Matemática Discreta – Información

Cota inferior (definición): Cota significa estar limitado. Un número n es una cota inferior de una sucesión si es menor o igual que todos los términos de la sucesión; a su vez, todos los números<=n serán también cotas inferiores incluido n.

- A = {2,5}, el 2 (y todos los números menores a 2) son cotas inferiores del subconjunto A.
- B = {-infinito, -2}, no tiene cotas inferiores, solo infinitas cotas superiores en los enteros (el -2 incluido).

Mínimo (definición): A diferencia de la cota, es UNICO. Es el mayor número de las cotas inferiores

- A = {2,5} el 2 es la mayor cota inferior y **pertenece a A** entonces es el mínimo del conj. A
- B = {-infinito, -2}, como no existe cota inferior, no hay mínimo en ese conjunto

Axioma de buena ordenación: (5.7.2 de Algebra)

- **ENUNCIADO.** Si X es un subconjunto de Z que no es vacío y tiene cota inferior, entonces X tiene un mínimo.
- **EXPLICACIÓN.** Si tratamos con conjuntos que no son enteros (fracciones, por ejemplo) el conjunto tendrá cota inferior pero no mínimo, ya que si mi cota inferior es 1, puedo elegir infinitamente números cercanos a 1 y no acabaría nunca.

Enunciado del principio de inducción: Sea P(n) una función proposicional, con npN tal que:

I. P(1) es verdadera, (caso base n=1) y,
II. Asumiendo que P(k) (hipótesis inductiva) es verdadera para k N arbitrario se deduce que P(k + 1) es verdadera,

Entonces P(n) es verdadera para todo n N.

*Demostración en la pág. 132 de Álgebra…

Enunciado del principio de inducción completa: Sea n0 un entero y P(n) una propiedad para n>=n0 tal que:

I. P(n0) es verdadera (base inductiva)
II. Asumiendo que P(1), P(2),…, P(k) (hipótesis) son verdaderas para un k Natural arbitrario se deduce que P(k +1) es verdadera.

Entonces P(n) es verdadera para todo n Natural.

*Ejemplo en pág. 140 de Álgebra, demostración (ejemplo) pág. Notas…

DEFINICIONES RECURSIVAS

- **N factorial (n!): n! = n . (n - 1) . (n – 2) … 3 . 2 . 1**
  Formalmente la definición recursiva de n! es
  $1! = 1$ y $(n + 1)! = (n + 1)n!$ Para todo n>=2.
  *0! = 1
- **Productoria:**
  $$\prod_{i=1}^{1} x_i = x_1 \qquad \text{y} \qquad \prod_{i=1}^{n} x_i = \left(\prod_{i=1}^{n-1} x_i\right) \cdot x_n, \quad \forall n \geq 2$$
- **Sumatoria:**

$$\sum_{i=1}^{1} x_i = x_1 \qquad \text{y} \qquad \sum_{i=1}^{n} x_i = \left(\sum_{i=1}^{n-1} x_i\right) + x_n, \quad \forall n \geq 2$$

- **X^n y sus propiedades:** Dado un x en los Reales, para todo n en los Naturales se define la potencia n-ésima de x, denotada x^n, recursivamente por:

  x^1 = x y x^n+1 = x^n . x para n>=2

  Propiedades de la potencia. Para todo x, y en los Reales y m, n en los Naturales valen

  x^m+n = x^m . x^n

  x^mn = (x^m)^n = (x^n)^m

  (xy)^n = x^n . y^n

Cantidad de subconjuntos de un conjunto de n elementos: (Proposición 2.2.2) La cantidad de subconjuntos de un conjunto de n elementos es 2^n. Dado X un conjunto, denotamos P(X) el conjunto formado por todos los subconjuntos de X, por ejemplo

P({1,2}) = {Vacío, {1}, {2}, {1, 2}}

Si X es un conjunto finito, se cumple que |P(X)| = 2^|X|

Definición de número combinatorio. Definimos el número (n k) (número combinatorio) como la cantidad de subconjuntos de k elementos que tiene un conjunto de n elementos (o equivalentemente la cantidad de formas de elegir k elementos de un conjunto de n elementos). O sea,

(n k) = #{AC=X : |A| = k, |X| = n} = #{AC=Isubn : |n| = k}

El número (n k) se llama *número combinatorio n en k* para 0<=k<=n y se lee simplemente “n en k”. Si k<0 o k>n definimos (n k) = 0.

Dado n en los Naturales incluido el 0, para todo 0<=k<=n se tiene

(n k) = n!/k!(n –k)! = n(n – 1) … (n –k + 1) /k!

Otra definición; Sean n, m Naturales incluido el 0, m<=n, suponemos que el conjunto X tiene n elementos. Entonces la cantidad de subconjuntos de X con m elementos es (n m).

