si es cierta P(k) para todo k con $n_o \leq k < n_1$ entonces $P(n_1)$ es cierta. (Motor de la inducción)

Entonces P(n) se satisface para todo $n \geq no$.

1-3-4 Aplicación de la inducción a la verificación de algoritmos

Una de las tareas más importantes que tiene que realizar el programador es la demostración de que un programa o un algoritmo es correcto, independientemente del conjunto de datos proporcionados. Uno de los métodos fundamentales para verificarlo es la inducción matemática.

Veamos cómo: un programa (o un algoritmo) es recursivo si resuelve un problema reduciéndolo a un caso del mismo problema, pero con datos de entrada más pequeños.

Como ejemplo podemos programar el cálculo del factorial n! de forma recursiva:

```
procedure factorial (n: entero no negativo)
if n=0 then
        factorial(n):=1;
else
        factorial(n):=n*factorial(n-1);
end procedure
```

Para comprobar formalmente que el algoritmo recursivo anterior es correcto, es decir, que calcula verdaderamente el factorial de n si dicho n es un entero no negativo, procederemos por inducción:

Caso base: si n = 0 entonces el programa devuelve 1, que es precisamente 0! Supongamos que para n - 1 el programa devuelve verdaderamente (n-1)! y que no es el caso base (es decir, ahora n > 0). Entonces paran el programa devuelve n.(n-1)! =n!

1-4 ECUACIONES DIOFÁNTICAS

Se dedica esta Sección a una introducción a las ecuaciones diofánticas. Se resuelven las ecuaciones lineales de dos variables en Z, las ecuaciones de la forma $x^2 - y^2 = n$ - que sirven para estudiar después el método de factorización de Fermat- y las ecuaciones pitagóricas $x^2 + y^2 = z^2$. Se termina la Sección con el así llamado Ultimo Teorema de Fermat.

1-4-1 Condiciones de solubilidad de una ecuación diofántica del tipo ax + by = n, y algoritmo de búsqueda de dichas soluciones cuando existan.

Teorema

Sean a, b y n números enteros. La ecuación lineal ax + by = n tiene solución entera x_o e y_o sí y solo si d = m.c.d.(a,b) divide a n.

Algoritmo para encontrar una solución

Dada la ecuación ax + by = n en primer lugar calculemos el m.c.d.(a, b) mediante el algoritmo de Euclides. Sabemos que:

$$\mathbf{a = b \cdot q_1 + r_1}$$
$$\mathbf{b = r_1 \cdot q_2 + r_2}$$
$$\mathbf{.}$$
$$\mathbf{.}$$
$$\mathbf{r_{t-2} = r_{t-1} \cdot q_t + r_t}$$
$$\mathbf{r_{t-1} = r_t \cdot q_{t+1}}$$

donde r_t = m.c.d.(a, b) = d. Por tanto, $r_{t-2} - r_{t-i}\, q_t = d$ y se puede escribir

$$r_{t-2} - (r_{t-3} - r_{t-2} \cdot q_{t-1}) \cdot q_t = d,$$

que es equivalente a

$$- r_{t-3} \cdot q_t + r_{t-2} \cdot (1 + q_{t-1} \cdot q_t) = d,$$

Si continuamos ascendiendo por las igualdades anteriores al final llegamos a poder escribir d como:

$$aq_1^* + bq_2^* = d,$$

donde q1* y q2* son expresiones en función de $q_1, \ldots, q_t$. Por el teorema anterior una solución de la ecuación será:

$$\mathbf{x_o = \frac{n \cdot q_1^*}{d}}$$
$$\mathbf{y_o = \frac{n \cdot q_2^*}{d}}$$

Teorema

Supongamos que a, b y n son enteros 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:

$$\left\{ x_o + \frac{t \cdot b}{d},\ y_o + \frac{t \cdot a}{d} \right\}$$

donde $t \in Z$ y $\{x_o, y_o\}$ es una solución de ax +by =n.

1-4-2 La ecuación diofántica $x^2 - y^2 = n$, n > 0.

Teorema

La ecuación diofántica $x^2 - y^2 = n$ 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

$$\left\{ x = \frac{a+b}{2},\ y = \frac{a-b}{2} \right\}$$

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

1-4-3 Algoritmo de Factorización de Fermat

A partir del resultado anterior, Fermat estableció en 1643 un algoritmo para estudiar si un número natural n impar es compuesto. Aunque el algoritmo puede resultar en algunos casos muy largo, no requiere conocer todos los primos menores que $\sqrt{n}$.

Sea n un número natural impar. Si n es compuesto se tiene que n = a·b donde a y b han de ser impares también. Además, podemos suponer que a b > 1. Por el teorema anterior se puede escribir:

$$\left(\frac{a+b}{2}\right)^2 - \left(\frac{a-b}{2}\right)^2 = n$$

Luego estudiar si un número impar es compuesto es un problema equivalente a resolver la ecuación $x^2 - y^2 = n$. Esta ecuación puede escribirse, $x^2 - n = y^2$.

El primer paso es determinar el mínimo entero positivo q que satisfaga que $q^2 \geq n$ y posteriormente habrá que estudiar si alguno de los números

$$q^2 - n,\ (q+1)^2 - n,\ (q+2)^2 - n,\ ...$$

es un cuadrado. Este proceso no es indefinido ya que

$$\left(\frac{n+1}{2}\right)^2 - n = \frac{n^2+2\cdot n+1-4\cdot n}{4} = \left(\frac{n-1}{2}\right)^2$$

Esta solución corresponde a la factorización trivial n = n.1. Luego los únicos valores que hay que estudiar son aquellos números m que satisfacen

$$q \le m < \frac{n-1}{2}$$

Si para ninguno de estos números m, m^2 - n es un cuadrado, entonces n será primo.

1-4-4 La ecuación pitagórica $x^2 + y^2 = z^2$

Consideremos ahora la ecuación pitagórica $x^2 + y^2 = z^2$ con x, y, z números naturales. Como en los casos anteriores solo nos interesan las soluciones enteras. En primer lugar, observemos que si la terna (x_o, y_o, z_o) es una solución de la ecuación $x^2 + y^2 = z^2$ entonces también es solución $(\lambda\cdot x_o, \lambda\cdot y_o, \lambda\cdot z_o)$ para cualquier número entero $\lambda \neq 0$ ya que:

$$\lambda^2\cdot x_o^2 + \lambda^2\cdot y_o^2 = \lambda^2\cdot\left(x_o^2 + y_o^2\right) = \lambda^2\cdot z_o^2$$

Por otra parte, si d es el máximo común divisor de x_o, y_o y z_o entonces $\left(\frac{x_o}{d}, \frac{y_o}{d}, \frac{z_o}{d}\right)$ también es solución y además $\frac{x_o}{d}, \frac{y_o}{d}$ y $\frac{z_o}{d}$ son primos entre sí.

Por tanto, para resolver el problema basta buscar las soluciones (x_o', y_o', z_o') con x_o', y_o', z_o' naturales y primos entre sí, llamadas ternas primitivas pitagóricas, ya que las demás soluciones serán éstas multiplicadas por cualquier número entero $\lambda \neq 0$.

Teorema

Las soluciones de la ecuación pitagórica $x^2 + y^2 = z^2$ que satisfacen las condiciones

$$\text{m.c.d.}(x, y, z) = 1,\ \ 2 \mid x,\ \ x, y, z > 0,$$

vienen dadas por las fórmulas,

$$x = 2st,$$
$$y = s^2 - t^2,$$
$$z = s^2 + t^2.$$

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

Las cinco primeras ternas primitivas pitagóricas son:

s	t	x = 2st	$y = s^2 - t^2$	$z = s^2 + t^2$
2	1	4	3	5
3	2	12	5	13
4	1	8	15	17
4	3	24	7	25
5	2	20	20	29

1-4-5 Teorema de Fermat

Fermat abordó el problema más general de buscar las soluciones enteras de la ecuación $x^n + y^n = z^n$, cuando $n \geq 3$ y dijo que esta ecuación no tiene solución con x, y, z naturales. Fermat afirmó tener una demostración de este resultado, pero no la escribió. A lo largo de los últimos cuatro siglos, algunos de los matemáticos más importantes dedicaron parte de sus esfuerzos a la demostración del resultado, sin conseguirlo hasta ahora, por lo que se piensa que Fermat estaba equivocado cuando creía tener una demostración. En el año 1995 el matemático *Andrew Wiles* en un artículo de 98 páginas publicado en *Annals of Mathematics* (1995), consiguió demostrar el teorema.

Teorema

La ecuación $x^4 + y^4 = z^2$ no tiene solución para números x, y, z naturales.

Corolario

La ecuación $x^4 + y^4 = z^4$ no tiene solución para x, y, z naturales.

Corolario

La ecuación $x^{4k} + y^{4k} = z^{4k}$, $k > 0$ no tiene solución para x, y, z naturales.

1-5 CONGRUENCIAS

1-5-1 Definición de congruencia y módulo. Propiedades

Definición

Sea $m > 0$. Dados $a, b \in Z$ se dice que a y b son congruentes módulo m si a - b es divisible por m. Simbólicamente esta relación se escribe

$$a \equiv b \text{ mód}(m) \text{ si y sólo si } m \mid (a - b).$$

El número m se denomina módulo de la congruencia. Es decir:

$$a \equiv b \text{ mód}(m) \Leftrightarrow a - b = mk \quad k \in Z$$
$$a \equiv b \text{ mód}(m) \Leftrightarrow a = b + mk \quad k \in Z$$

Teorema

Fijado $m > 0$, cada número entero a es congruente con uno de los enteros 0, 1, 2, ..., m-1.

Es decir que si tenemos $a \in Z$ y lo dividimos por m, por el Algoritmo de la División existen q y r únicos tal que $a = qm + r$, por lo tanto, se cumple que $a \equiv r$ mód(m). El número r se denomina menor residuo no negativo de a módulo m. Obsérvese que este menor residuo no negativo de a módulo m no es otra cosa sino a MOD m

Definición

El conjunto de enteros 0, 1, 2, ..., m-1 se denomina conjunto de menores residuos no negativos módulo m.

En general dada una colección de enteros $a_1, a_2, ..., a_m$ se dice que es un conjunto completo de residuos (o también sistema completo de residuos) módulo m si cada número entero es congruente módulo m con uno y sólo uno de los $a_i \leq 1 \leq m$ o lo que es equivalente, si cada uno de los ai es congruente módulo m a uno y sólo uno de los números 0, 1, 2,..., m-1.

Teorema

Sean a y b dos números enteros, entonces $a \equiv b$ mód(m) si y sólo si al dividir a y b por m el resto obtenido es el mismo.

Teorema

Una congruencia puede considerarse como una generalización de la igualdad de números enteros, por tanto, alguna de las propiedades de la igualdad también las tiene la relación de congruencia. Estas propiedades se recogen en el siguiente Teorema.

Sean a, b, c, d, h, m $\in$ Z con h $\neq$ 0 y m > 0 entonces

1) a $\equiv$ a mód(m).
2) Si a $\equiv$ b mód(m) entonces b $\equiv$ a mód(m).
3) Si a $\equiv$ b mód(m) y b $\equiv$ c mód(m) entonces a $\equiv$ c mód(m).
4) Si a $\equiv$ b mód(m) y c $\equiv$ d mód(m) entonces
   a+c $\equiv$ b+d mód(m), ac $\equiv$ bd mód(m).
5) Si a $\equiv$ b mód(m) entonces ha $\equiv$ hb mód(m).
6) Si h|a, h|b, m.c.d.(h, m) = 1 y a $\equiv$ b mód(m) entonces

$$\frac{a}{h} \equiv \frac{b}{h} \text{mód(m)}$$

Corolario

Supongamos que para $1 \leq i \leq n$ se tiene que $a_i = b_i$ mód(m), entonces

$$\sum_{i=1}^{n} a_i = \sum_{i=1}^{n} b_i \cdot \text{mód(m)}$$

$$\prod_{i=1}^{n} a_i = \prod_{i=1}^{n} b_i \cdot \text{mód(m)}$$

Teorema

Sean a y b números enteros y m_1, m_2, ..., m_r, enteros positivos. Sea M = m.c.m(m_1, m_2, ..., m_r). Si a $\equiv$ b mod(m_i), para todo i = 1, ..., r, entonces a $\equiv$ b mod(M).

1-5-2 Aplicaciones de las congruencias a los dígitos de control

Las congruencias pueden usarse para detectar errores de cadenas de dígitos. Tantas cadenas de bits (ceros y unos) corno cadenas de dígitos decimales que se utilizan en los documentos de identidad, ISBN, etc.

Cadenas de bits

Para detectar posibles errores en la transmisión de cadenas de bits $x_1\, x_2 ... x_n$, un método muy simple consiste en añadir un bit más x_{n+1} denominado bit de paridad. Este bit torna valor 0 ó 1 dependiendo de la cadena $x_1\, x_2 ... x_n$, de modo que se cumpla la siguiente relación:

$$x_1 + x_2 + ... + x_n + x_{n+1} = 0 \text{ mod}(2).$$

Supongamos que se reciben las cadenas de bits 1101110 y 1111110. Entonces, comprobando la relación anterior se detectaría un fallo en la primera cadena, y se podría solicitar nuevamente su transmisión. Utilizando más bits de control, se puede detectar varios fallos, e incluso corregir algunos.

Dígitos de control en publicaciones

Los libros se codifican mediante los números del I.S.B.N. (International Standard Book Number). Se utilizan los números del 0 al 9 y la letra X. Este sistema está en revisión, para pasar a uno de 13 dígitos.

El primer grupo de dígitos indica el país (o el idioma). En España es el 84. El segundo grupo de dígitos designa la editorial. El tercer grupo es un número asignado al libro por la editorial.

El último carácter, el décimo, es un factor de comprobación. Si designamos el número completo por $x_1x_2x_3x_4x_5x_6x_7x_8x_9x_{10}$ el décimo dígito verifica la relación

$$x_{10} \equiv 10x_1 + 9x_2 + 8x_3 + 7x_4 + 6x_5 + 5x_6 + 4x_7 + 3x_8 + 2x_9 \bmod(11),$$

y si $x_{10} = 10$, entonces se representa por la letra X.

Código de barras

Todos los productos que compramos hoy en día llevan un código de barras y un número. En la caja registradora, el código de barras se examina mediante un lector láser que envía un mensaje a un ordenador, donde se encuentran los precios de todos los productos, cuántos artículos como ese quedan, etc. El ordenador envía la información oportuna a la pantalla de la caja registradora y hace imprimir el recibo correspondiente. Los números del código de barras del artículo suelen seguir la siguiente estructura:
El primer grupo de dígitos indica el país. El segundo grupo de dígitos designa la referencia del fabricante. El tercer grupo es un número asignado al número del producto. El último carácter es el dígito de control.

El dígito de control se calcula del siguiente modo: se suman las seis cifras que ocupan los lugares impares empezando por la izquierda; llamemos a este valor X. A continuación, se suman las seis cifras de los puestos pares, Y. Se tiene que cumplir que

$$X - Y + \text{dígito de control} \equiv 0 \bmod(n),$$

donde el valor de n suele ser 8 ó 6, aunque para cada tipo de producto puede haber un n diferente.

Número de Identificación Fiscal

El cálculo de la letra del N.I.F. (Número de Identificación Fiscal) de cada D.N.I. obedece a un algoritmo y a una codificación. En primer lugar, se calcula el número del D.N.I. módulo 23 y al valor obtenido se le asigna una letra según la siguiente clave:

0 T; 1 R; 2 W; 3 A; 4 G; 5 M; 6 Y; 7 F; 8 P; 9 D; 10 X; 11 B; 12 N; 13 J; 14 Z; 15 S; 16 Q; 17 V; 18 H; 19 L; 20 C; 21 K; 22 E.

1-5-3 La ecuación $ax \equiv b \bmod(m)$

Después de haber definido las congruencias y haber estudiado sus propiedades básicas resolveremos a continuación la ecuación $ax \equiv b \bmod(m)$. Si existe una solución $x_0 \in Z$ de esta ecuación entonces $ax_0 - b = k_o m$, o equivalentemente, $ax_0 - k_0 m = b$. Por tanto, resolver la ecuación lineal $ax \equiv b \bmod(m)$ es equivalente a resolver la ecuación diofántica $ax + my = b$. De lo estudiado en la sección 1.4 se puede enunciar el siguiente

Teorema

La ecuación $ax \equiv b \bmod(m)$ tiene solución si y sólo si d divide a b donde d es el m.c.d.(a, m). Además, el número de soluciones no congruentes módulo m es exactamente d.

