

16/03/21

1.1

Regularidad: aprobar (50%) 8/10 tareas.

Axiomas: Reglas básicas, indiscutibles.

-Axiomas Enteros (\mathbb{Z})

I) $a+b \wedge a.b \in \mathbb{Z}$, $a \wedge b \in \mathbb{Z}$

II) Comunitatividad. $a+b = b+a$; $ab = ba$

III) Asociatividad.

$$(a+b)+c = a+(b+c)$$

$$(a.b).c = a.(b.c)$$

IV) Existencia elemento neutro.

Suma

$$a+0 = a$$

multiplicación

$$a \cdot 1 = a$$

Los elementos neutros
para la suma y multiplicación
son únicos

V) Distributividad.

$$a.(b+c) = (a.b) + (a.c)$$

VII) Existencia del inverso aditivo (opuesto).

$\forall a \in \mathbb{Z}, \exists a' = -a \in \mathbb{Z}, a + (-a) = 0$

$$a + (-a) = 0$$

Existe un único entero.

Me lo inventé
yo, xd

VIII) Cacelación.

¿Por qué este axioma existe, si con la ley
única se justifica? Porque con la ley uniforme
se siempre se puede operar con enteros. Los índices no están
definidos para los índices.

Si $a \neq 0$, entonces $a \cdot b = a \cdot c \rightarrow b = c$

-Definición de resta:

$a, b \in \mathbb{Z} \rightarrow a - b$ es la suma de a con el
opuesto de b .

$$a - b \rightarrow a + (-b)$$

Demostración $a - (-n) = a + n$

$a + (-(-n))$, Sabemos que $-(-n) = n$ por el opuesto del opuesto
entonces:

$$= a + n$$

(No es la regla de signos)

18/03/21

Axiomas de Orden

I) Tricotomía

No se pueden cumplir mas de 1 de estas relaciones:

$$a=b \vee a>b \vee a<b$$

II) Transitiva

Si $a < b \wedge b < c$, $a < c$

III) Compatibilidad de la suma.

Si $a < b$, $a+c < b+c$

IV) Compatibilidad del producto

$a < b$, entonces $a.c < b.c$ si $c > 0$

Axioma de buena ordenación

Si X es un subconjunto de \mathbb{Z} que no es vacío y tiene cota inferior, entonces X tiene mínimo.

que hace
un menor
elemento
indica que es
seccional

Definición

Si X es un subconjunto de \mathbb{Z} , entonces el entero b es una cota inferior de X si:

$$b \leq x \quad \forall x \in X$$

Definición

Una cota inferior de un conjunto X que a su vez es un elemento de X , es conocido como el mínimo de X .

Observaciones:

- Un subconjunto no tiene mínimo si se va haciendo infinitamente "más chico", es decir que infinitamente se mueve a la izquierda de la recta real. (puede tener cota inferior)

Ejemplo $A = \left\{ \frac{1}{m} = m \in \mathbb{N} \right\}$ (números racionales)

Se va acercando al cero pero nunca llega. No tiene mínimo, pero sí cota inferior.

- Un mínimo es una cota inferior pero no toda cota inferior es un mínimo.
- Hay una única cota inferior que es mínimo
- El mínimo (si existe) es mínimo.
- Si un subconjunto está acotado inferiormente, tiene infinitas cotas inferiores.
- TODO subconjunto de \mathbb{Z} acotado inferiormente (no vacío) tiene cota inferior
- El subconjunto no vacío de \mathbb{Z} de un subconjunto no vacío de \mathbb{Z} que está acotado inferiormente, tiene mínimo.

Otras Propiedades

I) Reflexividad $a \leq a$

II) Antisimetría. Si $a \leq b \wedge b \leq a \Rightarrow a = b$

III) Transitividad. Si $a \leq b \wedge b \leq c \Rightarrow a \leq c$

Conceptos anteriores a def. Recur.