Cálculo del número combinatorio por el triángulo de Pascal (Teorema 2.4.3 con demostración). (Fórmula del triángulo de Pascal). Sean m, n en los Naturales, tal que m<=n. Entonces

(n+1 m) = (n m-1) + (n m)

DEMOSTRACIÓN. El enunciado nos dice que debemos demostrar que

$$\frac{(n+1)!}{(n-m+1)!\,m!} = \frac{n!}{(n-m+1)!\,(m-1)!} + \frac{n!}{(n-m)!\,m!}$$

Hay varias forma de operar algebraicamente las expresiones y obtener el resultado. Nosotros partiremos de la expresión de la derecha y obtendremos la de la izquierda:

$$\begin{aligned}
\frac{n!}{(n-m+1)!\,(m-1)!} + \frac{n!}{(n-m)!\,m!} &= \frac{n!}{(n-m)!\,(m-1)!}\left(\frac{1}{(n-m+1)} + \frac{1}{m}\right) \\
&= \frac{n!}{(n-m)!\,(m-1)!}\left(\frac{m+n-m+1}{(n-m+1)m}\right) \\
&= \frac{n!}{(n-m)!\,(m-1)!}\left(\frac{n+1}{(n-m+1)m}\right) \\
&= \frac{n!(n+1)}{(n-m)!(n-m+1)\,(m-1)!\,m} \\
&= \frac{(n+1)!}{(n-m+1)!\,m!}.
\end{aligned}$$

□

Aunque por razones de conteo es obvio que los números combinatorios son números naturales, esto no es claro por la definición formal.

Enunciado del teorema del binomio (Teorema 2.5.1).

Demostración de que sumatoria bin (n, k) de k=0 a n es igual a 2^n.

22. Demostrar que para todo $n \in \mathbb{N}$ vale:

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

Rta: 2^n es la cantidad de subconjuntos de $\{1, 2, \ldots, n\}$. Si agrupamos los subconjuntos de acuerdo a su cardinal y usamos que $\binom{n}{k}$ es la cantidad de subconjuntos de k elementos de $\{1, 2, \ldots, n\}$ Se tiene la igualdad.
Alternativamente si conocemos la fórmula del binomio de Newton $(a+b)^n = \sum_{i=0}^{n} \binom{n}{i} a^i b^{n-i}$ podemos aplicarla al caso particular $a = 1, b = 1$ y obtener la igualdad del ejercicio.

Demostración de existencia en Teorema 3.1.1 (algoritmo de división).

Teorema 12.4 (Binomio de Newton). *Para todo $a, b \in \mathbb{R}$ y para todo $n \in \mathbb{N}$, se tiene*

$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k} \tag{12.8}$$

Demostración combinatoria. Podemos dar un argumento general, combinatorio. Está claro que

$$(a+b)^n = \underbrace{(a+b)(a+b)\cdots(a+b)}_{n\text{-veces}} \tag{12.9}$$

Un término cualquiera al expandir el producto es de la forma $c_1c_2\cdots c_n$ con $c_i \in \{a,b\}$, $i=1,\ldots,n$. Como hay n factores de la forma $(a+b)$ y de cada uno tenemos 2 posibles elecciones (a ó b), está claro que, por el **PM**, hay 2^n términos de esta forma. Como a y b conmutan, los términos son todos de la forma a^kb^{n-k} con $0 \le k \le n$. Lo que no sabemos es cuántos de éstos hay. Sea $c_k(n)$ el número de términos de la forma a^kb^{n-k}. Luego,

$$(a+b)^n = \sum_{k=0}^{n} c_k(n)\, a^k b^{n-k} \tag{12.10}$$

Sólo tenemos que determinar cuánto vale $c_k(n)$ para cada n y cada $0 \le k \le n$. Pero si pensamos bien, nos damos cuenta que $c_k(n)$ es igual al número de formas de elegir k factores iguales a a, y por lo tanto $n-k$ iguales a b, en (12.9). Es decir que $c_k(n) = \binom{n}{k}$, nuestro famoso número combinatorio. □

Demostración algebraica. Por inducción en n. El paso inicial es claro pues $(a+b)^1 = a+b$ y

$$\sum_{k=0}^{1} \binom{1}{k} a^k b^{n-k} = \binom{1}{0} a^0 b^1 + \binom{1}{1} a^1 b^0 = b + a$$

Supongamos que vale (12.8) para n y veamos que entonces vale

$$(a+b)^{n+1} = \sum_{k=0}^{n+1} \binom{n+1}{k} a^k b^{n+1-k}$$

Como $(a+b)^{n+1} = (a+b)^n(a+b) = (a+b)^n a + (a+b)^n b$, tenemos

$$\begin{aligned}
(a+b)^{n+1} &= \sum_{k=0}^{n} \binom{n}{k} a^{k+1} b^{n-k} + \sum_{k=0}^{n} \binom{n}{k} a^k b^{n+1-k} \\
&= \binom{n}{n} a^{n+1} + \sum_{k=0}^{n-1} \binom{n}{k} a^{k+1} b^{(n+1)-(k+1)} + \binom{n}{0} b^{n+1} + \sum_{k=1}^{n} \binom{n}{k} a^k b^{n+1-k} \\
&= \binom{n+1}{n+1} a^{n+1} + \binom{n+1}{0} b^{n+1} + \sum_{k=1}^{n} \left(\binom{n}{k-1} + \binom{n}{k} \right) a^k b^{(n+1)-k} \\
&= \sum_{k=0}^{n+1} \binom{n+1}{k} a^k b^{(n+1)-k}
\end{aligned}$$

donde hemos usado la identidad de Pascal en la última igualdad. Por el principio de inducción, la fórmula del binomio vale. □