Teorema

Si d = m.c.d.(a,m), entonces la congruencia lineal: $ax \equiv b \bmod(m)$ tiene solución si, y solo si d divide a b. Si d divide a b y x_0 es una solución, la solución general viene dada por:

$$\mathbf{x = x_0 + \frac{n \cdot t}{d} \quad t \in \mathbb{Z}}$$

En particular, las soluciones forman, exactamente d clases de congruencias modulo m, con representantes:

$$\mathbf{x = x_0,\ x_0 + \frac{n}{d},\ x_0 + \frac{2n}{d},\ \cdots,\ x_0 + \frac{(d-1)n}{d}}$$

Aplicación a la generación de números pseudoaleatorios

A menudo, para la realización de simulaciones en un ordenador se necesita disponer de números seleccionados aleatoriamente. Existen distintos métodos para la generación de números con propiedades similares a las de los números aleatorios, llamados pseudoaleatorios, ya que cualquier método sistemático nunca podrá generar números realmente aleatorios.

Un método eficiente se basa en las congruencias. Se eligen cuatro números enteros: el módulo m, el multiplicador a, el incremento c y la semilla xo, tales que $2 \leq a < m$, $0 \leq c < m$, y $0 \leq x_o < m$.

El método genera una sucesión $\{x_n\}$ de números pseudoaleatorios $0 \leq x_n < m$, por medio del siguiente procedimiento

$$x_{n+1} = (ax_n + c) \bmod(m).$$

Una secuencia de números $x_1, x_2, \ldots x_p$, generada por este método tendrá a lo más m elementos distintos antes de que aparezca una repetición. Se denomina periodo al menor entero p tal que $x_{p+1} = x_j$ para algún $j \leq p$.

El método de generación de números pseudoaleatorios será mejor cuanto mayor sea el periodo. En 1998 D. Knuth estableció que el periodo p es máximo (p = m) si y sólo si m.c.d.(c, m) =1, $a \equiv 1 \bmod(q)$ para todos los primos q tales que q|m, y $a \equiv 1 \bmod(4)$ si 4|m. Obsérvese que si m es primo y a = 1, se satisfacen todas las condiciones trivialmente.

Para completar el estudio de las congruencias lineales establecernos ahora el Teorema Chino del Resto. Este resultado aparece en algunos de los más importantes manuscritos chinos de la Antigüedad, por ejemplo, aparece en el siglo I en los trabajos de Sun Tsu. En esa misma época este resultado fue conocido también por el neopitagórico Nicómaco, que trabajó en Gerasa (Palestina).

1-5-4 El Teorema Chino del Resto (sistemas de congruencias)

El sistema de congruencias:

$$\begin{cases} \mathbf{a_1 x \equiv b_1 \bmod(m_1)} \\ \mathbf{a_2 x \equiv b_2 \bmod(m_2)} \\ \quad \cdots \\ \mathbf{a_i x \equiv b_i \bmod(m_i)} \\ \quad \cdots \\ \mathbf{a_k x \equiv b_k \bmod(m_k)} \end{cases}$$

donde m.c.d.(m_i, m_j) = 1 si $i \neq j$ y m.c.d.(a_i, m_i) = 1 para $1 \leq i \leq k$, tiene una única solución x_o módulo ($m_1 m_2 \ldots m_k$) y las demás soluciones son de la forma:

$$x = x_o + \lambda(m_1 m_2 \ldots m_k),\ \lambda \in Z.$$

Corolario

El sistema de congruencias $a_i x \equiv \bmod(m_i)$ con i = 1,2, …, k, donde m.c.d.(m_i, m_j) = 1 si $i \neq j$ y m.c.d.(a_i, m_i) = 1, i = 1,2, …, k tiene una única solución en cada conjunto completo de residuos módulo $m_1 m_2 \ldots m_k$.

Aplicación a la aritmética computacional con enteros grandes

Supongamos que un procesador realiza las operaciones aritméticas con enteros menores que un cierto q de un modo mucho más rápido que la aritmética con enteros más grandes y se desea restringir todos los cálculos de una operación de modo que sólo se utilicen enteros menores que q. Para ello se seleccionan como módulos números enteros primos entre si dos a dos m_1, m_2, ..., m_r. El teorema Chino del Resto permite representar cualquier número entero $0 \leq x < m_1 m_2 \ldots m_r$ mediante una n-upla consistente en los n restos de la división de x por m_i, i = 1, …, r

$$x \rightarrow (x \bmod(m_1), \ldots, x \bmod(m_r)),$$

por lo tanto, dados dos números x e y su suma seria

$$(x+y \bmod(m_1), \ldots, x+y \bmod(m_r) = (z_1, \ldots, z_r),$$

para encontrar el valor de la suma lo único que habría que resolver es el sistema $w \equiv z_1 \bmod(m_1)$, …, $w \equiv z_r \bmod(m_r)$. Este método permite realizar cálculos aritméticos con números grandes.

1-5-5 La función ϕ de Euler

A continuación, se introduce la función de Euler que permitirá después demostrar tres famosos teoremas sobre congruencias: el Teorema de Euler, el Pequeño Teorema de Fermat, y el Teorema de Wilson

Definición

Dado un número natural m, se designa por $\phi(m)$ al número de enteros positivos r que no exceden a m y son primos con m.

$$\phi(m) = \#\{r \in \mathbb{N} : r \leq m,\ m.c.d(r,m)=1\}$$

La función $\phi(m)$ se denomina función ϕ de Euler.

Propiedades

1) Si p es primo se cumple que $\phi(p) = 1 - p$
2) Si p es un número primo entonces:

$$\phi(p^r) = p^r - p^{r-1} = p^r \cdot \left(1 - \frac{1}{p}\right)$$

Definición

Un sistema reducido de residuos módulo m, es una colección maximal de enteros $a_1, a_2, \ldots, a_r$, tal que cada a_i es primo con m y cada par de enteros a_i y a_j tienen diferente resto módulo m. Cualesquiera dos sistemas reducidos de residuos módulo m tienen el mismo número de elementos, es decir, $\phi(m)$ elementos.

Proposición

Si m y n son dos números enteros primos entre sí, entonces $\phi(mn) = \phi(m)\phi(n)$.

Teorema

Sea $n = p_1^{r_1} \cdot p_2^{r_2} \cdot \cdots \cdot p_s^{r_s}$. Entonces

$$\phi(n) = n \cdot \left(1 - \frac{1}{p_1}\right) \cdot \left(1 - \frac{1}{p_2}\right) \cdot \ \cdots \cdot \left(1 - \frac{1}{p_s}\right)$$

1-5-6 Teorema de Euler

Sean a y m dos números enteros con m ≥ 1; entonces si m.c.d.(a, m) = 1 se tiene que $a^{\phi(m)} \equiv 1 \bmod(m)$.

1-5-7 Pequeño Teorema de Fermat

Si p es un número primo que no divide al número a entonces

$$a^{P-1} \equiv 1 \bmod(p).$$

1-5-8 Teorema de Wilson

Si p es un número primo entonces

$$(p - 1)! \equiv -1 \bmod(p).$$

1-5-9 Cifrado de mensajes. Criptografía

El sistema César

El cifrado César es uno de los más antiguos que se conocen. Debe su nombre a Julio César, que presuntamente lo utilizó para establecer comunicaciones seguras con sus generales durante las Guerras de las Gálias.

Dados a y b primos entre sí, la aplicación f(x) = ax + b mod(m) recibe el nombre de codificación módulo m con parámetros a, b; el par (a, b) es la clave de este cifrado.

Si asignamos a cada letra (A ... Z) un entero módulo 27, de la siguiente forma:

A-0 B=1 C=2 D=3 E=4 F=5 G=6 H=7 I=8 J=9 K=10 L=11 M=12 N=13 Ñ =14 O=15 P=16 Q=17 R=18 S=19 T=20 U=21 V=22 W=23 X=24 Y=25 Z=26

El cifrado César es la codificación módulo 27 con parámetros 1, b, la clave es (1, b), es decir, siempre tomaremos a=1. De esta forma, la anterior aplicación quedará f(x) = x + b mod(27) lo cual se traduce que para encriptar una letra hemos de tomar su entero correspondiente y sumarle b para obtener el texto cifrado. Análogamente, y gracias al hecho que f(x) siempre ha de ser biyectiva, independientemente del valor de b, para descifrar un texto tomamos la función inversa, definida por f(x) = x — b.

Veamos un sencillo ejemplo, en el que se toma b=4. Queremos cifrar, con la clave (1,4), la palabra CESAR. Tomando el valor de cada letra, tenemos el equivalente numérico de la palabra:

2 4 19 0 18

Aplicamos a cada número la función f(x) = x + 4 para obtener:

6 8 23 4 22

que retornado al alfabeto, sustituyendo cada valor por su equivalente, queda GIWEV.

Ahora, con la misma clave (1,4), buscamos descifrar FVYXYW. El valor de cada letra es

5 22 25 24 25 23

Tomando f(x) = x - 4, tenemos el resultado

1 18 21 20 21 19

que retornado al alfabeto significa BRUTUS, texto plano equivalente al cifrado FVYXYW.

El cifrado César tiene 27 claves diferentes, incluyendo la clave de identidad (b = 0), caso en el que el texto cifrado y el texto en claro son idénticos. Así pues, no resultaría muy difícil para una persona realizar un ataque exhaustivo, buscando en el texto cifrado palabras en claro con significado en el lenguaje utilizado. Por tanto, este cifrado es claramente vulnerable para un atacante, no ofreciendo una seguridad fiable en la transmisión de datos confidenciales.

El sistema RSA

Un tipo de cifrados más seguros son los llamados Cifrados de Clave Pública. Uno de ellos, es el introducido en 1977 por los profesores del MIT (Massachusetts Institute of Technology) Ronald R. Rivest, Adi Shamir y Leonard M. Adleman, de ahí las siglas RSA con las que es conocido.

La seguridad de RSA radica en la dificultad de la factorización de números grandes: es fácil saber si un número es primo, pero es extremadamente difícil obtener la factorización en números primos de un entero elevado, debido, no a la dificultad de los algoritmos existentes, sino al consumo de recursos físicos (memoria, necesidades hardware incluso tiempo de ejecución) de tales algoritmos.

El funcionamiento del algoritmo RSA es el siguiente: si un usuario A desea enviar información cifrada, ha de elegir aleatoriamente dos números primos grandes (del orden de cien dígitos), p y q. Estos números se han de mantener en secreto. Si llamamos N (N se conoce como módulo) al producto pq, el usuario ha de determinar otro entero, d, llamado exponente privado, que cumpla:

$$m.c.d.(d, (p - 1)(q - 1)) = 1,\ d < N$$

es decir, d y el producto $\phi(N) = (p - 1)(q - 1)$ función de Euler de N, han de ser primos entre sí. Con estos datos, ya tenemos la clave privada del cifrado: el par (N, d). Para obtener la clave pública, hallamos el inverso multiplicativo del número d respecto de $\phi(N)$, de la forma

$$ed \equiv 1 \bmod(\phi(N))$$

Entonces $ed = 1 + z \cdot \phi(N)$.

Calculado este entero e, llamado exponente público, la clave pública será el par (N, e).

Una vez el emisor A dispone de sus claves pública y privada, podría enviar un mensaje cifrado, que llamaremos m, a un posible receptor, mediante la operación

$$c = m^e \bmod(N)$$

aplicada a cada elemento del mensaje. El receptor del criptograma, realizaría la siguiente operación de descifrado:

$$C^d \bmod(N) \equiv m^{ed} \bmod(N) \equiv m^{1 + \phi(N)} \bmod(N) \equiv m \bmod(N)$$

puesto que por el Teorema de Euler (1-5.35) m4(N) -= 1 mod(N). Ahora bien, para aplicar el Teorema de Euler es necesario que el m.c.d. (m, N) =1, afortunadamente esta condición se cumple salvo casos muy excepcionales.

1-6 Sistemas de Numeración y Criterios de Divisibilidad

1-6-1 Representación de un número natural en una base dada

Teorema

Sea $b \geq 2$ un número natural (llamado base). Entonces todo número $n \in N$ puede escribirse de manera única en base b de la forma

$$n = a_k b^k + a_{k-1} b^{k-1} + ...+ a_1 b + a_0,$$

para algún $k \geq 0$, con $0 \leq a_i < b$, i = 0,1,..., k, y con $a_k \neq 0$.

Notación

De ahora en adelante cuando tengamos un número

$$n = a_k b^k + a_{k-1} b^{k-1} + ...+ a_1 b + a_0,$$

en base b, escribimos simplemente

$$n = (a_k\, a_{k-1} \,...a_1 a_0)_b$$

Hemos visto que los $a_i < b$. Si b es un número mayor que 10 los a_i pueden ser mayores o iguales que 10; por tanto, necesitamos nuevos símbolos. Usualmente se utilizan las letras del alfabeto. Así A = 10, B = 11, etc.

Si no se quiere utilizar más que las cifras del 0 al 9 otra opción sería representar el número $(a_k\, a_{k-1} \,...a_1 a_0)_b$ en la forma

$$(a_k\, a_{k-1} \,...a_1 a_0)_b$$

donde los $0 \leq a_i < b$ y no importa el número de cifras que tenga.

1-6-2 Criterio de divisibilidad por k

Sea n un número natural. Como:

$$n = a_t 10^t + a_{t-1} b^{t-1} + ...+ a_1 10 + a_0,$$

podemos escribir $\mathbf{n = \sum_{i=0}^{t} a_i 10^i}$

Consideramos ahora los restos de la división de 10^i por k para i = 0, 1, ..., t. Supongamos que son $r_0, r_1..., r_t$, donde $r_0 = 1$, ya que $10^0 = 1$ y estamos suponiendo $k \geq 2$. Tenemos entonces,

$$10^0 \equiv r_0 \text{ mód(k)}, 10^1 \equiv r_1 \text{ mód(k)}, ..., 10^t \equiv r_t \text{ mód(k)}.$$

Según visto en la sección 5:

$$\mathbf{n = \sum_{i=0}^{t} a_i 10^i \equiv \sum_{i=0}^{t} a_i r_i mód(k)}$$

luego n es divisible por k si y sólo si $\mathbf{\sum_{i=0}^{t} a_i r_i \equiv 0\ mód(k)}$ o, equivalentemente, si $\mathbf{\sum_{i=0}^{t} a_i r_i}$ es divisible por k.

2. INTRODUCCIÓN A LA TEORÍA DE GRAFOS

2.1 GRAFOS, DIGRAFOS Y MULTIGRAFOS

2-1-1 Definiciones: grafo (vértice, arista), multigrafo, pseudografo, digrafo, grafos isomorfos, grado de un vértice

Definición

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 el conjunto de aristas ("edges" en inglés) y sus elementos aristas. Se escribe G = (V, E) para designar el grafo G con conjunto de vértices V y conjunto 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 sus aristas.

Dado un grafo G.(V, E) sean u, v dos vértices de G, es decir u, v $\in$ V. Si e = {u, v } es una arista de G, {u, v } $\in$ 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.

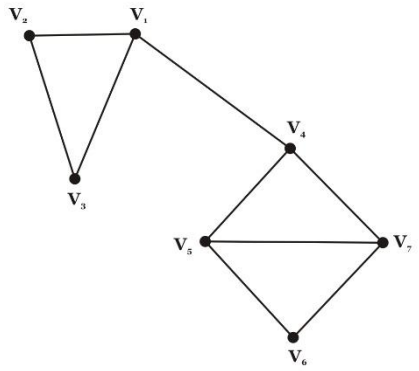


Fig. 2 Grafo con #V= 7 y #E = 9

Todo grafo se representa geométricamente (o se dibuja) mediante una figura (Fig. 2) construida del siguiente modo: a cada vértice se le hace corresponder un punto y si dos vértices son adyacentes se dibuja una línea uniendo los puntos correspondientes. Denotaremos por #V el número de vértices de un grafo (V, E) y por #E el número de aristas. Un grafo se dice que es finito si #V es finito. En estos apuntes solo estudiaremos los grafos finitos.

Un multigrafo es un grafo con (posiblemente) varias aristas entre dos vértices (Fig. 3.a), por tanto, en la definición formal de multigrafo, el conjunto de aristas puede contener algunas aristas distintas con el mismo par de extremos. Se denomina pseudografo cuando en un grafo están permitidas aristas cuyos extremos coinciden (Fig. 3.b), tales aristas se denominan lazos.

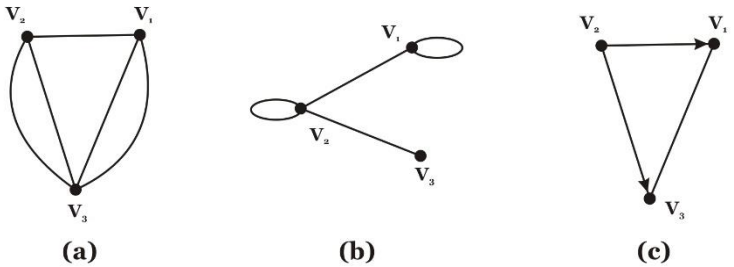


Fig. 3 (a) multigrafo (b) pseudografo (c) digrafo

Un digrafo 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 (Fig. 3.c). Se llama origen al primer vértice de una arista y fin al segundo. La diferencia formal consiste ahora en que los pares de vértices que definen las aristas en un digrafo son pares ordenados.