Sucesión: Serie de valores que toma una función sobre los naturales.

$$Ej: \textcircled{A} \quad U_n = 3n + 2$$

$$U_1 = 3(1) + 2 = 5$$

$$U_2 = 3(2) + 2 = 8$$

$$\textcircled{B} \quad W_n = (n+1)(n+2)(n+3)$$

$$W_1 = (1+1)(1+2)(1+3) = 2 \cdot 3 \cdot 4 = 24$$

$$W_2 = (2+1)(2+2)(2+3) = 3 \cdot 4 \cdot 5 = 60$$

- Cuando una sucesión puede expresarse como una combinación de un número determinado de operaciones diremos que tiene fórmula cerrada. En contraparte si no lo tiene la podremos definir de forma recursiva.

Definición Recursiva

Dado un caso base: $U_1 = 1, U_2 = 2$

y una definición recursiva: $U_n = U_{n-1} + U_{n-2}$, para $n \geq 3$

Podremos determinar todos los U_n .

Productoria

Primer término = $a_1 = \prod_{i=1}^1 a_i$

Todos los términos = $\prod_{i=1}^n a_i = \left(\prod_{i=1}^{n-1} a_i \right) \cdot a_n$, para $n \geq 2$

Números Factoriales

$$0! = 1$$

$$1! = 1$$

$$n! = (n-1)! \cdot n, \quad n > 1$$

$$n! = \prod_{i=1}^n i$$

No admite fórmula cerrada

Potencia enésima

Sea $n \in \mathbb{N}$

$$\begin{cases} x^1 = x \\ x^m = x^{m-1} \cdot x, \quad m > 1 \end{cases}$$

$$x^0 = 1, \forall x$$

Principio de Inducción

Sea $P(n)$ una propiedad verdadera para $n \in \mathbb{N}$

Si:

a) $P(1)$ es verdadera

b) para todo $k \in \mathbb{N}$, $P(k)$ verdadera implica $P(k+1)$ es verdadera.

Entonces $P(n)$ es verdadera para todo \mathbb{N}

Para demostrar basta tomar:

$$S = \{n \in \mathbb{N} / P(n) \text{ es verdadera}\}$$

$S \subseteq \mathbb{N}$, no es vacío por a), y por b) $S = \mathbb{N}$, es decir que $P(n)$ es verdadera para todo $n \in \mathbb{N}$.

Demonstración de que b) $\Rightarrow S = \mathbb{N}$

Dado un subconjunto de los naturales S que satisface:

a) 1 e s

b) $\forall k \in N$, si $k \in S$ entonces $k+1 \in S$

$$S = N$$

Si fuese falso: $S \neq N \rightarrow$ No significa disjunto

$$S \neq S^c = \{ r \in N \mid r \notin S \}$$

- Si S^c no es vacío, tiene mínimo.

- Por a) Se sabe que $1 \notin S^c$, entonces $m \neq 1$, $m > 1$ por lo tanto $m \in N$

- Por lógica $m-1 \in \mathbb{N}$. ($m = \text{mínimo de } S^c$)

- Si m es el mínimo de S^c , entonces $m-1$ es

$$\text{Si } K = \underbrace{m - 1}_{\begin{array}{l} \text{Número} \\ \downarrow \\ \text{mínimo} \end{array}} \rightarrow \notin S^c$$

Es decir $K \in S^c$

Operando

$$K+1 = m - 1 + 1$$

a) Caso base

En el enunciado:

$$X_1 = 2$$

En la igualación a demostrar:

$$X_1 = 1(1+1) = 1 \cdot 2 = 2$$

b) Paso inductivo

$$n = k$$

$$P(k): X_k = k(k+1) \rightsquigarrow \text{Hipótesis inductiva}$$

$$n = k+1$$

$$P(k+1): X_{k+1} = (k+1)((k+1)+1) = (k+1)(k+2)$$

(Queremos probar: $X_k = k(k+1) \Rightarrow X_{k+1} = (k+1)(k+2)$)

Esto es Verdadero (Por lo que asumimos para demostrar)
Por lo tanto necesitamos
que lo otro sea
Verdadero

Número anterior

$$X_{K+1} = X_K + 2(K+1)$$

Por def recursión

$$= \underbrace{K(K+1)}_{\text{Por hipótesis}} + 2(K+1)$$

Factor común

inductiva

$$\boxed{X_{K+1} = (K+1)(K+2)}$$

Inducción Completa.