TEOREMA 2.5.1. *Sea n un entero positivo. El coeficiente del termino $a^{n-r}b^r$ en el desarrollo de $(a+b)^n$ es el número binomial $\binom{n}{r}$. Explícitamente, tenemos*

$$(a+b)^n = \binom{n}{0} a^n + \binom{n}{1} a^{n-1} b + \binom{n}{2} a^{n-2} b^2 + \cdots + \binom{n}{n} b^n.$$

DEMOSTRACIÓN. (Primera) Considerar que ocurre cuando multiplicamos n factores

$$(a+b)(a+b)\cdots(a+b).$$

Un término en el producto se obtiene seleccionando o bien a o bien b de cada factor. El número de términos $a^{n-r}b^r$ es solo el número de formas de seleccionar r b's (y consecuentemente $n-r$ a's), y por definición éste es el número binomial $\binom{n}{r}$. □

OBSERVACIÓN 2.5.1. Antes de hacer una segunda demostración del teorema del binomio veamos el siguiente resultado que nos resultará útil: sea $a_k, a_{k+1}, \ldots, a_{m-1}, a_m$ una sucesión de números reales $(k \leq m)$ y sea $r \in \mathbb{N}_0$. Entonces

$$\sum_{i=k}^{m} a_i = \sum_{i=r}^{m-k+r} a_{i+k-r}.$$

Demostración de la existencia en Teorema 3.1.1 (algoritmo de la división).

TEOREMA 3.1.1. *Sean a y b números enteros cualesquiera con $b \in \mathbb{N}$, entonces existen enteros únicos q y r tales que*

$$a = b \times q + r \qquad y \qquad 0 \leq r < b.$$

DEMOSTRACIÓN. Debemos aplicar el axioma del buen orden al conjunto de los "restos"

$$R = \{x \in \mathbb{N}_0 | a = by + x \text{ para algún } y \in \mathbb{Z}\}.$$

Primero demostraremos que R no es vacío. Si $a \geq 0$ la igualdad

$$a = b0 + a$$

demuestra que $a \in R$, mientras que si $a < 0$ la igualdad

$$a = ba + (1-b)a$$

demuestra que $(1-b)a \in R$ (en ambos casos es necesario controlar que el elemento es no negativo.)

Ahora, como R es un subconjunto no vacío de $\mathbb{N}_0$, tiene un mínimo r, y como r esta en R se sigue que $a = bq + r$ para algún q en $\mathbb{Z}$. Además

$$a = bq + r \Rightarrow a = b(q+1) + (r-b)$$

de manera que si $r \geq b$ entonces $r - b$ esta en R. Pero $r - b$ es menor que r, contradiciendo la definición de r como el menor elemento de R. Como la suposición $r \geq b$ nos lleva a una contradicción, solo puede ocurrir que $r < b$, como queríamos demostrar.

Definición de "divide a". Dados dos enteros x e y decimos que y "divide a" x, y escribimos y|x, si

X = yq para algún q en los Enteros.

Es lo mismo que decir y es un factor de x, y divide a x, que x es divisible por y, y que x es múltiplo de y. Algunas propiedades de "divide a". Sean a, b, c enteros, entonces

1. 1|a, a|0, a|+-a;
2. Si a|b, entonces a|bc para cualquier c:
3. Si a|b y a|c, entonces a|b + c;
4. Si a|b y a|c entonces a|rb + sc para cualquier s, s en los Enteros.

Definición de Máximo Común Divisor (MCD). Dados dos enteros a y b no simultáneamente nulos, el MCD de a y b, es el mayor de los divisores comunes de a y b. Se denota por (a, b) o también por mcd(a, b). Dos enteros se dicen coprimos si (a, b) = 1.

El MCD es único (enunciado y demostración de teorema 3.3.1) Sean a, b enteros con alguno de ellos no nulo. Si el mcd entre a y b existe, entonces es único.

DEMOSTRACIÓN. Sean d y d' dos enteros no negativos que satisfacen las propiedades de la definición del máximo común divisor. Es decir

$$(11) \qquad (i)\ d|a \text{ y } d|b; \quad (ii) \text{ si } c|a \text{ y } c|b \text{ entonces } c|d$$

$$(12) \qquad (i)\ d'|a \text{ y } d'|b; \quad (ii) \text{ si } c|a \text{ y } c|b \text{ entonces } c|d'$$

Ahora bien, d satisface la propiedad $(11)(i)$, aplicando la propiedad $(12)(ii)$ obtenemos que $d|d'$. Análogamente, d' satisface la propiedad $(12)(i)$, luego aplicando la propiedad $(11)(ii)$ obtenemos que $d'|d$. Por lo tanto $d, d' \geq 0$ y se dividen mutuamente y en consecuencia son iguales (ver ejemplo 3.2.1). □

Cuando el máximo común divisor entre a y b existe lo denotaremos $\text{mcd}(a, b)$.