Por supuesto pueden aparecer multitud de variaciones de los conceptos anteriores como multidigrafos o pseudomultidigrafos.

Definición

Sean G = (V, E) y G' = (V', E') dos grafos y sea f: V $\rightarrow$ V' una biyección entre los conjuntos de vértices tal que uv $\in$ E si y sólo si f(u)f(v) $\in$ E'. La biyección f se denomina isomorfismo de G a G'. Se dice entonces que los grafos G y G' son isomorfos.

Definición

Sea G un grafo y u un vértice de G. Se llama grado de un vértice u en G, gr(u), al número de aristas de G que tienen al vértice u por extremo.

El grado de un vértice es un concepto que depende únicamente de la estructura matemática del grafo y por tanto se conserva por isomorfismo.

Proposición

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)).

2-1-2 Primer Teorema de la Teoría de Grafos

Teorema (Lema del apretón de manos)

Sean G = (V, E) un grafo, V = {v_1, …, v_p} el conjunto de vértices y #E el número de aristas. Entonces:

$$\sum_{i=1}^{p} \mathbf{gr}(\mathbf{v}_i) = 2\#\mathbf{E}$$

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

Definición de Grafo

Definición: Un **grafo**, es un para *G = (V, E)*, donde *V* es un conjunto finito no vacío cuyos elementos se llaman **vértices** o **nodos** y *E* es un conjunto cuyos elementos se llaman **aristas** o **ejes**.

- Si las aristas son "*pares no ordenados*" de vértices de *V*, entonces decimos que el grafo *G* es **no dirigido**. En este caso, denotaremos las aristas por *e* = {*u, v*} indicando que la arista *e* une los vértices *u* y *v*.
- Si las aristas son "*pares ordenados*" de vértices *V*, entonces decimos que el grafo G es **dirigido**. En este caso, denotaremos las aristas por *e* = (*u*, *v*) indicando que la arista *e* sale del vértice *u* y termina en el vértice *v*.

Si una arista une un vértice consigo mismo, se denomina **lazo**. Si un vértice no está conectado con a ningún otro vértice, se llama **vértice aislado**. Si un par de vértices están unidos por más de una arista, estás reciben el nombre de **aristas múltiples** o **aristas paralelas**. Un grafo sin lazos y aristas múltiples se denomina **grafo simple**.

Definición:

- Un par de vértices *u* y *v* son **adyacentes** si existe una arista que los une. Se dice que *e* = {*u*,*v*} **incide** en los vértices *u* y *v*, o que la arista *e* conecta *u* y *v*, o que los vértices *u* y *v* son **extremos** de la arista *e*.
- El **grado de un vértice** *v*, se denota por $\partial(v)$, es el número de aristas incidentes en *v*. Puesto que cada arista añade una unidad al grado de cada vértice en la que incide, por convención, un lazo en v contribuye con 2 unidades al grado de v. Todos los vértices que tienen grado 0 son **aislados** y los vértices con grado 1 se llaman **hojas**.
- La **sucesión de grados** de *G*, $(\partial(v))_{v\in V}$ es la sucesión formada por los grados de los vértices de G.

2-1-3 Subgrafo

Definición

Sea G = (V, E) un grafo. Un subgrafo de G es cualquier grafo H = (V(H), E(H)) de modo que V(H) está contenido en V y E(H) está contenido en E.

Los subgrafos de G se obtienen "borrando" o eliminando algunas aristas y vértices de G (Fig. 4Fig. 4), de modo que si suprimimos un vértice hemos de borrar todas las aristas que tienen tal vértice como extremo.

Se tiene que si H es un subgrafo de G y $v \in V(H) \subset V(G)$,

$$gr_H(v) \leq gr_G(v),$$

donde $gr_H(v)$ denota el grado del vértice y como vértice del grafo H y $gr_G(v)$ es el grado del vértice y como vértice del grafo G.

Definición de Subgrafo

Definición: Sea *G = (V, E)*, un grafo. Si *G'* = (*V'*, *E'*) es otro grafo donde $V' \subseteq V$ y $E' \subseteq E$, se dice que *G'* es un **subgrafo** de G. Si *V'* = *V* se llama **subgrafo recubridor** o **grafo parcial** de *G*.

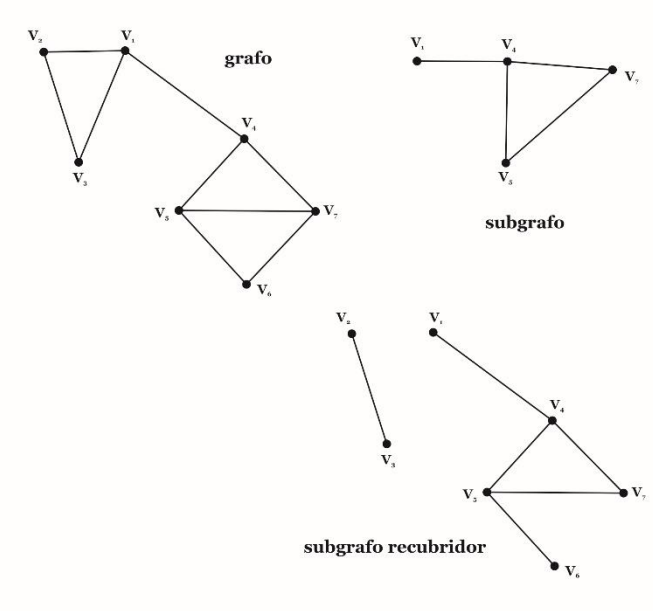


Fig. 4 Grafo, subgrafo y subgrafo recubridor

2-1-4 Grafo regular y grafo completo

Definición

Un grafo se dice regular si todos sus vértices tienen el mismo grado. Si dicho grado es k entonces el grafo se llama k-regular.

Definición

Un grafo para el que cualquier par de vértices está formado por los extremos de una arista se llama grafo completo.

Proposición

Dos grafos completos con el mismo número de vértices son isomorfos.

Designaremos al grafo completo con n vértices por K_n.

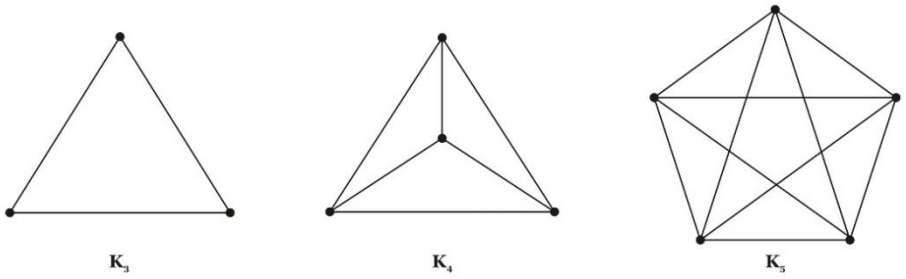


Fig. 5 Grafos completos

Grafos regulares y completos

Si *G* es un grafo con *n* vértices $|V| = n$, se dice que G es un grafo de **orden *n***. Si *G* es simple y de orden *n*, el grado de cada vértice está entre 0 y $n - 1$. Si *G* es un grafo simple y todos los vértices tienen grado r se dice que G es un grafo ***r*-regular**.

Se dice que un grafo simple es **completo** si cada vértice es adyacente a todos los demás, es decir, contiene, exactamente una arista entre cada par de vértices distintos. Un grafo completo de n vértices se denota por K_n. Este grafo es *$(n - 1)$-regular* y su número de aristas es n(n-1)/2.

2.2 GRAFOS EULERIANOS Y HAMILTONIANOS

2-2-1 Definiciones: camino, extremos de un camino, longitud de un camino

Definiciones

Sea G un grafo o un multigrafo. Un camino en G es una sucesión (finita) en la que aparecen alternadamente vértices y aristas de G:

$$v_0, v_0v_1, v_1, v_1v_2, v_2, \ldots, v_{n-1}, v_{n-1}\, v_n, v_n,$$

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

A los vértices v_0 y v_n se les denomina extremos del camino. También se dice que el camino conecta v_0 con v_n o que va de v_0 a v_n. La longitud del camino es el número n de aristas que contiene.

2-2-2 Tipos de caminos: cerrado, simple, ciclo, circuito, conexo

Un camino se dice que es cerrado si sus extremos coinciden, es decir $v_0 = v_n$. En un grafo (pero no en un multigrafo) un camino puede ser especificado simplemente por la sucesión de los vértices: $(v_0, \ldots v_n)$. 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 último, además, en el caso de caminos de longitud dos, sólo consideramos ciclos a aquellos caminos cerrados en multigrafos que no repiten aristas. Un circuito es un camino cerrado que no repite aristas.

Teorema

En un grafo G si existe un camino que conecta dos vértices distintos x e y de G entonces existe un camino simple con extremos x e y.

Definición

Un grafo G es conexo si para cada par de vértices u, v existe un camino cuyos extremos son u y v. En caso contrario decimos que G es desconexo.

2-2-3 Grafo euleriano

En la (Fig. 6.a) hemos esquematizado un plano de la antigua ciudad de Königsberg en la Prusia oriental, mostrando el río Pregel que pasa por la ciudad y los siete puentes que lo atravesaban en el siglo XVIII. Muchos habitantes de Königsberg se plantearon el reto de encontrar una ruta en la ciudad que recorriera los siete puentes cruzando cada uno de ellos una única vez y volviendo al punto de partida. Puesto que todos los intentos fueron fallidos se comenzó a pensar que era imposible encontrar tal recorrido. Este problema no fue estudiado matemáticamente hasta 1736 por Euler quien escribió un artículo

donde probó que no existía tal ruta[1]. Además, Euler en su artículo desarrolló una teoría que podía ser aplicada a otras muchas situaciones.

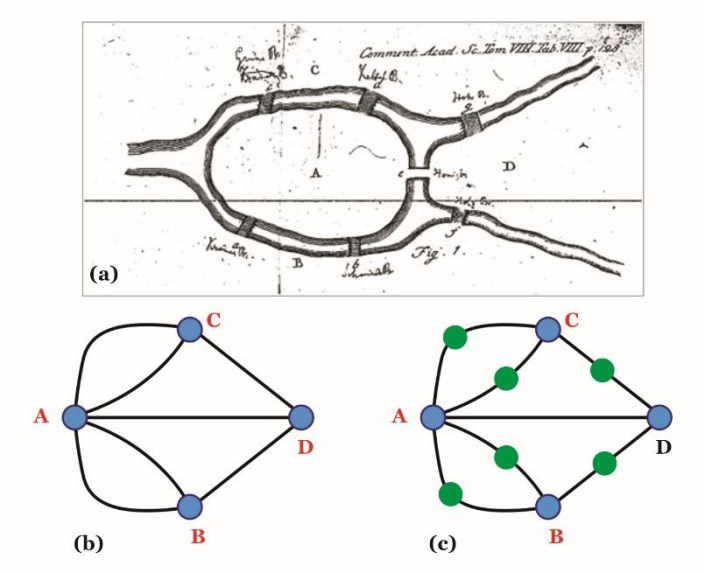


Fig. 6 Problema de los puentes de Königsberg

La primera gran idea de Euler fue reducir el problema de Königsberg a una cuestión de teoría de grafos. Para tal fin representó el mapa por un multigrafo donde cada sector terrestre de la ciudad venía representado por un vértice y cada puente por una arista que unía los vértices correspondientes a los sectores unidos por dicho puente. El resultado es el multigrafo (Fig. 6.b). Para conseguir un verdadero grafo basta añadir un vértice en el punto medio de cada arista obteniéndose el grafo G (Fig. 6.c). Así el problema de los puentes de Kiinigsberg se reduce a encontrar un circuito en el grafo que contenga todas las aristas, es el que se denomina como grafo euleriano.

Definición

Sea G un grafo, un camino (circuito) euleriano es un camino (resp. 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.

Otro modo de entender qué es un camino euleriano 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.

2-2-4 Caracterización de grafos eulerianos

Lema

Sea G un grafo. Si G es euleriano todo vértice de G tiene grado par.

[1] Euler, Leonhard (1736). *Solutio problematis ad geometriam situs pertinentis*. Comment. Acad. Sci. U. Petrop 8, 128-40 (en latín)

Lema

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 tienen grado impar.

Lema

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 a la arista uv.

Teorema

Un grafo conexo es euleriano si y solo si cada vértice tiene grado par.

Corolario

Un grafo conexo admite un camino euleriano no cerrado si y sólo si exactamente dos vértices tienen grado impar.

2-2-5 Grafo hamiltoniano

Hasta el momento, hemos considerado el problema de determinar si en un grafo hay un circuito que contiene todas las aristas. Otro problema famoso en Teoría de Grafos es determinar cuándo un grafo admite un ciclo que contiene a todos sus vértices.

Definición

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.

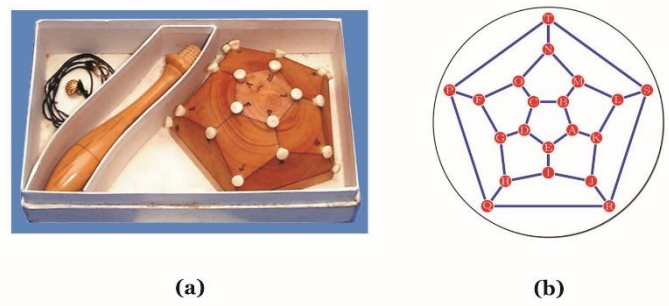


Fig. 7 (a) El *dodecaedro del viajero* (b) Grafo asociado

El problema de conocer si un grafo es hamiltoniano y en tal caso encontrar un ciclo hamiltoniano debe su nombre al famoso matemático Sir William R. Hamilton. Sin embargo, es de justicia señalar al matemático T. P. Kirkman como el primero en investigarlo. El motivo de la atribución a Hamilton es que éste diseñó un juego llamado El *dodecaedro del viajero* o el *viaje alrededor del mundo* (Fig. 7.a). Tal juego constaba de

un dodecaedro sólido donde los vértices del poliedro representaban veinte ciudades importantes de la época: Bruselas, Cantón, …, Zanzíbar. El juego consistía en encontrar un recorrido a través de las aristas del dodecaedro pasando una única vez por cada cuidad, tal recorrido se denominaba "un viaje alrededor del mundo". Con nuestra terminología el juego consistía en encontrar un ciclo hamiltoniano en el grafo de la (Fig. 7.b)

Por supuesto basta construir todos los ciclos de un grafo para saber si es hamiltoniano. Esta operación puede ser enormemente complicada si el grafo tiene muchos vértices. Más adelante se da una condición necesaria para que un grafo sea hamiltoniano. El problema de decidir si un grafo es hamilitoniano es un caso particular del problema "del vendedor ambulante" que trata de encontrar un camino hamiltoniano de longitud mínima atribuyendo a cada arista una longitud.

2-2-6 Componentes conexas de un grafo

Para enunciar la condición necesaria para que un grafo sea hamiltoniano necesitamos la noción de componentes conexas de un grafo.

Definición

Sea G un grafo y u, y dos vértices de G. Se dice que u y v están conectados en G si existe un camino de u a v.

Proposición

En un grafo G la relación en el conjunto de vértices dada por "estar conectado con" es una relación de equivalencia.

Definición

Las clases de equivalencia que define la relación "estar conectado con" en un grafo G se denominan componentes conexas de G.

Teorema

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 tienen extremos en V - U, tiene a lo más #U componentes.

2-2-7 Condición necesaria para que un grafo sea Hamiltoniano

Para acabar enunciaremos algunas condiciones suficientes, que aparecen en muchos tratados de Teoría de Grafos, para que un grafo sea hamiltoniano, o en otros casos posea un camino hamiltoniano. Las condiciones de estos resultados están en términos del número de vértices del grafo y de los grados de dichos vértices.

El siguiente resultado fue probado en 1952 por el matemático Gabriel A. Dirac (que no se debe confundir con el famoso matemático y físico, premio Nobel, Paul A. M. Dirac).

Proposición

Sea G= (V, E) un grafo con #V = n > 2. Si para todo vértice v $\in$ V se verifica que gr(v) ≥ n/2, entonces G es hamiltoniano.

El teorema siguiente es también bastante reciente, del año 1960, y se debe a Oystein Ore.

Proposición

Sea G = (V, E) un grafo con #V = n. Si gr(v) + gr(w) ≥ n - 1 para todo v, w $\in$ V, v ≠ w, entonces G tiene un camino hamiltoniano.

Corolario

Sea G = (V, E) un grafo con #V = n > 1. Si para todo vértice v $\in$ V se verifica que $\mathbf{gr(v) \geq \frac{n-1}{2}}$, entonces G tiene un camino hamiltoniano.