Sea $n_0 \in \mathbb{Z} \rightarrow P(n)$ una propiedad para todo $n \geq n_0$

Si

a) $P(n_0)$ es verdadera

b) $P(h)$ es verdadera para todo h tal que $n_0 \leq h \leq K$ implica que $P(k+1)$ es verdadera

\rightarrow Representa el

intervalo de

números anteriores

a K

Entonces $P(n)$ es verdadera para todo $n \geq n_0$

Ejemplo:

Dado

$$U_1 = 3, U_2 = 5$$

$$U_n = 3 \cdot U_{n-1} - 2U_{n-2}, \quad n \geq 3$$

Demoststrar que $U_n = 2^n + 1, \quad n \in \mathbb{N}$

a) Caso base

Enunciado

$$\boxed{n=1}$$

$$U_1 = 3$$

$$\boxed{n=2}$$

$$U_2 = 5$$

Propiedad a demostrar

$$\boxed{n=1}$$

$$U_1 = 2^1 + 1 = 3$$

$$\boxed{n=2}$$

$$U_2 = 2^2 + 1 = 5$$

b) Pás inductivo

$$P(n) : U_h = 2^h + 1 \quad \text{para todo } 1 \leq h \leq k \wedge k \geq 2 \quad (\text{HI})$$

$$P(k+1) : U_{k+1} = 2^{k+1} + 1$$

$$P(h) \Rightarrow P(k+1)$$

30/03/21

$$U_{k+1} = 3(U_{(k+1)-1}) - 2U_{(k+1)-2}$$

Por def recursiva

$$= 3U_k - 2U_{k-1}$$

Por HI se cumple para los
números menores ya los 2^k
(así en este caso entonces podemos
reemplazar)

$$= 3(2^k + 1) - 2(2^{k-1} + 1)$$

$$= 3 \cdot 2^k + 3 - 2 \cdot 2^{k-1} - 2$$

$$= 3 \cdot 2^k - 2 \cdot 2^{k-1} \cdot 2^k + 1$$

$$= 2^k(3-1) + 1$$

$$= 2^k \cdot 2 + 1$$

$$\boxed{U_{k+1} = 2^{k+1} + 1}$$

Resumen y Ejercicios

En la práctica el principio de Inducción lo utilizamos para demostrar que cierta sucesión tiene fórmula cerrada.

Ejemplo 1

Dado $X_n = \sum_{i=1}^n i$

Demoststrar que $X_n = \frac{n(n+1)}{2}$

a) enunciado
 $n=1$

$$\sum_{i=1}^1 i = \boxed{1}$$

A demostrar
 $n = 1$

$$\frac{1(1+1)}{2} = \frac{1(2)}{2} = \boxed{1}$$

b)

$$\sum_{i=1}^k i = \frac{k(k+1)}{2} \implies \sum_{i=1}^{k+1} i = \frac{(k+1)((k+1)+1)}{2}$$

$$\sum_{i=1}^{k+1} i = \sum_{i=1}^k i + (k+1)$$

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

$$= (k+1)\left(\frac{k}{2} + 1\right)$$

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

Ejemplo 2

Dado $q > 0 \wedge q \neq 1$, $X_n = \sum_{i=0}^n q^i$

Demoststrar que $X_n = \frac{q^{n+1} - 1}{q - 1}$

a) Enunciado

A demostrar

$$X_1 = \sum_{i=0}^1 q^i = q^0 + q^1 = q + 1$$

$$X_1 = \frac{q^{1+1} - 1}{q - 1} = \frac{(q-1)(q+1)}{(q-1)} = q + 1$$

b)