Enunciado del teorema 3.3.6 Sean a y b enteros, b no nulo y sea d = mcd(a, b). Entonces existen enteros s y t tales que

d = sa + tb

A esta escritura se le llama combinación lineal del mcd(a, b)

Demostración del corolario 3.3.7. Sean a y b enteros, b no nulo, entonces

mcd(a, b) = 1 si y solo si existen s, t enteros tales que 1 = sa + tb.

Demostración: Sea d = mcd(a, b), entonces d|a y d|b y por lo tanto d|sa + tb para cualesquiera s, t enteros. En particular, la hipótesis implica que d|1 y, en consecuencia d = 1.

Otra demostración. Dados a, b enteros, no simultáneamente nulos, a/(a, b) y b/(a, b) son coprimos.

1 = r a/(a, b) + s b/(a, b) Se sigue lo que se quería demostrar

Definición de enteros coprimos. (Definición 3.3.2) Si el mcd(a, b) = 1 entonces decimos que a y b son coprimos.

Definición de Mínimo Común Múltiplo (MCM). Dados dos enteros a y b, el mínimo común múltiplo de a y b es el menor entero no negativo que es múltiplo de ambos. Denotamos al mínimo común múltiplo de a y b por [a, b] o mcm(a, b).

Definición 3.3.3. Si a y b son enteros decimos que un entero no negativo m es el mínimo común múltiplo, o mcm de a y b si

1. a|m y b|m;
2. si a|n y b|n entonces m|n.

La condición 1 nos dice que m es múltiplo común de a y b, la condición 2 nos dice que es mínimo. Por ejemplo hallemos el mínimo común múltiplo entre 8 y 14. Escribamos los múltiplos
de ambos números y busquemos el menor común a ambos. Los primeros múltiplos de 8 son:

8; 16; 24; 32; 40; 48; 56; : : :. Los primeros múltiplos de 14 son: 14; 28; 42; 56; 72; : : :. Luego se tiene mcm(8; 14) = 56.

Relación entre el mcd y el mcm (enunciado del teorema 3.3.8) Sean a y b enteros no nulos, entonces

mcm(a, b) = ab/mcd(a, b)

Definición de número primo. Se dice que un entero positivo p es primo si p>=2 y los únicos enteros que dividen p son 1 y p mismo. De acuerdo a la definición 1 no es primo.

Todo entero mayor que 1 es producto de números primos (enunciado y demostración del teorema 3.4.1)

DEMOSTRACIÓN. Sea B el conjunto de enteros positivos que no tienen una factorización en primos.

Si B no es vacío entonces, por el axioma del buen orden, tiene un mínimo m. Si m fuera un primo p entonces tendríamos la factorización trivial $m = p$; por lo tanto m no es primo y existen m_1, m_2 enteros positivos con $1 < m_1 < m$ y $1 < m_2 < m$ tal que $m = m_1 m_2$.

Como estamos suponiendo que m es el menor entero (≥ 2) que no tiene factorización en primos, entonces m_1 y m_2 tienen factorización en primos. Pero entonces la ecuación $m = m_1 m_2$ produce una factorización en primos de m, contradiciendo la suposición de que m era un elemento de B. Por lo tanto B debe ser vacío, y la afirmación esta probada. □

Enunciado y demostración del teorema 3.4.4(1).

Sea p un número primo, (1) Si p|xy entonces p|x o p|y

DEMOSTRACIÓN (1). Si p|x ya está probado el resultado. Si p no divide a x entonces tenemos mcd(x, p) = 1. Por la combinación lineal del mcd (el teorema 3.3.6) existen enteros r y s tales que rp + sr = 1. Por lo tanto tenemos

$$y = (rp + sx)\, y = (ry)p + s(xy).$$

Como p|p y p|xy, entonces divide a ambos términos y se sigue que p|y.

Demostrar que existen infinitos números primos (proposición 3.4.6)

DEMOSTRACIÓN. Haremos la demostración por el absurdo: supongamos que existen en total r números primos $p_1, p_2, \ldots, p_r$. Sea $n = p_1 p_2 \ldots p_r + 1$. Sea p primo tal que $p|n$. Como la lista de primos es exhaustiva, existe i con $1 \leq i \leq r$ tal que $p = p_i$. Ahora bien $p_i|n$ y $p_i|p_1 p_2 \ldots p_r$, luego $p_i|n - p_1 p_2 \ldots p_r = 1$, lo cual es un absurdo que vino de suponer que el número de primos es finito. □

Teorema Fundamental de la Aritmética (TFA) (teorema 3.4.5 y 6.24 de n. m. y Álgebra respectivamente)

- **3.4.5:** La factorización en primos de un entero positivo n>=2 es única, salvo el orden de los factores primos.