2.3 EXPLORACIÓN DE GRAFOS

2-3-1 Matriz de Adyacencia. Propiedades

Definición

Sea G = (V, E) un grafo con V = {v_1, ..., v_p}. Se denomina matriz de adyacencia a la matriz M = (m_{ij}) de orden p×p cuyas entradas son unos o ceros siguiendo la siguiente ley:

$$\mathbf{m_{ij} = 1 \quad si \quad v_i v_j \in E}$$
$$\mathbf{m_{ij} = 0 \quad si \quad v_i v_j \notin E}$$

Para el caso de digrafos se define la matriz de adyacencia del siguiente modo:

Definición

Sea G = (V, E) un digrafo con V = {v_1, ..., v_p}. La matriz de adyacencia de G es la matriz M = (m_{ij}) de orden p×p cuyas entradas son unos o ceros definida por:

$$\mathbf{m_{ij} = 1 \quad si \quad v_i v_j \in E \text{ y la orientación de tal arista es } v_i \to v_j}$$
$$\mathbf{m_{ij} = 0 \quad si \quad v_i v_j \notin E \text{ o bien } v_i v_j \in E \text{ y la orientación de tal arista en G es } v_j \to v_i}$$

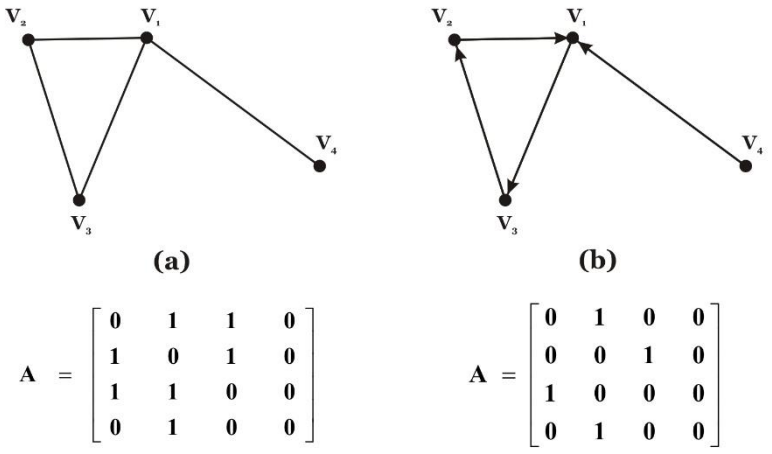


Fig. 8 Matriz de adyacencia (a) grafo y (b) digrafo

Proposición

Sean G y G' dos grafos con la misma matriz de adyacencia, entonces G y G' son isomorfos.

Análogamente si dos digrafos tienen la misma matriz de adyacencia entonces son digrafos isomorfos. Sin embargo, puede ocurrir que dos grafos isomorfos estén representados por matrices diferentes (basta permutar el orden de los vértices).

Puesto que en un grafo G = (V, E) con vértices V = {v_1, ..., v_p} la arista $v_iv_j \in E$ es la misma que v_jv_i, la matriz de adyacencia de un grafo es una matriz simétrica, cosa que no ocurre para los digrafos.

Una de las grandes ventajas de la representación de grafos mediante matrices es el uso de las técnicas de álgebra lineal. Aunque ya habíamos definido camino en grafos y multigrafos necesitamos ahora caminos en digrafos y los conceptos de origen y fin de un camino.

Definición

Sea G un digrafo. Un camino en G es una sucesión (finita) en la que aparecen alternativamente vértices y aristas de G:

$$v_0, v_0v_1, v_1, v_1v_2, v_2, \ldots, v_{n-1}, v_{n-1}v_n, v_n,$$

donde cada arista v_iv_{i+1} tiene por origen a v_i y por fin a v_{i+1}. A los vértices v_0 y se les denomina origen y fin del camino respectivamente. El número de aristas del camino se denomina longitud.

Teorema

Sea M la matriz de adyacencia de un grafo (digrafo) G con p vértices, p>1. Entonces la entrada (i, j) de la matriz $\mathbf{M^n} = \mathbf{M} \times \overset{n}{\cdots} \times \mathbf{M}$ es el número de caminos de longitud n con extremos v_i y v_j (en el caso de digrafos es el número de caminos de longitud n con origen v_i y fin v_j).

Corolario

Sea M la matriz de adyacencia de un grafo G con p vértices, v_1, ..., v_p, con p > 1. Sea C = $M^{p-1} + M^{p-2} + \cdots + M$. Existe un camino entre v_i y v_j si y sólo si la entrada en el lugar (i, j) de la matriz C es no nula.

Corolario

Sea M la matriz de adyacencia de un grafo G con p vértices, p > 2. Sea C = $M^{p-1} + M^{p-2} + \cdots + M$. El grafo G es conexo si y solo si todas las entradas de C son no nulas.

2-3-2 Árbol

Hasta el momento hemos estado interesados en conocer si en un grafo dado existe un camino que une dos vértices, en ocasiones es conveniente construir o considerar grafos donde cada par de vértices está unido por un único camino simple. Demostraremos que en tales grafos no pueden existir ciclos. En la siguiente definición introducimos este tipo especial de grafos que constituye uno de los más útiles.

Definición

Un árbol es un grafo conexo sin ciclos.

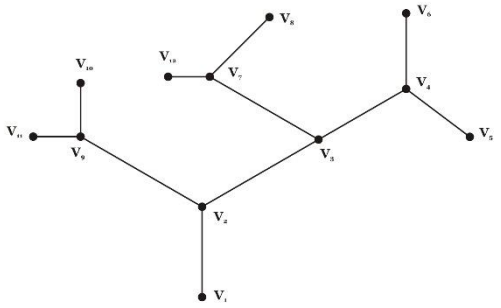


Fig. 9 Árbol

Teorema

Un grafo T es un árbol, si y sólo si, cada dos vértices distintos de T se conectan por un único camino simple.

Es importante observar que en virtud del teorema anterior en un árbol no hay que elegir entre varias opciones para determinar el camino entre dos vértices. Esta observación es muy importante sobre todo en informática. El tener varias opciones para ir de un lugar a otro es una riqueza que puede ofrecer grandes ventajas. Sin embargo, al construir un algoritmo en el que es necesario unir vértices de un grafo conexo es importante establecer una estrategia para elegir en cada momento el camino que se debe seguir. El siguiente resultado, al menos de modo teórico soluciona el problema, pues nos dice que en todo grafo conexo existe un subgrafo que es un árbol y que tiene el mismo conjunto de vértices. Eligiendo un tal árbol en un grafo, cada par de vértices del grafo se une por un único camino contenido en el árbol, esto precisamente soluciona el problema de elección que comentábamos.

Teorema

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 se denomina subárbol conectante o subárbol maximal de G (en inglés: *spanning-tree*).

Definición

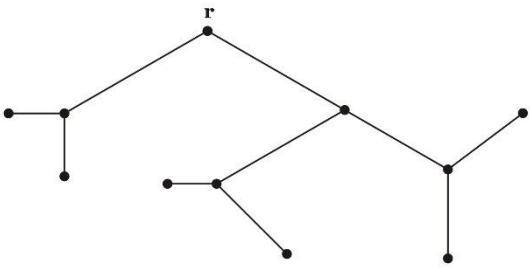


Fig. 10 Árbol con raíz r

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 y será mayor que otro w si y "está más cerca que" w de la raíz r. Es una relación de orden parcial porque en general no siempre se pueden comparar dos vértices del árbol.

Definición

Sea (T, r) un árbol con raíz y v, w dos vértices de T. Se dice que $v \geq w$ si el camino simple que une r con w pasa por el vértice v.

Obsérvese que es de importancia capital en la definición anterior el hecho de que entre dos vértices de un árbol hay un único camino simple que los une.

Proposición

La relación entre los vértices de un árbol con raíz (T, r) es una relación de orden. Es decir, verifica las propiedades:

(a) Reflexiva: $v \geq v$ para cada vértice de T.
(b) Antisimétrica: Si $v \geq w$ y $w \geq v$ entonces $v = w$.
(c) Transitiva: Si u, y, w son tres vértices de T tales que $u \geq v$ y $v \geq w$, entonces $u \geq w$.

La relación de orden de la proposición anterior permite definir un digrafo a partir de un árbol con raíz. En efecto, sea (T, r) un árbol con raíz (Fig. 10), Hemos de orientar las aristas de T. Si vw es una arista de T, v será el origen y w el final si $v \geq w$. Es decir, orientamos cada arista en el sentido de alejamiento de la raíz r (Fig. 11).

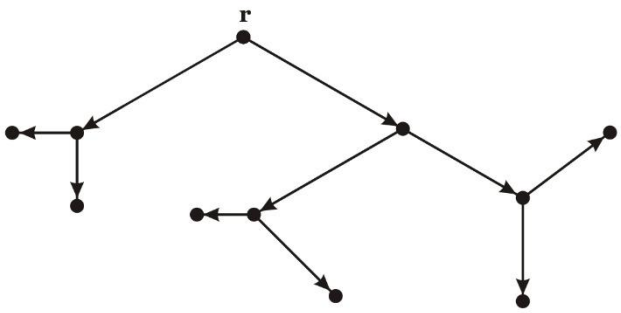


Fig. 11 Digrafo asociado al árbol Fig. 10

Normalmente los árboles con raíz se suelen representar de forma que la raíz esté situada en la parte más alta de la figura y que las aristas desciendan siguiendo la orientación y distribuyendo así los vértices en niveles por altura. El digrafo de la Fig. 11 se representaría como muestra la Fig. 12.

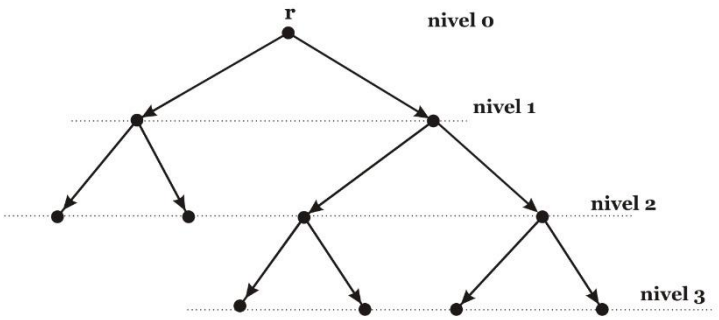


Fig. 12

En un grafo con raíz, los vértices que tienen grado uno y son distintos de la raíz se llaman vértices terminales o siguiendo una terminología más natural y botánica hojas (Fig. 13).

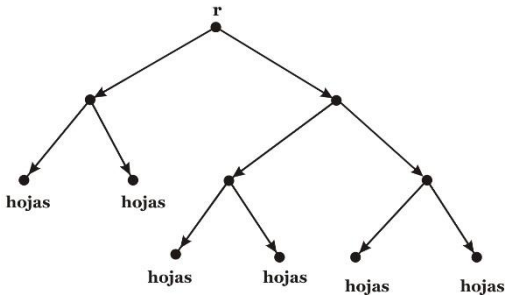


Fig. 13 Vértices terminales o hojas

2-3-3 Grafo etiquetado

A continuación, vamos a estudiar un método para obtener los caminos más económicos que unen dos vértices. Con el método que presentaremos también se pueden conseguir subárboles maximales que optimizan los recorridos dentro de un grafo.

Definición

Un grafo o digrafo G se dice que es un grafo etiquetado si sus aristas tienen asignado un número. Es decir, existe una aplicación d: E(G) $\rightarrow$ 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 a_1, …, a_r, se denomina longitud de tal camino a $d(a_1)$ +...+ $d(a_r)$.

Obsérvese que si todas las etiquetas son 1 la definición de longitud en un grafo o digrafo etiquetado coincide con la de longitud de un camino en un grafo o digrafo. Dados dos vértices de un grafo etiquetado se denomina distancia entre tales vértices a la longitud del camino de longitud mínima entre dichos vértices.

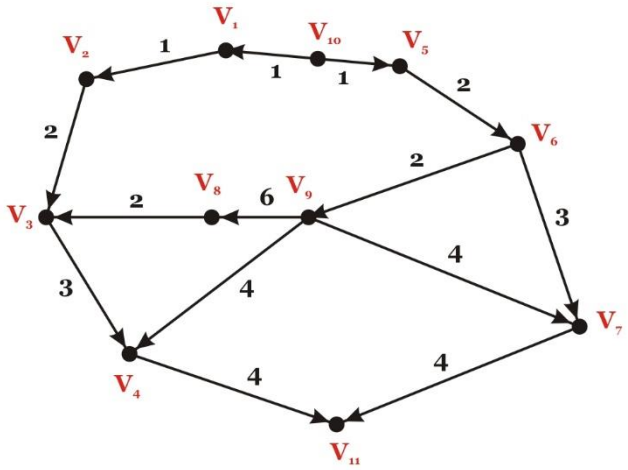


Fig. 14 Digrafo etiquetado

2-3-4 Algoritmo de Dijkstra

Sea G = (V, E) un digrafo etiquetado, es decir tenemos d: E $\rightarrow$ 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 $\rightarrow$R $\cup$ {∞} (donde R es el conjunto de números reales), dada 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 $\in$ 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 $\in$ 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.

2.4 MAPAS Y COLORACIONES

2-4-1 Grafos Planos

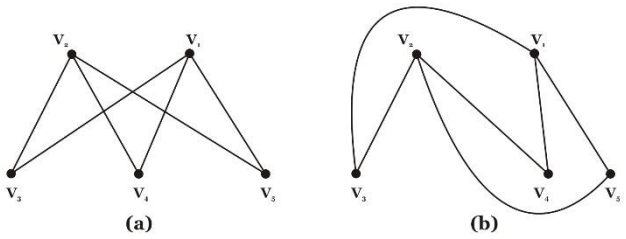


Fig. 15 El grafo (a) es plano pues se puede representar por (b)

Definición

Un grafo (multigrafo) 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.

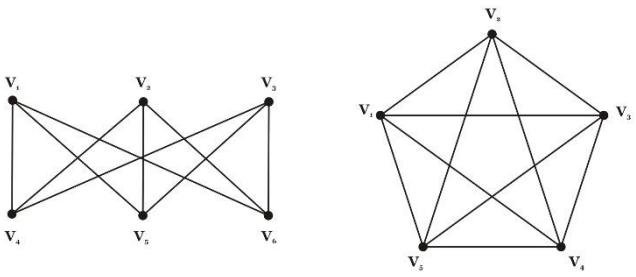


Fig. 16 Grafos no planos

2-4-2 Mapa asociado a un grafo plano. Región y grado de una región

Definición

Sea G un grafo (multigrafo) plano, una representación del grafo en el plano en las condiciones de la definición anterior se denomina mapa. Diremos que el mapa es conexo si el grafo que representa es conexo. Un mapa divide al plano en varias *partes* que se denominan regiones y su número lo representaremos por #R.

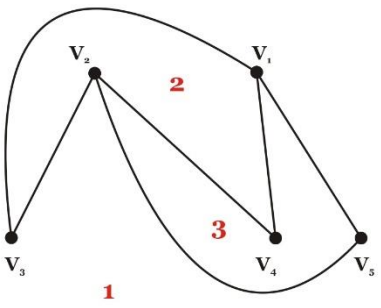


Fig. 17 Regiones de un mapa

Definición

Se denomina grado de una región a la longitud del camino que la bordea.

Teorema

La suma de los grados de las regiones de un mapa es igual al doble del número de aristas del grafo que representa.

2-4-3 Fórmula de Euler

Teorema

Sea M un mapa conexo con #R regiones que represente el grafo G = (V, E), entonces:

$$\#V - \#E + \#R = 2.$$

Corolario

Sea G = (V, E) un grafo plano conexo, con #V > 2. Entonces: $\#E \leq 3\#V - 6$.

Corolario

Sea G = (V, E) un grafo plano, conexo, con #V > 2. Supongamos que en G no existe ningún subgrafo isomorfo a K_3, entonces $\#E \leq 2\#V - 4$.

2-4-4 Subdivisión de un grafo

Definición

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 número finito (puede ser cero) de subdivisiones elementales sucesivas.