DEMOSTRACIÓN. Por el axioma del buen orden, si existe un entero para el cual el teorema es falso, entonces hay un entero mínimo $n_0 \geq 0$ con esta propiedad. Supongamos entonces que

$$n_0 = p_1 p_2 \dots p_k \quad \text{y} \quad n_0 = p'_1 p'_2 \dots p'_l,$$

donde los p_i $(1 \leq i \leq k)$ son primos, no necesariamente distintos, y los p'_i $(1 \leq i \leq l)$ son primos, no necesariamente distintos. La primera ecuación implica que $p_1 | n_0$, y la segunda ecuación implica que $p_1 | p'_1 p'_2 \dots p'_l$. Por consiguiente por teorema 3.4.4 tenemos que $p_1 | p'_j$ para algún j $(1 \leq j \leq l)$. Reordenando la segunda factorización podemos asumir que $p_1 | p'_1$, y puesto que p_1 y p'_1 son primos, se sigue que $p_1 = p'_1$ (observación 3.4.2 3)). Luego por el axioma **I7**, podemos cancelar los factores p_1 y p'_1, y obtener

$$p_2 p_3 \dots p_k = p'_2 p'_3 \dots p'_l,$$

y llamemos a esto n_1. Pero supusimos que n_0 tenía dos factorizaciones diferentes, y hemos cancelado el mismo número $(p_1 = p'_1)$ en ambas factorizaciones, luego n_1 tiene también dos factorizaciones primas diferentes. Esto contradice la definición de n_0 como el mínimo entero sin factorización única. Por lo tanto el teorema es verdadero para $n \geq 2$. □

- **6.24:** Todo número entero no nulo distinto de 1 ó -1 es el producto de números primos si es positivo y es el producto de -1 por un producto de números primos si es negativo. Los distintos factores primos que aparecen y sus multiplicidades son únicos. Es decir, la factorización mencionada es única salvo el orden de sus factores.

Demostración. Basta suponer que a es natural.

EXISTENCIA: Se sigue directamente de la Proposición 6.15.

UNICIDAD: Sean $a = p_1 \dots p_r$ y $a = q_1 \dots q_s$ dos factorizaciones de a como producto de números primos, con $r, s \geq 1$. Debemos mostrar que $r = s$ y que para cada $1 \leq i \leq r$ existe un $1 \leq j_i \leq s$ tal que $p_i = q_{j_i}$ donde $j_i \neq j_k$ si $i \neq k$. Hacemos esto por inducción en el mayor de los naturales r y s, que podemos suponer sin pérdida de generalidad que es r.

PASO 1: Si $r = 1$, entonces $a = p_1$ y $a = q_1$, luego $r = s$ y $p_1 = q_1$.

PASO 2: Supongamos que $r = n + 1$. Así $a = p_1 \dots p_n p_{n+1}$ y $a = q_1 \dots q_s$ con $s \leq n + 1$. Ahora, $p_{n+1} \mid a$, luego por el Lema 6.14 $p_{n+1} \mid q_j$ para algún $1 \leq j \leq n + 1$. Siendo ambos primos, se sigue que son iguales, es decir $p_{n+1} = q_j$. Si $j \neq s$, permutamos en la segunda factorización q_j con q_s, y así resulta que $p_{n+1} = q_s$. Por la propiedad cancelativa se sigue que

$$a' = p_1 \cdots p_n = q_1 \cdots q_{s-1}.$$

Tenemos ahora dos factorizaciones de a' como producto de números primos, una con n factores y otra con $s - 1$ factores, con $n \geq s - 1$. Por lo tanto, por hipótesis inductiva, se sigue que $n = s - 1$ y que para cada $1 \leq i \leq n$ existe un $1 \leq j_i \leq s$ tal que $p_i = q_{j_i}$, donde $j_i \neq j_k$ si $i \neq k$. De esto se sigue que $n + 1 = s$ y que para cada $1 \leq i \leq n + 1$ existe un $1 \leq j_i \leq s$ tal que $p_i = q_{j_i}$ donde $j_i \neq j_k$ si $i \neq k$. □

El TFA tiene consecuencias profundas en la aritmética entera y también, por ejemplo, en la estructura y aritmética de los reales, como muestran los siguientes problemas.

Definición de Congruencia

Definición. Dados a, b, m enteros con $m > 0$, decimos que a *es congruente a* b *módulo* m si m divide a la diferencia de a y b. En este caso, escribimos $a \equiv b \pmod{m}$. En símbolos,

$$a \equiv b \pmod{m} \qquad \Leftrightarrow \qquad m \mid a - b$$

El entero m se llama el *módulo* de la congruencia. Si a no es congruente a b módulo m, es decir, si $m \nmid a - b$, entonces decimos que a y b son *incongruentes* módulo m y escribimos $a \not\equiv b \pmod{m}$ en este caso.

Esto es lo mismo a decir que (por proposición 4.1.1) que a y b enteros y m un entero positivo. Entoces a es congruente a b modulo m si y sólo si a y b tienen en mismo resto en la división por m.

DEMOSTRACIÓN. Si $a = mh + r$ y $b = mk + s$, con $0 \leq r, s < m$, podemos suponer, sin perdida de generalidad, que $r \leq s$, luego

$$b - a = m(k - h) + (s - r) \quad \text{con } 0 \leq s - r < m.$$

Se sigue que $s - r$ es el resto de dividir $b - a$ por m.