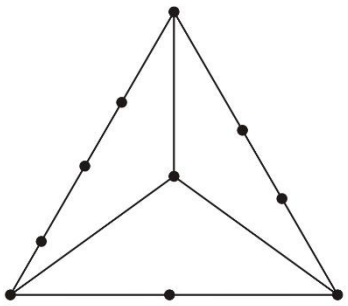


Fig. 18 Subdivisión de K_4

2-4-5 Teorema de Kuratowski

Teorema

Un grafo G es plano si y sólo si no contiene ningún subgrafo que sea isomorfo a una subdivisión de K_5 o $K_{3,3}$

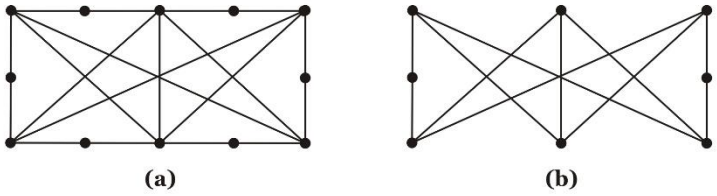


Fig. 19 El grafo (a) no es plano pues contiene el subgrafo (b) que es una subdivisión de $K_{3,3}$

2-4-6 Pseudomultigrafo dual de un mapa

La noción de mapa nos permite enunciar uno de los problemas más famosos en la historia de las Matemáticas: *el problema de los cuatro col*ores. Este problema apareció por primera vez en una carta enviada por Augusto DeMorgan a Sir William R. Hamilton con fecha de 23 de octubre de 1852. En su carta, DeMorgan se refiere a una cuestión que le preguntó uno de sus estudiantes. Como él no había conseguido una respuesta satisfactoria trasladaba la pregunta a su colega Hamilton. La pregunta era la siguiente: En un mapa se dice que dos regiones distintas son adyacentes si en los caminos cerrados que definen sus bordes hay alguna arista común. ¿Se puede colorear cualquier mapa plano con cuatro colores diferentes de modo que no haya dos regiones adyacentes con el mismo color? Durante más de 100 años se hicieron muchos intentos para resolver el problema, algunos de tales intentos dieron lugar a falsas soluciones siendo algunas publicadas como ciertas y originando ideas matemáticas interesantes y útiles. En 1977, K.Appel, W. Haken y J. Koch publicaron una prueba de que todo mapa plano se puede colorear con, a lo más, cuatro colores (Teorema de los Cuatro Colores). Sin embargo la demostración de Appel, Haken y Koch ha generado grandes controversias pues se apoya esencialmente en cálculos efectuados por un ordenador. Más concretamente unos dos mil casos tuvieron que ser analizados por un ordenador que tardó más de 1 200 horas. Sin embargo, después de más de quince años los matemáticos que han analizado la prueba han dado crédito a los autores. De todos modos, una prueba más directa de este bello resultado es un sueño que muchos matemáticos anhelan y no pierden la esperanza de encontrar.

Veremos ahora una traducción a la teoría de grafos del Teorema de los cuatro colores por medio del concepto de grafo dual de un mapa:

Definición

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 arista en común. El pseudomultigrafo dual G_M de M se define como un pseudomultigrafo

construido del siguiente modo: tomamos como conjunto de vértices las regiones de M y a cada arista e de G le asociamos una arista e* de G_M de modo que, si e separa las regiones adyacentes s, t de M (podría ser s = t) entonces e* conecta los vértices correspondientes a dichas regiones (si s = t, entonces e* es un lazo).

El pseudomultigrafo dual G_M de un mapa M es un pseudomultigrafo plano pues se puede conseguir un mapa que represente GM del siguiente modo: Cada vértice de G_M se representará por un punto en la región correspondiente de M, para representar cada arista de G_M 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 (Fig. 20)

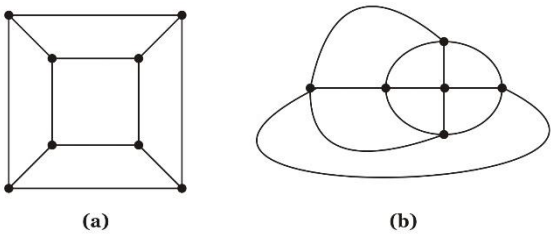


Fig. 20 Mapa (a) y su grafo dual (b)

2-4-7 Coloración de un mapa

Definición

Sea G = (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 $\gamma: V \to C$, de modo que si u, v $\in$ V y uv $\in$ E entonces $\gamma(u) \neq \gamma(v)$.

2-4-8 Teorema de los Cuatro Colores

Corolario

Todo grafo plano admite una coloración con cuatro colores.

2-4-9 Grafos Bipartitos

Existen grafos (por supuesto no planos) que exigen más de cuatro colores para colorear sus vértices y también otros grafos que exigen menos. A continuación, estudiaremos el caso más sencillo de los grafos que admiten coloraciones con dos colores.

Definición

Un grafo G = (V, E) se dice que es bipartito si existe una coloración con dos colores, γ: $V \to \{0, 1\}$. Normalmente se consideran los colores blanco y negro en lugar de 0 y 1.

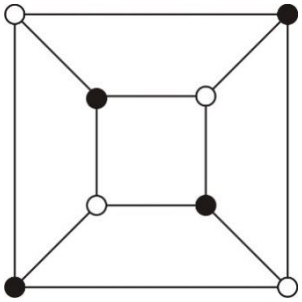


Fig. 21 Grafo bipartito

Teorema

Un grafo es bipartito si y sólo si no tiene ciclos con longitud impar.

Definición

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.

3. MÉTODOS COMBINATORIOS

3.1 TÉCNICAS BÁSICAS

3-1-1 Principio de Adición

Sea S un conjunto finito no vacío. Se designará por |S| al cardinal de S, es decir, el número de elementos de S. En particular $|\varnothing| = 0$.

Teorema (Principio de Adición)

Sean $A_1, A_2, ..., A_n$ conjuntos finitos tales que $A_i \cap A_j = 0$ para cada $i \neq j$, $i, j \in \{1, 2,..., n\}$, entonces:

$$I\, A_1 \cup A_2 \cup \cdots \cup A_n\, I = IA_1I + IA_2I + \cdots + IA_nI.$$

3-1-2 Principio de Multiplicación

Teorema (Principio de Multiplicación)

Sean $A_1, A_2, ..., A_n$ una colección de conjuntos finitos no vacíos, entonces:

$$I\, A_1 \times A_2 \times \cdots \times A_n\, I = IA_1I \cdot IA_2I \cdot \cdots \cdot IA_nI.$$

El resultado del Teorema anterior se puede exponer de un modo informal, pero más práctico, como sigue: Supongamos que un experimento consiste en seleccionar n objetos de manera que la primera elección consiste en elegir un elemento de un subconjunto de m_1, objetos, la segunda elección consiste en elegir otro elemento de un subconjunto de m_2 objetos y así sucesivamente. Para la elección n-ésima se dispone de m_n objetos. Entonces, la selección se puede realizar de $m_1m_2 ... m_n$ formas diferentes.

3-1-3 Principio de Distribución

Supongamos ahora que se desea introducir m objetos en n cajas siendo m > n. Intuitivamente vemos que alguna de las cajas deberá contener más de un objeto. Vamos a generalizar y probar este resultado.

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.

Este principio también es conocido como el *Principio del Cajón de Dirichlet*, desde que el matemático alemán Peter G. L. Dirichlet (1805-59)10 usó para probar algunos resultados en Teoría de Números.

Corolario

Dados n números enteros positivos m_1, m_2, ..., m_n tal que

$$\frac{\sum_{I=1}^{N} m_i}{n} > p$$

entonces para algún $1 \leq i \leq n$ se tiene que $m_i > p$.

Podemos expresar el Principio de Distribución de la siguiente manera: Si se efectúa una partición en n partes de un conjunto finito T entonces al menos una de las partes posee $|T|/n$ o más elementos.

3.2 PERMUTACIONES, VARIACIONES Y COMBINACIONES

3-2-1 Permutaciones

Definición

Sea A un conjunto finito no vacío. Una permutación de A es una biyección de A en A. Diremos que dos permutaciones son diferentes si las biyecciones son diferentes.

Sean $A = \{ a_1, a_2,..., a_n\}$ y $\sigma: A \rightarrow A$ una permutación. Sea $\sigma(a_i)$ la imagen de a_i $1 \leq i \leq n$. La permutación a usualmente se representa por

$$\begin{pmatrix} \mathbf{a_1} & \mathbf{a_2} & \cdots & \cdots & \mathbf{a_n} \\ \boldsymbol{\sigma}(\mathbf{a_1}) & \boldsymbol{\sigma}(\mathbf{a_2}) & \cdots & \cdots & \boldsymbol{\sigma}(\mathbf{a_n}) \end{pmatrix}$$

Obsérvese que a cada ordenación de los elementos de A $(a_{\alpha(1)}, a_{\alpha(2)}, ..., a_{\alpha(n)})$ se le puede asociar una biyección de A definida por $\sigma(a_i) = a_{\alpha(i)}$, y recíprocamente a cada biyección σ se le puede asociar la ordenación $(\sigma(a_i), \sigma(a_2),..., \sigma(a_n))$, así las permutaciones pueden considerarse como las ordenaciones de los elementos de A.

Puesto que las permutaciones de A son biyecciones de A en A tiene sentido efectuar la composición de dos permutaciones consideradas como aplicaciones. Llamaremos a esta operación producto de permutaciones.

Definición

Sean σ_1 y σ_2 dos permutaciones del conjunto A. Llamaremos producto de σ_1 y σ_2, y escribiremos $\sigma_1 \cdot \sigma_2$, a la permutación σ de A tal que

$$\sigma(a) = \sigma_2(\sigma_1(a)) \text{ para todo } a \in A.$$

El conjunto de todas las permutaciones de un conjunto A con la operación de producto tiene estructura algebraica de grupo y se denomina grupo simétrico de A. Se designa habitualmente por S_A.

$$\text{Si } A = \{1, 2, \ldots, n\} \in N, \text{ entonces denotaremos a } S_A \text{ por } S_n.$$

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 colocación de n objetos. Si las localizaciones se numeran de 1 a n, al proceso que mueve un objeto del lugar i al lugar j, se le puede asociar a una permutación a de S_n tal que $\sigma(i) = j$.

3-2-2 Número de permutaciones de un conjunto de n elementos

Teorema

Sean A y B conjuntos con n elementos cada uno. El número de biyecciones distintas de A a B es $n\cdot(n - 1)\cdot(n - 2)...2\cdot1$.

El número de biyecciones distintas de A a 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:

Corolario

El número de permutaciones de un conjunto de n, elementos que designaremos por P(n), es n! Así $|Sn| = n!$

3-2-3 Variaciones y variaciones con repetición

Definición

Sean A un conjunto finito con n elementos ($n > 0$) y r un número natural $r < n$. Una variación de orden r de A es una lista ordenada $(a_1, a_2, a_3, ..., a_r)$ de elementos de A distintos. Diremos que dos variaciones son diferentes si algún elemento de una de las dos listas no se encuentra en la otra, o bien si las dos listas contienen 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 utiliza la frase: V(n, r) es el número de variaciones de n elementos tomados de r en r.

Observación

Si $(a_1, a_2, a_3, ..., a_r)$ es una variación de orden r de A, entonces podemos asociarle la aplicación inyectiva:

$$\sigma: \{1,2,...,r\} \rightarrow A,$$

definida por $\sigma(i) = a_i$ para $1 \leq i \leq r$. Además, a cada aplicación inyectiva

$$\sigma: \{1,2,...,r\} \rightarrow A$$

le podemos asociar la variación, $(\sigma(1), \sigma(2), ...,\sigma(r))$.

Por lo tanto, es equivalente el definir una variación de orden r como una lista ordenada $(a_1, a_2, a_3, ..., a_r)$ de elementos de A distintos, o bien mediante una aplicación inyectiva

$$\sigma: \{1,2,...,r\} \rightarrow A.$$

Por esta observación, se tiene que las permutaciones del conjunto A pueden ser consideradas un caso particular de variaciones de orden r de A, con r = n.

Definición

Sean A un conjunto finito con n elementos (n > 0) y r un número natural. Una variación con repetición de orden r, de A es una lista ordenada (a_1, a_2, a_3, ..., a_r) de elementos de A, en donde los elementos pueden ser iguales. Diremos que dos variaciones con repetición son diferentes si algún elemento de una las dos listas no se encuentra en la otra, o bien si las dos listas contienen los mismos elementos en distinto orden.

Designaremos el número 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.

Observación

Si (a_1, a_2, a_3, ..., a_r) es una variación con repetición de orden r de A, entonces podemos asociarle la aplicación:

$$\sigma: \{1,2,...,r\} \rightarrow A,$$

definida por $\sigma(i) = a_i$ para $1 \leq i \leq r$. Además, a cada aplicación

$$\sigma: \{1,2,...,r\} \rightarrow A,$$

le podemos asociar la variación con repetición de orden r, ($\sigma(1)$, $\sigma(2)$, ...,$\sigma(r)$).

Por lo tanto, es equivalente el definir una variación con repetición de orden r como una lista (a_1, a_2, a_3, ..., a_r) de elementos de A, o bien mediante una aplicación

$$\sigma: \{1,2,...,r\} \rightarrow A.$$

3-2-4 Número de variaciones, de orden r, de un conjunto de n elementos (con y sin repetición)

De la misma forma que en el caso de las permutaciones nos podemos plantear ahora el cálculo de V(n, r).

Teorema

Sean A y B dos conjuntos no vacíos con IAI = r, IBI=n y $r \leq n$. Entonces el número de aplicaciones inyectivas de A a B es

$$n \cdot (n-1) \cdots (n-r+1) = \frac{n!}{(n-r)!}$$

Corolario

Sean A un conjunto finito con n elementos (n > 0) y r un número natural r ≤ n. Entonces el número de variaciones de orden r de A es

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

El cálculo de la variaciones con repetición VR(n, r), será:

Teorema

Sean A y B dos conjuntos no vacíos con |A| = r, |B|= n. Entonces el número de aplicaciones de A a B es

n^r.

Corolario

Sean A un conjunto no vacío con n elementos (n > 0) y r un número natural. Entonces el número de variaciones con repetición de orden r de A es

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

3-2-5 Combinaciones y combinaciones con repetición

Definición

Sean A un conjunto finito con n elementos (n > 0) y r un número natural r ≤ n. Una combinación de orden r de A es una lista (a_1, a_2, a_3, ..., a_r) 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 $\binom{n}{r}$ (esta notación fue introducida por Euler). Llamaremos a $\binom{n}{r}$ número combinatorio.

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

Definición

Sean A un conjunto finito con n elementos (n > 0) y r un número natural. Una combinación con repetición de orden r de A es una lista (a_1, a_2, a_3, ..., a_r) de elementos

de A, en donde los elementos pueden ser iguales. Diremos que dos combinaciones con repetición son diferentes si algún elemento de una la dos listas no se encuentra en la otra.

Designaremos el número de combinaciones con repetición 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.

3-2-6 Número de combinaciones, de orden r, de un conjunto de n elementos (con y sin repetición)

Teorema

Para todo $n \in N$ y para todo $r \leq 1 \leq n$,

$$V(n, r) = r!\, C(n, r).$$

Por lo tanto

$$\mathbf{C(n,r) = \frac{n!}{r!\ (n\text{-}r)!}}$$

En el caso particular de r = 0, definiremos C(n, 0) = 1.

El problema de encontrar el número de combinaciones con repetición de orden r de un conjunto $A = \{b_1, ..., b_n\}$, es equivalente al problema de encontrar el número de soluciones enteras no negativas de la ecuación

$$x_1 + x_2 + ... + x_n = r.$$

Sea $(a_1, a_2, a_3, ..., a_r)$ una lista de elementos de A, si designamos por y_i i = 1, …, n, el número de veces que aparece el elemento b_i , i = 1, …, n, de A en la lista, se tiene una solución de la ecuación, puesto que

$$y_1 + y_2 + ... + y_n = r.$$

Recíprocamente, a cada solución $x_1, ..., x_n$ de la ecuación le podemos asociar la lista $(\mathbf{b_1,..^{x_1}..,b_1,... ,b_n,..^{x_n}..,b_n})$.

Teorema

Sean k y n enteros positivos. El número de soluciones enteras no negativas de la ecuación

$$x_1 + x_2 + ... + x_n = r.$$

es C(n + k - 1, k).

Corolario

El número de combinaciones con repetición de orden k de un conjunto A de n elementos es CR(n,k) = C(n + k - 1, k)

3-2-7 Permutación circular de n objetos

Definición

Una permutación circular de n objetos distintos de orden r, r ≤ n, es una colocación ordenada de r de los n objetos en r posiciones igualmente espaciados sobre una circunferencia.

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

Teorema

El número de permutaciones circulares de n objetos distintos de orden r, r ≤ n es

$$C(n, r)\cdot(r - 1)!.$$

Definición

Una permutación circular de n objetos distintos de orden n se denominará permutación circular de n objetos.