Luego si $a \equiv b \pmod{m}$, el resto de dividir $b - a$ por m es 0, y por lo tanto $s - r = 0$ y $s = r$.

Si a y b tienen el mismo resto en la división por m, entonces $a = mh + r$ y $b = mk + r$, luego $a - b = m(h - k)$ que es divisible por m. □

Demostración del teorema 4.1.2.

TEOREMA 4.1.2. *Sea m un entero positivo y sean x_1, x_2, y_1, y_2 enteros tales que*

$$x_1 \equiv x_2 \pmod{m}, \qquad y_1 \equiv y_2 \pmod{m}.$$

Entonces

(i) $x_1 + y_1 \equiv x_2 + y_2 \pmod{m}$,
(ii) $x_1 y_1 \equiv x_2 y_2 \pmod{m}$,
(iii) *Si* $x \equiv y \pmod{m}$ *y* $j \in \mathbb{N}$, *entonces* $x^j \equiv y^j \pmod{m}$.

DEMOSTRACIÓN. (i) Por hipótesis tenemos que existen enteros x, y tales que $x_1 - x_2 = mx$ e $y_1 - y_2 = my$. Se sigue que

$$\begin{aligned}(x_1 + y_1) - (x_2 + y_2) &= (x_1 - x_2) + (y_1 - y_2) \\ &= mx + my \\ &= m(x + y),\end{aligned}$$

y por consiguiente el lado izquierdo es divisible por m, como queríamos demostrar.

(ii) Aquí tenemos

$$\begin{aligned} x_1y_1 - x_2y_2 &= x_1y_1 - x_2y_1 + x_2y_1 - x_2y_2 \\ &= (x_1 - x_2)y_1 + x_2(y_1 - y_2) \\ &= mxy_1 + x_2my \\ &= m(xy_1 + x_2y), \end{aligned}$$

y de nuevo el lado izquierdo es divisible por m.

(iii) Lo haremos por inducción sobre j.

Es claro que si $j = 1$ el resultado es verdadero. Supongamos ahora que el resultado vale para $j - 1$, es decir que si $x \equiv y \pmod{m}$, entonces

$$x^{j-1} \equiv y^{j-1} \pmod{m}.$$

Como $x \equiv y \pmod{m}$, por *(ii)* tenemos que

$$x^{j-1}x \equiv y^{j-1}y \pmod{m},$$

es decir

$$x^j \equiv y^j \pmod{m}.$$

□

Enunciado del teorema 4.2.1: Existen soluciones en la ecuación lineal de congruencia. Sean a. b números enteros y m un entero positivo y denotamos d = mcd(a, m). La ecuación "ax congruente a b (modulo m)" admite solución si y sólo si d|b, y en este caso dada x0 una solución, todas las soluciones son de la forma "x = x0 + kn, con k en Enteros y n = m/d". Con las demostraciones podemos obtener un método general para encontrar soluciones de la ecuación lineal de congruencia

"ax congruente a b (modulo m)" con mcd(a, m)|b

*Demostración anexada en pág. 65 de Notas.

Teorema de Fermat (teorema 4.3.2) Sea p un número primo y a número entero, entonces

- "*a*^p congruente a *a* (modulo p)"

Supongamos que a y p son coprimos, por Fermat p|(a^p – a) = a(a^(p – 1) – 1). Como p no divide a a, tenemos que p|(a^(p – 1) – 1), es decir "si a y p son coprimos, entonces

- a^(p-1) congruente 1 (modulo p)""

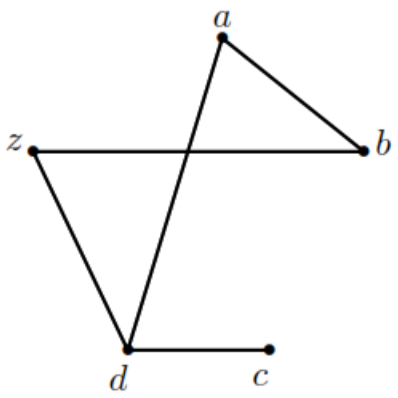
DEMOSTRACIÓN. Supongamos que $a \geq 0$, entonces hagamos inducción en a. Si $a = 0$, el resultado es trivial. Supongamos el resultado probado para k, es decir $k^p \equiv k \pmod{p}$. Entonces $(k+1)^p \equiv k^p + 1^p \equiv k + 1 \pmod{p}$. La primera congruencia es debido al lema 4.3.1 (ii) y la segunda es válida por hipótesis inductiva. Luego $a^p \equiv a \pmod{p}$ cuando $a > 0$.