3-2-8 Resumen

Agrupación	Importa el Orden	Puede Repetirse	En cada Agrupación	FÓRMULA
Variaciones	SI	NO	$r < n$	$V(n,r) = \frac{n!}{(n-r)!}$
Variaciones Repetición	SI	SI	$r < n$	$VR(n,r) = n^r$
Permutaciones	SI	NO	$r = n$	$P(n) = n!$
Permutaciones Repetición	SI	SI	$r = n$	$PR_n^r = \frac{n!}{r_1!\cdot r_2!\cdot r_3!\ldots}$
Combinaciones	NO	NO	$r \leq n$	$C(n,r) = \binom{n}{r} = \frac{n!}{r!\cdot(n-r)!}$
Combinaciones Repetición	NO	SI	$r \leq n$	$CR(n,r) = \binom{n+r-1}{r}$

3.3 TEOREMA DEL BINOMIO

3-3-1 Propiedades algebraicas de los números combinatorios

Proposición

Sean k y n números enteros tales que 0 ≤ k ≤ n, entonces

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

Corolario (Fórmula de Pascal)

Si n y k son enteros tales que 1 ≤ k ≤ n-1, entonces

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

3-3-2 El Triángulo de Pascal

La fórmula de Pascal da un método para el cálculo de los coeficientes binómicos, dado el valor inicial:

$$\binom{n}{0}=\binom{n}{n}=1$$

para todo n ≥ 0. Los coeficientes de las sucesivas potencias de $(a + b)^n$ se pueden distribuir en una figura como sigue, que se conoce como triángulo de Pascal

$$\begin{array}{ccccccc}
 & & & \binom{0}{0} & & & \\
 & & \binom{1}{0} & & \binom{1}{1} & & \\
 & \binom{2}{0} & & \binom{2}{1} & & \binom{2}{2} & \\
\binom{3}{0} & & \binom{3}{1} & & \binom{3}{2} & & \binom{3}{3}
\end{array}$$

Desarrollando los números combinatorios se tiene:

$$
\begin{array}{ccccccccccc}
 & & & & & 1 & & & & & \\
 & & & & 1 & & 1 & & & & \\
 & & & 1 & & 2 & & 1 & & & \\
 & & 1 & & 3 & & 3 & & 1 & & \\
 & 1 & & 4 & & 6 & & 4 & & 1 & \\
1 & & 5 & & 10 & & 10 & & 5 & & 1
\end{array}
$$

En el triángulo de Pascal se tiene que:

1) El primer y último elemento de cada fila es 1.
2) Cualquier otro número del triángulo se puede obtener sumando los dos números que aparecen encima de él.

El triángulo de Pascal es una de las tablas de números que más ha influido en la historia de las Matemáticas. Fue descubierto en occidente por Blaise Pascal en su tratado *Traité du Triangle Arithmétique* que fue publicado en 1665. Este triángulo también es llamado el *triángulo de Yang Hui's*, porque fue descubierto en 1261 por este matemático chino. El mismo triángulo también fue incluido en el libro *El espejo precioso de los cuatro elementos* por otro matemático chino Chu Shih-Chieh en 1303.

3-3-3 Teorema del Binomio (coeficientes binomiales)

Teorema

Para cada n ∈ N y para cada par de elementos x, y ∈ R.

$$(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} \cdot x^{n-k} \cdot y^k$$

Esta fórmula se denomina también fórmula del Binomio de Newton (1642-1727), esta fórmula fue generalizada por Newton en 1 676 en el caso de que n fuese racional y por Abel (1 802-1 829) en el caso de n fuese complejo.

En el Teorema anterior haciendo y = 1 obtenemos el siguiente:

Corolario

Para cada n ∈ N y para cada par de elementos x, y ∈ R.

$$(1+x)^n = \sum_{k=0}^{n} \binom{n}{k} \cdot x^k$$

R se puede sustituir por cualquier conjunto con una estructura de cuerpo.

A los coeficientes $C(n,k)=\binom{n}{k}$ también se les llama coeficientes binómicos.

Si en $(1+x)^n=\sum_{k=0}^{n}\binom{n}{k}\cdot x^k$ hacemos x = 1, tenemos:

$$2^n=\binom{n}{1}+\binom{n}{2}+\binom{n}{3}+\cdots+\binom{n}{n}=\sum_{k=0}^{n}\binom{n}{k}$$

Y para x = -1, tenemos:

$$0=\binom{n}{1}-\binom{n}{2}+\binom{n}{3}-\cdots\pm(-1)^n\binom{n}{n}$$

Teorema

Para cada m, k $\in$ N $\cup$ {0} y para k ≤ m se tiene la siguiente igualdad

$$\binom{m+1}{k+1}=\binom{k}{k}+\binom{k+1}{k}+\cdots+\binom{m}{k}$$

3-3-4 Coeficientes multinómicos

Definición

Sean n, n_1, n_2, ..., n_k números enteros no negativos, con $n=\sum_{1}^{k}n_i$. Se define el coeficiente multinómico P(n_1, n_2, ..., n_k) como

$$\frac{n!}{n_1!n_2!\cdots n_k!}$$

que también se escribe $\binom{n}{n_1n_2\cdots n_k}$

Teorema

Dados n objetos de k tipos, con n_i objetos del tipo i, para 1 ≤ i ≤ k y con $\sum_{1}^{k}n_i=n$, entonces hay $\frac{n!}{n_1!n_2!\cdots n_k!}$ diferentes ordenaciones de estos n objetos. En donde consideráremos que dos ordenaciones son iguales si para cada i, 1 ≤ i ≤ k, los objetos que ocupan el lugar i son del mismo tipo.

3-3-5 Fórmula de Leibniz

Los coeficientes multinómicos surgen, al igual que los binómicos, de la consideración de expresiones algebraicas del tipo

$$(x_1 + x_2 + \ldots + x_k)^n$$

donde los x_i son elementos de un cuerpo y n es un número natural. Si escribimos

$$(x_1 + x_2 + \cdots + x_k)^n = (x_1 + x_2 + \cdots + x_k) \cdot (x_1 + x_2 + \cdots + x_k) \cdots^{n-1} \cdots (x_1 + x_2 + \cdots + x_k)$$

tras efectuar los productos de la derecha y agrupar los términos semejantes tenemos que cada término es de la forma

$$x_1^{n_1} \cdot x_2^{n_2} \cdots x_k^{n_k} \text{ con } n_1 + n_2 + \cdots + n_k = n$$

multiplicado por un coeficiente. Este coeficiente es el número de formas distintas de seleccionar n_1 factores x_1, n_2 factores x_2, etc. Con $n_1 + n_2 + \ldots + n_k = n$. Por tanto el coeficiente es $\begin{pmatrix} n \\ n_1 n_2 \cdots n_k \end{pmatrix}$ Luego:

$$(x_1 + x_2 + \cdots + x_k)^n = \sum_{\substack{n_1 n_2 \cdots n_k = 0 \\ n_1 + n_2 + \cdots + n_k = n}}^{n} \begin{pmatrix} n \\ n_1 n_2 \cdots n_k \end{pmatrix} x_1^{n_1} \cdot x_2^{n_2} \cdots x_k^{n_k}$$

Esta fórmula se debe Leibnitz (1646-1716) y se le suele llamar Fórmula de Leibnitz. Él fue uno de los más importantes matemáticos del siglo XVIII y publicó la mayoría de sus trabajos en una revista que él mismo editaba denominada *Acta Eruditorum*.

3.4 PRINCIPIO DE INCLUSIÓN-EXCLUSIÓN

3-4-1 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 podremos 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 (Fig. 22).

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

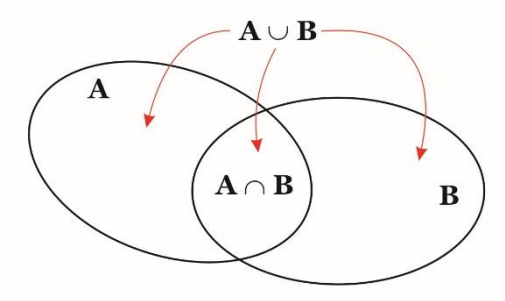


Fig. 22

Sean S un conjunto finito y P_1, P_2, ..., P_n propiedades que cada uno de los elementos de S puede o no satisfacer. Para cada i = 1,2, …, n, sea

S_i = { x ∈ S I x satisfice P_i}

Entonces

$$\bigcup_{i=1}^{n} S_i = \{x \in S |\ x \text{ satisface al menos una de las propiedades } P_i, i = 1,2,...n\}$$

$$\bigcap_{i=1}^{n} (S - S_i) = \bigcap_{i=1}^{n} S_i' = \{x \in S |\ x \text{ no satisface al menos una de las propiedades } P_i, i = 1,2,...n\}$$

donde Sí es el complementario de Si en S.

Teorema (Principio de Inclusión-Exclusión)

Con la notación anterior:

$$\left|\bigcap_{i=1}^{n} S_i'\right| = |S| - \sum_{i=1}^{n} |S_i| + \sum_{i=1}^{n} |S_{i_1} \cap S_{i_2}| - \sum |S_{i_1} \cap S_{i_2} \cap S_{i_3}| + \cdots + (-1)^k \sum |S_{i_1} \cap S_{i_2} \cap \cdots \cap S_{i_k}| + \cdots$$
$$+ (-1)^k \sum |S_{i_1} \cap S_{i_2} \cap \cdots \cap S_{i_k}| + \cdots + (-1)^k |S_1 \cap S_2 \cap \cdots \cap S_n|$$

donde para $2 \leq k \leq n$, las sumas $\sum \left| S_{i_1} \cap S_{i_2} \cap \cdots \cap S_{i_k} \right|$ se extienden a todas las combinaciones de orden k, $\{i_1, i_2, \ldots, i_k\}$, de {1, 2, …, n}.

Corolario

El número de elementos de S que satisfacen al menos una de las propiedades $P_1, P_2, \ldots, P_n$ es

$$\left| \bigcup_{i=1}^{n} S_i \right| = \sum_{i=1}^{n} |S_i| - \sum_{i=1}^{n} \left| S_{i_1} \cap S_{i_2} \right| + \sum \left| S_{i_1} \cap S_{i_2} \cap S_{i_3} \right| - \cdots$$
$$+ (-1)^{k-1} \sum \left| S_{i_1} \cap S_{i_2} \cap \cdots \cap S_{i_k} \right| + \cdots$$
$$+ (-1)^{n-1} \left| S_1 \cap S_2 \cap \cdots \cap S_n \right|$$

donde para $2 \leq k \leq n$, las sumas $\sum \left| S_{i_1} \cap S_{i_2} \cap \cdots \cap S_{i_k} \right|$ se extienden a todas las combinaciones de orden k, $\{i_1, i_2, \ldots, i_k\}$, de {1, 2, …, n}.

Ejemplo

En un teatro de Operan personas dejan sus abrigos en el guardarropa. Cuando acaba la representación vuelven a recogerlos; los abrigos han sido mezclados y se devuelven de forma aleatoria. ¿Cuál es el número de formas de llevar a cabo dicha devolución de modo que ninguna persona reciba su propio abrigo?

Solución:

Sea S el conjunto de todas las formas posibles de que las n personas reciban los n abrigos. Es evidente que |S| = n!. Vamos a designar por p_i , ..., p_r, a las n personas. Para cada i = 1, 2, …, n, sea P_i la propiedad de que p_i reciba su propio abrigo, y sea $S_i = \{x \in S |$ x satisface $P_i\}$, entonces

$$T = S'_1 \cap S'_2 \cap \ldots \cap S'_n = \{x \in S |\ x \text{ no satisface } P_i,\ i = 1, \ldots, n\}$$

Es decir, T es el conjunto de formas de devolver los abrigos sin acertar en la devolución de ninguno de ellos.

Sea k un entero, k = = 1, 2, …, n, y $\{i_1, i_2, \ldots, i_k\}$ una k-combinación de {1, 2, …, n}, para poder aplicar el Principio de Inclusión-Exclusión es necesario calcular

$$\left| S_{i_1} \cap S_{i_2} \cap \cdots \cap S_{i_k} \right|$$

Este cardinal es el número de formas de devolver los abrigos propios a $p_{i_1}, p_{i_2}, \cdots, p_{i_k}$. Como este número es igual al número de permutaciones que se pueden hacer con n - k abrigos se tiene que es (n - k)!, luego

$$|T| = |S| - \sum_{i=1}^{n} |S_i| + \cdots + (-1)^k \sum |S_i^1 \cap S_i^2 \cap \cdots \cap S_i^k| + \cdots + (-1)^n |S_{i_1} \cap S_{i_2} \cap \cdots \cap S_{i_k}| =$$

$$= n! - n \cdot (n-1)! + C(n,2) \cdot (n-2)! - C(n,3) \cdot (n-3)! + \cdots + (-1)^k C(n,k)(n-k)! + \cdots + (-1)^n 0! =$$

$$= n! \cdot \left(1 - 1 + \frac{1}{2!} - \frac{1}{3!} + \cdots + \frac{(-1)^k}{k!} + \cdots + \frac{(-1)^n}{n!} \right) = n! \sum_{j=0}^{n} \frac{(-1)^j}{j!}$$

3-4-2 Desordenaciones

En el ejemplo anterior el conjunto S era el conjunto de permutaciones de n objetos. Y por lo tanto el problema consistía en determinar el número de permutaciones de n objetos que no dejaban a ninguno fijo, es decir, para A = {1, 2, ..., n}, habrá que determinar el número de permutaciones σ: A $\rightarrow$ A tal que $\sigma(x) \neq x$, para todo x $\in$ A. Una permutación de este tipo se denomina una desordenación y se dice que los n elementos de A están desordenados. Si se denota el número de desordenaciones de n objetos por d(n), entonces el resultado del ejemplo anterior nos dice que

$$d(n) = n! \sum_{j=0}^{n} \frac{(-1)^j}{j!}$$

El problema de las desordenaciones de n elementos se puede reinterpretar en términos geométricos. Consideremos un tablero de ajedrez de n × n casillas. Se representa una permutación de {1, 2, …, n} colocando una pieza de ajedrez sobre la casilla intersección de la línea i y la columna j, si la permutación cambia el número i al j. Por ejemplo, la permutación σ: { 1, 2, 3, 4} $\rightarrow$ {3, 1, 4, 2} se puede representar de la forma (Fig. 23).

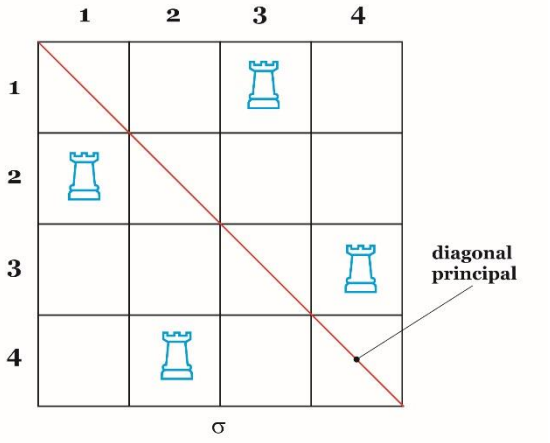


Fig. 23

Es decir, una permutación de n objetos es equivalente a colocar n piezas sobre un tablero de dimensiones n × n, de forma que no se encuentren dos piezas en la misma fila o columna. Para una desordenación evidentemente las piezas no pueden estar sobre la diagonal principal. Entonces d(n) se puede interpretar como el número de formas de colocar n torres, sobre un tablero de ajedrez de dimensiones n × n, de modo que ninguna se encuentre sobre la diagonal principal, y tal que ninguna torre pueda comer a otra (Fig. 23).

Esta interpretación del problema de las desordenaciones ha servido para resolver algunos tipos de problemas combinatorios, reduciéndolos a la colocación de torres, que no se comen unas a otras, sobre tableros de diferentes dimensiones y formas geométricas.

3.5 Recursividad y Relaciones Recurrentes

3-5-1 Concepto de recursión

Se dice que un objeto es recursivo si forma parte de sí mismo o está definido en función de sí mismo. La recursión aparece en la estructura de la naturaleza que da origen al carácter fractal de la misma, en Matemáticas y en la vida diaria, por ejemplo en los anuncios publicitarios que se contienen a sí mismos.

Las definiciones y las estructuras recursivas en Matemáticas son un medio poderoso de plantear y resolver problemas y de definir conjuntos. Por ejemplo: los números naturales, ciertas funciones como el factorial, las estructuras en árbol, etc.

Definición

Un conjunto de objetos está definido recursivamente siempre que

i) Se especifiquen de forma explícita algunos elementos del conjunto.
ii) Los demás elementos del conjunto se definan en términos de los elementos dados en i).

3-5-2 Funciones definidas recursivamente

En el caso particular de funciones matemáticas definidas de **N** de **R** se tiene la siguiente definición.

Definición

Una función f: $\mathbf{N} \rightarrow \mathbf{R}$ se dice que está definida recursivamente, si para algún $n_o \in \mathbf{N}$, se verifica

i) Los valores de f(1), f(2),..., f(n_o) son conocidos.
ii) Para $n > n_o$, f(n) está definida en términos de f(1), f(2),..., f(n-1).

Los f(1), f(2),..., f(n_o) se llaman valores o condiciones iniciales de f y nos referiremos a la ecuación que describe f(n) en términos de f(1), f(2),..., f(n-1) como una relación de recurrencia para f. Es decir, dada una sucesión de números

$$f(1), f(2),..., f(n),...,$$

cualquier ecuación que describa f(n) en términos de sus precedentes en la sucesión y que es válida para todos los enteros m mayores que algún entero fijo y positivo n_0, se denomina relación de recurrencia para f. A veces interesa buscar una relación de recurrencia donde el dominio de definición de la función sea $\mathbf{N} \cup \{0\}$, debiendo entonces extender la definición de recursividad a dicho conjunto ampliado.

La potencia de las definiciones y procesos recursivos, reside en la posibilidad de definir un número infinito de objetos mediante un enunciado finito. Del mismo modo, se puede

describir un número infinito de operaciones de cálculo mediante un proceso recursivo finito.

Evidentemente la utilidad de estos métodos está limitada a aquellos tipos de problemas que presentan en su estructura cierto aspecto recursivo.

3-5-3 Relaciones de recurrencia lineales con coeficientes constantes

Definición

Una relación de recurrencia de la forma

$$r(n) = a_1 \cdot r \cdot (n - 1) + a_2 \cdot r \cdot (n - 2) + \ldots + a_t \cdot r \cdot (n - t) + k(n),$$

donde $n \geq t + 1$ y $a_1, a_2, \ldots, a_t$ 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

$$(n - t) \cdot r \cdot (n - s), \quad 1 \leq s \leq t \text{ ó } [r \cdot (n - s)]^5.$$

Un ejemplo de relación de recurrencia que satisface la definición anterior es

$$r(n) = 6 \cdot r \cdot (n - 1) + 8 \cdot r \cdot (n - 2) - 4 \cdot r \cdot (n - 3) + 3 \cdot r \cdot (n - 4) + n^3.$$

Para $n \geq 5$ es lineal con coeficientes constantes.

3-5-4 La sucesión de Fibonacci

Definición

Se denomina sucesión de Fibonacci a la sucesión obtenida a partir de la relación de recurrencia:

$$fib(n) = fib(n - 1) + fib(n - 2) \text{ para } n \geq 3,$$

con condiciones iniciales fib (1) = 1, fib (2) = 2.

• El nombre de sucesión de Fibonacci se debe al matemático francés Edouard Locus (1842-91) al estar asociada a un famoso problema "el problema de los conejos" que está contenido en el *Liber Abaci* (1202) escrito en la edad media por el matemático Leonardo de Pisa (1175-1230) conocido por el sobrenombre de Fibonacci. Este problema se puede enunciar así: ¿Cuántas parejas de conejos habrá al cabo de un año a partir de una primera pareja, si cada pareja origina una nueva cada mes, tal pareja se vuelve fértil a partir del segundo mes y además no ocurren muertes?

La sucesión de Fibonacci está definida mediante una relación recurrente lineal y homogénea con coeficientes constantes.

En general, una relación de recurrencia tiene más de una solución, pero las condiciones iniciales especifican cuál de las soluciones es la que resuelve el problema.

Una relación de recurrencia de la forma:

$$F(n) = F(n - 1) + F(n - 2) \text{ para } n \geq 3$$

Se denominará una relación de recurrencia de tipo Fibonacci. Obsérvese que en este caso no se fijan las condiciones iniciales. Para F(1) y F(2).

3-5-5 Ecuación característica asociada a una relación de recurrencia lineal homogénea

Definición

Sea $r(n) = a_1 \cdot r \cdot (n -1) + a_2 \cdot r \cdot (n - 2) + \ldots + a_t \cdot r \cdot (n - t) = 0$, 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:

$$x^t - a_1 x^{t-1} - a_2 x^{t-2} - \ldots - a_{t-1} x - a_t = 0.$$

A continuación, describiremos algunos métodos para resolver algunos tipos especiales de relaciones de recurrencia.

Teorema

Sea Sea $r(n) = a_1 \cdot r \cdot (n -1) + a_2 \cdot r \cdot (n - 2) + \ldots + a_t \cdot r \cdot (n - t) = 0$, con $n > t+1$, una relación de recurrencia lineal y homogénea de coeficientes constantes. Entonces $r(n) = b^n$ es una solución si y sólo si b es una raíz de la ecuación característica.

Si la ecuación $x^t - a_1 x^{t-1} - a_2 x^{t-2} - \ldots - a_{t-1} x - a_t = 0$, tiene t raíces no nulas y distintas b_1, b_2, ..., b_t, entonces

$$r(n) = c_1 b_1^n + c_2 b_2^n + \ldots + c_t b_t^n,$$

es una solución de la ecuación de recurrencia (donde las constantes c_i son arbitrarias) llamada solución general.

Si se dan t condiciones iniciales $r(i) = d_i$, i = 1, …, t, entonces se puede obtener una solución particular de la ecuación, puesto que estas condiciones determinan un sistema de ecuaciones lineales en las incógnitas c_i:

$$\begin{cases} \mathbf{c_1 \cdot b_1 + c_2 \cdot b_2 + \cdots + c_t \cdot b_t = d_1} \\ \mathbf{c_1 \cdot b_1^2 + c_2 \cdot b_2^2 + \cdots + c_t \cdot b_t^2 = d_2} \\ \cdots \\ \mathbf{c_1 \cdot b_1^t + c_2 \cdot b_2^t + \cdots + c_t \cdot b_t^t = d_t} \end{cases}$$

y puesto que las b_i son distintas y no nulas, el sistema tiene una solución única, (esto es una consecuencia de que el determinante de la matriz de los coeficientes es distinto de cero: es el producto del número no nulo $b_1 \cdot b_2 \cdots b_t$ por un determinante de Vandermonde). Obtenemos por tanto una solución particular para r(n). En el caso de raíces múltiples o raíces complejas el proceso de obtener soluciones generales se complica mucho, y no lo veremos

Teorema

La función fib(n), solución de la relación de recurrencia de Fibonacci:

$$\text{fib}(n) = \text{fib}(n-1) + \text{fib}(n-2), \text{ para } n \geq 3, \text{fib}(1) = 1, \text{fib}(2) = 2,$$

viene dada por

$$\mathbf{fib(n)} = \frac{1}{\sqrt{5}} \cdot \left(\frac{1+\sqrt{5}}{2} \right)^{n+1} - \frac{1}{\sqrt{5}} \cdot \left(\frac{1-\sqrt{5}}{2} \right)^{n+1} \qquad \mathbf{n \geq 1}$$

La fórmula que expresa fib(n) se llama formula de Binet, debido a que fue obtenida por el matemático francés J. P. M. Binet (1786-1856). Esta fórmula también fue deducida independientemente por Moivre (1667-1754) y D. Bernoulli (1700-1782).

El número irracional $\frac{1+\sqrt{5}}{2}$ llamado razón aúrea es quizá el número irracional más famoso después del número π. Aparece en la construcción del pentágono regular dada por Euclides y ya en 1509 se escribió un libro dedicado únicamente a él. Además de aparecer como hemos visto en el estudio de la sucesión de Fibonacci, surge en la llamada espiral aúrea o de Arquímedes y en el fenómeno botánico llamado filotaxia (literalmente *disposición de hojas*), entre otras muchas aplicaciones.

Aplicando el Teorema del Binomio a la ecuación anterior se tiene

$$\mathbf{fib(n)} = \frac{1}{\sqrt{5}} \cdot \left(\frac{1}{2^{n+1}} \right) \cdot \left[\sum_{r=0}^{n+1} \binom{n+1}{r} \cdot 5^{r/2} - \sum_{r=0}^{n+1} \binom{n+1}{r} \cdot (-1)^r \cdot 5^{r/2} \right] =$$

$$= \frac{1}{\sqrt{5}} \cdot \frac{1}{2^n} \cdot \left[\binom{n+1}{1} \cdot 5^{1/2} + \binom{n+1}{3} \cdot 5^{3/2} + \binom{n+1}{5} \cdot 5^{5/2} + \cdots \right] =$$

$$= \frac{1}{2^n} \cdot \left[\binom{n+1}{1} + 5 \cdot \binom{n+1}{3} + 5^2 \cdot \binom{n+1}{5} + \cdots \right]$$

y debido a que fib(n) tiene que ser un número entero, se obtiene el resultado, nada obvio, que 2^n divide a la suma de los términos que se encuentran dentro del corchete.

Puesto que $\mathbf{0} < \left[\frac{\mathbf{1}}{\mathbf{2}} \cdot \left(\sqrt{\mathbf{5}} - \mathbf{1}\right)\right] < \mathbf{1}$, se tiene que $\left(\frac{\mathbf{1}+\sqrt{\mathbf{5}}}{\mathbf{2}}\right)^{\mathbf{n+1}} \rightarrow \mathbf{0}$, cuando n tiende a infinito. Por tanto

$$\mathbf{fib(n)} = \frac{\mathbf{1}}{\sqrt{\mathbf{5}}} \cdot \left(\frac{\mathbf{1}+\sqrt{\mathbf{5}}}{\mathbf{2}}\right)^{\mathbf{n+1}}$$

para n suficientemente grande.

GLOSARIO DE TÉRMINOS

A

Algoritmo de Dijkstra Este algoritmo calcula la distancia entre dos vértices *x* e *y* de un grafo dirigido, cuyas aristas están etiquetadas por números positivos (distancias).

Algoritmo de Euclides Algoritmo para el cálculo del máximo común divisor de dos números *a* y *b.*

Algoritmo de Factorización de Fermat Este algoritmo se basa en el siguiente resultado: si *n* es un número natural impar y compuesto, entonces *n=a.b* donde *a* y *b* son impares tales que $1<b\leq a$. De modo que, podemos escribir:

$$\left(\frac{\mathbf{a+b}}{\mathbf{2}}\right)^{\mathbf{2}} - \left(\frac{\mathbf{a-b}}{\mathbf{2}}\right)^{\mathbf{2}} = \mathbf{n}$$

El Algoritmo de factorización de Fermat relaciona el estudio de si un número impar *n* es compuesto, con la resolución de la ecuación diofántica $x^2 - y^2 = n$.

Algoritmo de la División Sean $a \in \mathbf{Z}$ y $b \in \mathbf{N}$. Entonces existen números enteros *q* y *r* tales que $b=a.q+r$, con $0 \leq r< b$. Además, *q* y *r* son únicos. A los números *a*, *b*, *q* y *r* se les suele llamar *dividendo*, *divisor*, *cociente* y *resto*.

Árbol Grafo conexo y sin ciclos.

Arista Par de vértices (u,v), de un grafo. Los vértices *u* y *v* se llaman extremos de la arista. *u* es el origen de la arista, y *v* el fin.

B

Base Se dice que un número natural *n* está escrito en base *b*, cuando está expresado como una combinación (única) de potencias de *b*:

$$n = a_k b^k + a_{k-1} b^{k-1} + \ldots + a_1 b + a_0,$$

para algún $k \geq 0$, con $0 \leq a_i < b$, y con $a_k \neq 0$. Entonces, el número *n* escrito en base *b* es: $a_k\, a_{k-1} \ldots a_0$.

C

Camino Un camino en un grafo G es una sucesión (finita) v_0, v_0v_1, v_1, v_1v_2, v_2, ..., v_{n-1}, v_{n-1} v_n, v_n, en la que aparecen alternadamente vértices y aristas de G, tal que cada arista tiene por extremos los vértices adyacentes de la sucesión. A los vértices v_0 y v_n se les llama *extremos* del camino.

Camino cerrado Un camino es cerrado si sus extremos coinciden.

Camino Euleriano Camino que contiene todas las aristas del grafo, apareciendo cada una de ellas exactamente una vez.

Camino Hamiltoniano Camino simple en un grafo *G*, que contiene todos los vértices de *G*.

Camino simple Un camino se dice que es *simple* si en la sucesión de vértices no hay ninguno repetido.

Ciclo Camino cerrado donde los únicos vértices repetidos son el primero y el último.

Ciclo Hamiltoniano Un ciclo que a su vez es un camino Hamiltoniano.

Circuito Camino cerrado que no repite aristas.

Circuito Euleriano circuito que contiene todas las aristas del grafo.

Cociente Véase Algoritmo de la División.

Coeficientes binomiales Se denominan *coeficientes binomiales* a los coeficientes del desarrollo del binomio $(x+y)^n$. Estos coeficientes son los números combinatorios:

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

Coeficientes multinómicos Son los coeficientes del desarrollo de la expresión polinómica $(x_1 + x_2 + \ldots + x_k)^n$. Tienen la forma

$$\binom{n}{n_1 n_2 \cdots n_k} = \frac{n!}{n_1!\, n_2!\, \cdots\, n_k!}$$

Coloración de un grafo Colorear un grafo consiste en asignar colores a sus vértices de modo que dos vértices unidos por una arista tengan distinto color.

Combinaciones Si *A* es un conjunto finito de cardinal $n > 0$, y *r* es un número natural $r \leq n$, una *combinación de orden r* de *A* es una lista $(a_1, a_2, \ldots, a_r)$ de *r* elementos distintos de A.

Combinaciones con repetición Si *A* es un conjunto finito de cardinal $n > 0$, y *r* es un número natural $r \leq n$, una *combinación con repetición de orden r* de *A* es una lista $(a_1, a_2, \ldots, a_r)$ de *r* elementos (no necesariamente distintos) de A.

Componente conexa Las clases de equivalencia que define la relación "estar conectado con", en un grafo G, se denominan *componentes conexas* de G. Si un grafo es conexo, posee una única componente conexa que es el propio grafo.

Condiciones iniciales Véase función recursiva.

Congruencia Dos números enteros *a* y *b* se dice que son **congruentes** módulo un entero $m > 0$, y se escribe

$$a \equiv b \ mod(m),$$

si $a-b$ es divisible por *m*. Esta definición es equivalente a decir que los restos de la división de *a* por *m,* y de *b* por *m* son iguales. $a \equiv b \ mod(m)$ es equivalente a $(a-b)$**MOD***m*=0, véase el operador módulo.

Criba de Eratóstenes Método para la obtención de números primos basado en el resultado siguiente: *Si todo número primo* $p \leq raiz(a)$, *no es divisor del número* $a \geq 1$, *entonces a es primo.*

D

Desordenaciones Una *desordenación* de *n* objetos es una permutación en la que ningún objeto queda fijo.

Digrafo Grafo cuyas aristas están dirigidas, desde un vértice llamado *origen* a otro vértice llamado *fin.*

Distancia La distancia entre dos vértices de un grafo etiquetado es la longitud del camino más corto que los une.

Dividendo Véase Algoritmo de la División.

Divisor Si $a \neq 0$ *y* $b = a \cdot q$ diremos de forma equivalente que *a* **divide** a *b, a* es un **divisor** o un **factor** de *b,* o que *b* es un **múltiplo** de *a.*

E

Ecuación característica Se llama *ecuación característica* asociada a una relación de recurrencia lineal homogénea de la forma $r(n) = a_1 \cdot r \cdot (n-1) + a_2 \cdot r \cdot (n-2) + \ldots + a_t \cdot r \cdot (n-t) = 0$ con $n > t$, a la ecuación

$$x^t - a_1 x^{t-1} - a_2 x^{t-2} - \ldots - a_{t-1} x - a_t = 0.$$

Ecuación Diofántica Se usa el nombre de **ecuaciones diofánticas** para designar una amplia clase de ecuaciones algebraicas, con más de una indeterminada, de las que se pretende obtener sus soluciones en **Z** (enteros) o **Q** (racionales).

Ecuación lineal Dentro de las ecuaciones diofánticas estudiaremos las *ecuaciones lineales* en dos variables en **Z**:

$ax + by = n$, $a, b, n \in \mathbf{Z}$.

Esta ecuación tiene soluciones enteras x e y si y sólo si d = m.c.d. (a,b) divide a n.

Ecuación pitagórica Ecuación diofántica de la forma $x^2 + y^2 = z^2$ con $x, y, z \in \mathbf{N}$. La terna (x, y, z) se denomina *terna Pitagórica*

F

Fórmula de Leibniz Se denomina *Fórmula de Leibniz* al desarrollo de la expresión algebraica $(x_1 + x_2 + ... + x_k)^n$ Los coeficientes de dicho desarrollo se llaman *coeficientes multinómicos.*

$$(\mathbf{x_1 + x_2 + \cdots + x_k})^{\mathbf{n}} = \sum_{\substack{\mathbf{n_1 n_2 \cdots n_k = 0} \\ \mathbf{n_1 + n_2 + \cdots + n_k = n}}} \binom{\mathbf{n}}{\mathbf{n_1 n_2 \cdots n_k}} \mathbf{x_1^{n_1} \cdot x_2^{n_2} \cdots x_k^{n_k}}$$

Fórmula de Pascal La *Fórmula de Pascal* expresa la siguiente propiedad algebraica de los números combinatorios

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

Factor Véase divisor.

Factorial Se denomina *factorial* de un número natural n, y se denota por $n!$, al número $n! = n \cdot (n\text{-}1) \cdot (n\text{-}2) \cdots 2 \cdot 1$. Por convenio $0! = 1$.

Función de Euler La *función* ϕ *de Euler* está definida en el conjunto de los números naturales. Dado $m \in \mathbf{N}$, $\phi(m)$ es el número de enteros positivos menores o iguales que m, que son primos con m.

Función recursiva Una función f: $\mathbf{N} \rightarrow \mathbf{R}$ se dice que está definida *recursivamente*, si para algún $n_0 \in \mathbf{N}$ se verifica:

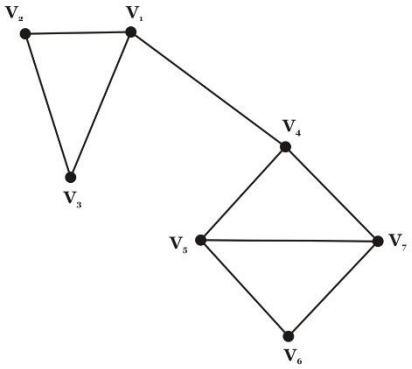
> (i) Los valores $f(1), f(2), ..., f(n_0)$ son conocidos.
> (ii) Para $n > n_0$, $f(n)$ está definida en términos de $f(1), f(2), ..., f(n\text{-}1)$. Los valores $f(1), f(2), ..., f(n0)$ se llaman *valores o condiciones iniciales* de f. La ecuación que describe $f(n)$ en términos de $f(1), f(2), ..., f(n\text{-}1)$ es una *relación de recurrencia* para f.