Si $a < 0$, entonces $-a > 0$ y ya vimos que $(-a)^p \equiv -a \pmod{p}$, es decir que $(-1)^p a^p \equiv (-1)a \pmod{p}$. Si $p \neq 2$, entonces $(-1)^p = -1$ y se deduce el resultado. Si $p = 2$, entonces $(-1)^p = 1$, pero como $1 \equiv -1 \pmod{2}$, obtenemos también $a^p \equiv a \pmod{p}$. □

Definición de grafo. Un grafo G consiste de un conjunto finito V, cuyos miembros son llamados vértices, y un conjunto de 2-subconjuntos de V, cuyos miembros son llamados aristas. Nosotros usualmente escribiremos G = (V, E) y diremos que V es el conjunto de vértices y E es el conjunto de aristas. La propiedad característica de un grafo es la manera en que los vértices están conectados por aristas. Es conveniente restringirnos a grafos finitos por ahora. Como ejemplo de grafo G = (V, E) es dado por los conjuntos

V = {a, b, c, d, z}, E = {{a, b}, {a, d}, {b, z}, {c, d}, {d, z}}

Este ejemplo y la definición misma no son suficientemente esclarecedoras, por lo que se considera una representación pictórica de un grafo (del ejemplo anterior)



*Se amplía con videos de grafos

Definición de isomorfismo de grafos. Dos grafos G1 y G2 se dicen que son isomorfos cuando existe una biyección *a* entre el conjunto de vértices de G1 y el conjunto de vértices de G2 tal que si {x, y} es una arista de G1 entonces {*a*(x), *a*(y)} es una arista de G2 y recíprocamente si {z, w} es una arista de G2 entonces {*a*^(-1)(z), *a*^(-1)(w)} es una arista de G1. La biyección *a* es llamada un isomorfismo.

Definición de valencias.

5.3. Valencias

La *valencia* de un vértice v en un grafo $G = (V, E)$ es el número de aristas de G que contienen a v. Usaremos la notación $\delta(v)$ para la valencia de v, formalmente

$$\delta(v) = |D_v|, \quad \text{donde} \quad D_v = \{e \in E | v \in e\}.$$

El grafo descrito en Fig. 1 tiene $\delta(a) = 2$, $\delta(b) = 2$, $\delta(c) = 1$, $\delta(d) = 3$, $\delta(z) = 2$. El primer teorema de la teoría de grafos nos dice que la suma de estos números es dos veces el número de aristas.

Demostrar que la suma de las valencias de un grafo es dos veces el número de aristas.

TEOREMA 5.3.1. *La suma de los valores de las valencias $\delta(v)$, tomados sobre todos los vértices v del grafo $G = (V, E)$, es igual a dos veces el número de aristas:*

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

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

Hay un útil corolario de este resultado. Diremos que un vértice de G es *impar* si su valencia es impar, y *par* si su valencia es par. Denotemos V_i y V_p los conjuntos de vértices impares y pares respectivamente, luego $V = V_i \cup V_p$ es una partición de V. Por teorema 5.3.1, tenemos que

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

Ahora cada término en la segunda suma es par, luego esta suma es un número par. Puesto que el lado derecho también es un número par, la primera suma debe ser también par. Pero la suma de números impares solo puede ser par si el número de términos es par. En otra palabras:

Teorema 5.3.2. El número de vértices impares es par.

Este resultado es a veces llamado el "handshaking lemma" (handshake=estrechar la mano, darse la mano), debido a que se puede interpretar en términos de gente y darse la mano: dado un conjunto de personas, el número de personas que le ha dado la mano a un número impar de miembros del conjunto es par.

Un grafo en el cual todos los vértices tienen la misma valencia r se llama *regular* (con valencia r), o *r-valente*. En este caso, el resultado del teorema 5.3.1 se traduce

$$r|V| = 2|E|.$$

Muchos de los grafos que aparecen en las aplicaciones son regulares. Ya conocemos los grafos completos K_n; ellos son regulares, con valencia $n - 1$. De geometría elemental conocemos los polígonos de n lados, los cuales en teoría de grafos son llamados *grafos cíclicos* C_n. Formalmente, podemos decir que el conjunto de vértices de C_n es $\mathbb{Z}_n$, y los vértices i y j están unidos si $j = i+1$ o $j = i - 1$ en $\mathbb{Z}_n$. Claramente, C_n es un grafo regular con valencia 2, si $n \geq 3$.

Una aplicación importante de la noción de valencia es en el problema de determinar si dos grafos son o no isomorfos. Si $\alpha : V_1 \to V_2$ es un isomorfismo entre G_1 y G_2, y $\alpha(v) = w$, entonces cada arista que contiene a v se transforma en una arista que contiene a w. En consecuencia $\delta(v) = \delta(w)$. Por otro lado, si G_1 tiene un vértice x, con valencia $\delta(x) = \delta_0$, y G_2 no tiene vértices con valencia δ_0, entonces G_1 y G_2 no pueden ser isomorfos. Esto nos da otra manera para distinguir los grafos de la Fig 4, puesto que el primer grafo tiene un vértice de valencia 1 y el segundo no.

Definición de caminara y camino (definición 5.4.1) Una caminata en un grafo G es una secuencia de vértices (v1, v2, …, vk) tal que vi y v(i + 1) son adyacentes (1 <= i <= k – 1). Si todos los vértices son distintos, una caminata es llamado un camino.

Definición de ciclo. Un ciclo es una caminata (v1, v2, …, v(r + 1)) cuyos vértices son distintos exceptuando los externos, es decir que v1 = v(r + 1) y a menudo diremos que es r-ciclo, o un ciclo de longitud r en G.