G

Grado de un vértice Número de aristas que tienen dicho vértice como extremo.

Grado de una región Longitud del camino que la bordea.

Grafo Un *grafo* puede ser considerado como un diagrama o un dibujo en que aparecen una serie de puntos (*vértices*) conectados entre sí por segmentos (aristas)

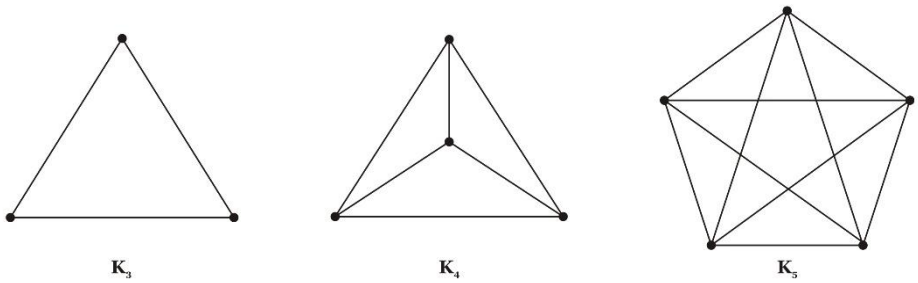


Formalmente, un grafo es un par $G = (V, E)$ donde V es un conjunto de vértices y E es un conjunto de pares no ordenados de elementos de V, llamados aristas.

Grafo *k*-regular Grafo en el que todos los vértices tienen grado k. Ejemplo: el grafo completo K_n es $(n\text{-}1)$-regular.

Grafo bipartito Grafo que puede ser coloreado con **dos** colores.

Grafo completo Grafo en el que cada par de vértices están conectados por una arista. Se denota por K_n al grafo completo de n vértices. En las siguientes figuras se muestran los grafos K_3, K_4 y K_5.



Grafo conexo Grafo en el que para todo par de vértices existe un camino que los conecta.

Grafo desconexo Grafo en el que existen vértices que no pueden conectarse mediante ningún camino.

Grafo etiquetado Grafo cuyas aristas están marcadas con una etiqueta. La etiqueta suele representar la distancia o el coste en recorrer la arista asociada.

Grafo Euleriano Grafo que posee un circuito Euleriano: circuito que contiene todas las aristas sin repeticiones.

Grafo finito Grafo con un número finito de vértices.

Grafo Hamiltoniano Grafo que posee un circuito Hamiltoniano: circuito que contiene todos los vértices sin repeticiones.

Grafo plano Grafo que admite una representación gráfica en el plano, de modo que las aristas no se corten, salvo en los vértices.

Grafo regular Grafo en el que todos sus vértices tienen el mismo grado. Véase grafo *k*-regular.

Grafos isomorfos Sean G = (V, E) y G' = (E',V') dos grafos y sea f:V→V' una biyección entre los conjuntos de vértices, tal que $uv \in E$ si y sólo si $f(u)f(u) \in V'$. La biyección f se denomina *isomorfismo* de G a G'. Se dice entonces que los grafos G y G' son *isomorfos.*

Grupo simétrico El conjunto de todas las permutaciones de un conjunto *A,* con la operación producto, tiene estructura de grupo y se denomina *grupo simétrico* de *A.*

I

Isomorfismo de grafos Véase grafos isomorfos.

L

Lazo Arista cuyos extremos coinciden.

Lema de Euclides Sean *a, b* y *c* números enteros. Supongamos que *a* y *c* son primos entre sí y que $c|ab$. Entonces $c|b$.

M

Máximo común divisor El *máximo común divisor* de dos números *a* y *b* es, como su nombre indica, un número $d \neq 0$ que divide a *a* y a *b,* y es el mayor de los que cumplen esa condición. De forma que, dado cualquier otro divisor común, *d',* de *a* y de *b,* se cumple que *d'* es un divisor de *d.* Se denota por *d = m.c.d.(a,b).*

Mínimo común múltiplo El *mínimo común múltiplo* de dos números *a* y *b* es el menor entero positivo múltiplo de *a* y *b.* Se denota por *m.c.m.*(*a,b*).

Módulo Sean *a* y *b* números enteros con $b \neq 0$, tales que $a = bq + r$, donde $0 \leq r < |b|$. Se define el operador *módulo "**MOD**"* por *a***MOD***b=r.* Obsérvese que *r* es el menor residuo no negativo de *a* módulo *b.*

Múltiplo Véase divisor.

Mapa Representación gráfica en el plano de un grafo (o multigrafo) plano.

Matriz de Adyacencia Dado un grafo $G=(V, E)$ con p vértices $V=\{v1 , v2 ,...., vp\}$ se denomina **Matriz de Adyacencia** de G, a la matriz $\mathbf{M}=(m_{i,j})$ de orden p x p cuyas entradas son ceros y unos de acuerdo a la siguiente ley:

$m_{i,j} = 1$ si existe una arista de v_i *a* v_j
$m_{i,j} = 0$ si no existe una arista de v_i *a* v_j.

Menor residuo no negativo El *menor residuo no negativo de a módulo m* es el único número r tal que $0 \leq r < m$ y $a = qm + r$.

Multigrafo Grafo en el que un par de vértices distintos pueden estar conectados por más de una arista.

N

Números combinatorios Son números de la forma

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

Véase *coeficientes binómicos*.

Números compuestos Números no primos.

Números primos Todo número $p > 1$ es divisible por 1 y por p. Si éstos son los únicos divisores positivos de p, diremos entonces que p es **primo**.

Números primos entre sí Dos números enteros a y b son **primos entre sí**, cuando no tienen divisores comunes, excepto el 1, o lo que es lo mismo m.c.d.$(a,b) = 1$.

P

Permutaciones Sea A un conjunto finito no vacío. Una *permutación* de A es una biyección, $\sigma: A \rightarrow A$. De forma equivalente se puede definir una permutación de A, como una ordenación de los elementos de A.

Permutaciones circulares Una permutación circular de n objetos, de orden r, $r \leq n$ es una colocación ordenada de r de los n objetos en r posiciones igualmente espaciadas sobre una circunferencia. Dos permutaciones circulares son iguales, si una puede ser obtenida de la otra, mediante una rotación apropiada de la circunferencia alrededor de su centro. El número de estas permutaciones es $C(n,r).(r-1)!$.

Principio de Adición Sean $A_1, A_2, ..., A_n$ *conjuntos* finitos y disjuntos dos a dos, entonces

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

Principio de Distribución Supongamos que se desean introducir m objetos en n cajas siendo $m > n$. Entonces, intuitivamente vemos que al menos en una caja tendremos que

introducir dos objetos. La generalización de este resultado es el *Principio de Distribución* cuyo enunciado es el siguiente: 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. Este principio también se conoce con los nombres de *Principio del cajón de Dirichlet*, *Principio de los casilleros,* o en la literatura inglesa *The pigeonhole principle.*

Principio de Inducción Sea *S* un conjunto de números naturales que satisface las siguientes condiciones:

1) El número $1 \in S$.
2) Para cada número natural $k > 0$, si $k \in S$ entonces $k+1 \in S$.

Entonces el conjunto *S* es igual a **N**.

Principio de la Buena Ordenación *"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. Este primer elemento, *m*, puede sustituir al "1" en el Principio de Inducción, para demostrar que una propiedad *P(n)* se cumple para todo natural $n \geq m$.

Principio de Multiplicación Sean $A_1, A_2, ..., A_n$ conjuntos finitos no vacíos, entonces

$$|A_1 \times A_2 \times ... \times A_n| = |A_1| \cdot |A_2| \cdot ... \cdot |A_n|.$$

Principio Fuerte de Inducción Sea *S* un conjunto de números naturales que satisface las siguientes condiciones:

1) El número $1 \in S$.
2) Para cada número natural $n > 1$, si $k \in S$ para todo natural $1 \leq k < n$, entonces $n \in S$.

Entonces $S = \mathbf{N}$.

Pseudografo grafo que contiene lazos.

Pseudomultigrafo dual Dado un mapa **M** (que representa a un grafo G), podemos asociarle un grafo que se construye del siguiente modo: se asocia un vértice a cada región del mapa, y por cada arista *e* del mapa, que separa dos regiones, se considera una arista *e** que una los vértices asociados a dichas regiones. Este grafo se denota por $\mathbf{G_M}$ y se llama **pseudomultigrafo dual** de **M**.

R

Recursivo Véase función recursiva.

Región cada una de las partes en que un mapa divide al plano.

Regiones adyacentes regiones con una arista en común.

Relación de recurrencia Véase función recursiva.

Relación de recurrencia lineal Relación de la forma

$$r(n)= a_1 r(n\text{-}1) + a_2 r(n\text{-}2) + ... + a_t r(n\text{-}t) + k(n)$$

con $n \geq t+1$ y $a_1, a_2, ..., a_t$ constantes.

Relación de recurrencia lineal homogénea Relación de la forma

$$r(n)=a_1 r(n\text{-}1) + a_2 r(n\text{-}2) + ... + a_t r(n\text{-}t)$$

con $n \geq t+1$ y $a_1, a_2, ..., a_t$ constantes.

Residuos El conjunto de enteros {0, 1, 2, ..., *m*-1} se denomina *conjunto (o sistema) completo de residuos* módulo *m.* Cualquier número entero es congruente, módulo *m*, con algún elemento del conjunto completo de residuos. Véase *menor residuo no negativo.*

Resto Véase Algoritmo de la división.

S

Sistemas de Numeración Un número natural *n* representado en un *sistema de numeración* de *base b* ≥ 2, tiene la siguiente expresión $n=a_k\, a_{k-1} ... a_0$ donde

$$n = a_k b^k + a_{k-1} b^{k-1} + ... + a_1 b + a_0,$$

para algún $k \geq 0$, con $0 \leq a_i < b$, y con $a_k \neq 0$.

Subdivisión elemental de un grafo Sea G = (V, E) un grafo $u,v \in V$ y $uv \in E$. Una subdivisión elemental de G es un grafo G'=(V ∪ {*w*}, E-{*uv*} ∪ {*uw, wv*}), donde $w \notin V$. Es decir, se suprime en G la arista *uv*, y se incluye un nuevo vértice *w* y dos aristas *uw* y *wv.* Una *subdivisión* de un grafo G es el grafo obtenido efectuando un número finito de subdivisiones elementales.

Subgrafo Un subgrafo de un grafo G se obtiene eliminando algunas aristas y vértices de G, de modo que, si suprimimos un vértice, hemos de borrar todas las aristas que tienen tal vértice como extremo.

Sucesión de Fibonacci Sucesión obtenida a partir de la relación de recurrencia:

$$fib(n) = fib(n\text{-}1) + fib(n\text{-}2), \text{ para } n \geq 3,$$

con condiciones iniciales fib(1) = 1, fib(2) = 2.

T

Teorema Chino del Resto El sistema de congruencias $a_i x \equiv b_i \bmod(m_i)$ $i = 1, 2, ..., k$, donde m.c.d.$(m_i, m_j)=1$ si $i \neq j$ y m.c.d.$(a_i, m_i) = 1$ para $1 \leq i \leq k$, tiene un única solución $x_0$módulo $m_1 m_2....m_k$ y las demás soluciones son de la forma $x = x_0 + \lambda m_1 m_2....m_k$, $\lambda \in$ **Z.**

Teorema de Euler Sean a y m números enteros $m \geq 1$; entonces si $m.c.d.(a,m) = 1$ se tiene que $a^{\phi(m)} \equiv 1 \bmod(m)$. Donde ϕ(m) es la función ϕ de Euler, que cuenta el número de enteros positivos que no exceden a m y son primos con m.

Teorema de Fermat (Último Teorema de Fermat) Dado un número natural $n \geq 3$, la ecuación $x^n + y^n = z^n$ no tiene soluciones naturales.

Teorema de Fermat (Pequeño Teorema de Fermat) Si p es un número primo que no divide al número a entonces: $a^{p-1} \equiv 1 \bmod(p)$. Este teorema resulta muy útil para calcular el resto de una división cuando el dividendo es muy grande.

Teorema de Wilson Si p es un número primo, entonces $(p-1)! \equiv -1 \bmod (p)$.

Teorema del Binomio Para cada número natural n y para cada par de números reales x e y, se tiene que

$$(\mathbf{x+y})^{\mathbf{n}} = \sum_{\mathbf{k=0}}^{\mathbf{n}} \binom{\mathbf{n}}{\mathbf{k}} \cdot \mathbf{x}^{\mathbf{n-k}} \cdot \mathbf{y}^{\mathbf{k}}$$

Teorema Fundamental de la Aritmética Todo número entero $n > 1$ se puede descomponer como producto de números primos $n=p_1 p_2 \ldots p_r$, donde $p_1 \leq p_2 \leq ... \leq p_r$. Además, esta factorización es única.

V

Vértices adyacentes En un grafo G=(V, E) los vértices u, v ∈ V son *adyacentes* si uv ∈ E, es decir si existe en G la arista uv.

Valor absoluto Se llama *valor absoluto* a la aplicación $|\ |: \mathbf{Z} \rightarrow \mathbf{Z}$ definida por: $|n|=n$ si $n \geq 0$ ó $|n|=-n$ si $n < 0$.

Variaciones Si A es un conjunto finito de cardinal $n>0$, y r es un número natural $r \leq n$, una *variación de orden r* de A es una lista ordenada $(a_1, a_2..., a_r)$ de r elementos distintos de A.

Variaciones con repetición Si A es un conjunto finito de cardinal $n > 0$, y r es un número natural $r \leq n$, una *variación con repetición de orden r* de A es una lista ordenada $(a_1, a_2..., a_r)$ de r elementos (no necesariamente distintos) de A.

BIBLIOGRAFÍA

Textos base

Bujalance García, Emilio; Bujalance García, José; Costa, Antonio F.; Martínez, Ernesto: *Elementos de Matemática Discreta*. Editorial Sanz y Torres, 1993.

Bujalance García, Emilio; Bujalance García, José; Costa, Antonio F.; Martínez, Ernesto: *Problemas de Matemática Discreta*. Editorial Sanz y Torres, 1993.

Textos complementarios

Anderson, Ian: *Introducción a la Combinatoria*. Vicens Vives, 1993.

Se recomienda la lectura de los capítulos 1, 2, 4 y 5.

Bogart, Kenneth P.: *Introductory Combinatorics*. A Harcourt Science and Technology Company, 3ª Edición, 2000.

Se recomienda la lectura de los capítulos 1, 3 y 4.

García Merayo, Félix: *Matemática Discreta*. Editorial Paraninfo, 2001.

En este texto de exposición sencilla se recomienda la lectura del Capítulo 1 en el que se desarrollan los contenidos de Teoría de Números. En los capítulos 7 y 9 encontrará todos los contenidos de la Teoría de grafos que se desarrollan en el texto base. El capítulo 8 está dedicado a los árboles. En los capítulos 5 y 6 encontrará todos los contenidos de Combinatoria que se desarrollan en el texto base.

Grimaldi, Ralph P.: *Matemáticas Discreta y Combinatoria*. Addison Wesley Iberoameticana, 3ª Edición, 1997.

Los conceptos sobre Teoría de grafos se desarrollan en el Tema 11. Se recomienda la lectura del Tema 12 (Árboles) y el Tema 13 (Optimización y emparejamiento), aunque sus contenidos no formen parte de la materia objeto de examen. Este texto contiene muchos ejemplos y ejercicios propuestos, así como numerosas aplicaciones que conducen a procesos iterativos y a la obtención de algoritmos.

Jones G.A. y Jones, J. M.: *Elementary Number Theory*. Springer Undergraduate Mathematics Series. Springer-Verlag, 1998.

Se recomienda la lectura de los capítulos 1, 2, 3, 4, 5 y 11.

Meavilla Seguí, Vicente: *201 Problemas resueltos de Matemática Discreta*. Prensas Universitarias de Zaragoza, 2000.

Rosen, Kenneth H.: *Discrete Mathematics and its Applications* (4a edición). McGraw-Hill International Editions. Mathematics Series, 1999.

En el capítulo 7 encontrará todos los contenidos de la Teoría de grafos que se desarrollan en el texto base. El capítulo 8 está dedicado a los árboles. En los capítulos 4 y 5 se desarrollan los conceptos de Combinatoria que contiene el programa de la asignatura.

Rosen, Kenneth H.: *Elementary Number Theory and its Applications* (3a edición). Addison-Wesley Publishing Company, 1992.