Definición de ciclo hamiltoniano y caminata euleriana (definición 5.4.3). Un ciclo hamiltoniano en un grafo G es un ciclo que contiene a todos los vértices del grafo. Una caminata euleriana en un grafo G, en cambio, es una caminata que usa todas las aristas de G exactamente una vez. Una caminata euleriana que comienza y termina en un mismo vértice se llama también circuito euleriano.

Enunciado del teorema de caminos eulerianos (teorema 5.4.2). Un grafo conexo con más de un vértice posee una caminata euleriana de v a w, con v distinto a w si y sólo si v y w son los únicos vértices de grado impar. Un grafo conexo con más de un vértice tiene un circuito euleriano si y sólo si todos los vértices tienen grado par.

Definición de árbol.

5.5. Árboles

DEFINICIÓN 5.5.1. Diremos que un grafo T es un *árbol* si cumple

(T1) T es conexo y no hay ciclos en T.

Algunos árboles típicos han sido dibujados en la Fig. 9. A causa de su particular estructura y propiedades, los árboles aparecen en diversas aplicaciones de la matemática, especialmente en investigación operativa y ciencias de la computación. Comenzaremos el estudio de ellos estableciendo algunas propiedades sencillas.

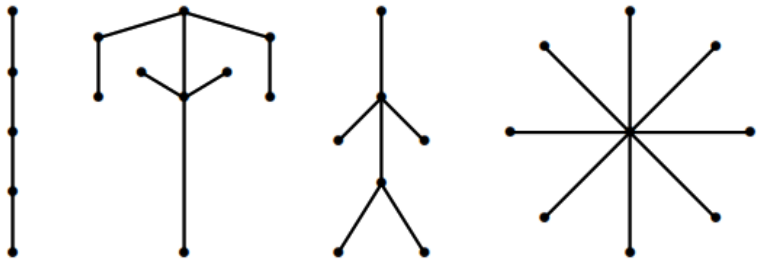


FIGURA 9. Algunos árboles

Teorema 5.5.2 (T1 => T2) Si T = (V, E) es un grafo conexo con al menos dos vértices, entonces son equivalentes las siguientes propiedades

(T1) T es un árbol.

(T2) Para cada par x, y de vértices existe un único camino en T de x a y,

(T3) El grafo obtenido de T removiendo alguna arista tiene dos componentes, cada una de las cuales es un árbol,

(T4) |E| = |V| - 1

La demostración de (T1) => (T2): Puesto que T es conexo, existe un camino de x a y, digamos
X = v0, v1,…, vr = y.
Si existiera otro camino, digamos
X = u0, u1,…, us = y
Consideremos i el más pequeño subíndice para el cual se cumple que u(i + 1) es distinto v(i + 1) (Fig. 10)

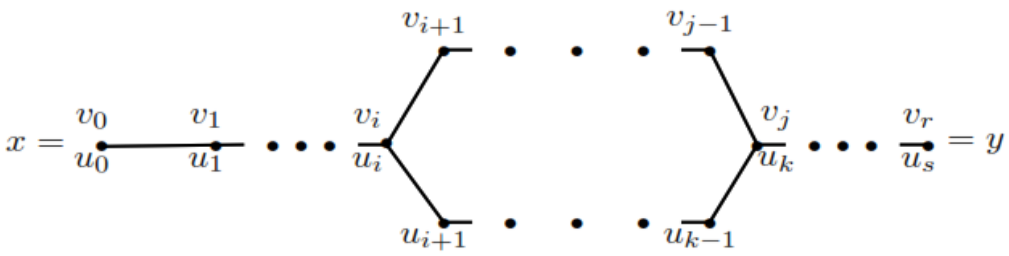


FIGURA 10. Dos caminos diferentes determinan un ciclo

Puesto que ambos caminos finalizan en y ellos se encontrarán de nuevo, y entonces podemos definir j como el más pequeño subíndice tal que

$$j > i \quad \text{y} \quad v_j = u_k \quad \text{para algún } k.$$

Entonces $v_i, v_{i+1}, \ldots, v_j, u_{k-1}, u_{k-2}, \ldots, u_{i+1}, v_i$ es un ciclo en T, y esto contradice a las hipótesis. Por consiguiente solo existe un camino en T de x a y.

(T2) $\Rightarrow$ (T3): Supongamos que uv es una arista en T, y sea $S = (V, E')$ el grafo con el mismo conjunto de vértices que T y con el conjunto de aristas $E' = E - uv$. Sea V_1 el conjunto de los vértices x de T para los cuales existe un único camino en T de x a v que pasa por u. Claramente, este camino debe finalizar con la arista uv, pues sino T tendría un ciclo. Sea V_2 el complemento de V_1 en V.

Cada vértice en V_1 se une por un camino en S a u, y cada vértice en V_2 se une por un camino en S a v, pero no existe camino de u a v en S. Se sigue entonces que V_1 y V_2 son las dos componentes del conjunto de vértices de S. Cada componente es conexa (por definición), y no contiene ciclos, pues sino habría ciclos en T. Es decir que las dos componentes son árboles.