$$X_k = \sum_{i=0}^k q^i = \frac{q^{k+1} - 1}{q - 1} \Rightarrow X_{k+1} = \sum_{i=0}^{k+1} q^i = \frac{q^{(k+1)+1} - 1}{q - 1}$$

$$\sum_{i=0}^{k+1} q^i = \sum_{i=0}^k q^i + q^{k+1}$$

$$= \frac{q^{k+1} - 1}{q - 1} + q^{k+1}$$

Luego de operar:

$$= \frac{q^{k+2} - 1}{q - 1}$$

Ejemplo 3

Esto es la sumatoria aritmética del ejemplo 1 entonces

$$\text{Demostrar: } \overbrace{(1+2+3+\dots+n)}^2 = X_n = \left(\sum_{i=1}^n i \right)^2 = \left(\frac{n(n+1)}{2} \right)^2$$

Prado: $X_n = 1^3 + 2^3 + 3^3 + \dots + n^3 = \sum_{i=1}^n i^3$

a) Demostrar

$n=1$

enunciado

$$\left(\sum_{i=1}^1 i \right)^2 = X_1 = 1$$

$$X_1 = \sum_{i=1}^1 i^3 = 1^3 = 1$$

b)

$$X_k = \left(\sum_{i=1}^k i \right)^2 = \left(\frac{k(k+1)}{2} \right)^2 \Rightarrow X_{k+1} = \left(\sum_{i=1}^{k+1} i \right)^2 = \frac{(k+1)^2(k+2)}{4}$$

$$X_{k+1} = \left(\sum_{i=1}^k i + (k+1) \right)^2$$

$$= \left(\frac{k(k+1)}{2} + (k+1) \right)^2 = \left(\frac{k(k+1) + 2(k+1)}{2} \right)^2 = \left(\frac{(k+1)(k+2)}{2} \right)^2$$

$$= \frac{(k+1)^2 + (k+2)^2}{4}$$

Ejemplo 4

Dado

$$U_0 = 1$$

$$U_1 = 0$$

$$U_n = 5 \cdot U_{n-1} - 6 \cdot U_{n-2}, \quad n \geq 2$$

Demoststrar $U_n = 3 \cdot 2^n - 2 \cdot 3^n \quad (n \in \mathbb{N}_0)$

a) Enunciado

La fórmula recursiva aplica para los $n \geq 2$, entonces con $\boxed{n=2}$

A demostrar

$$\boxed{n=2}$$

$$U_2 = 5U_{2-1} - 6U_{2-2}$$

$$U = 3 \cdot 2^2 - 2 \cdot 3^2$$

$$= 5U_1 - 6U_0$$

$$= 3 \cdot 4 - 2 \cdot 9$$

$$= 5 \cdot 0 - 6 \cdot 1 = \boxed{-6}$$

$$= 12 - 18 = \boxed{-6}$$

b)

Tomar para $k \geq 1$ para que $(k+1)$ sea ≥ 2 porque los U_0, U_1 ya estén demostrados.

$$U_h = 3 \cdot 2^h - 2 \cdot 3^h, \quad 0 \leq h \leq k \Rightarrow U_{k+1} = 3 \cdot 2^{k+1} - 2 \cdot 3^{k+1}$$

minimizamos que
muestra el
enunciado.

Como U_{k+1} es algún U_n entonces

$$U_{k+1} = 5(U_{(k+1)-1}) - 6(U_{(k+1)-2})$$

Def recursiva

$$= 5U_k - 6U_{k-1}$$

La hipótesis inductiva
varía entre $0 \leq h \leq k$,
entonces esa fórmula
la podemos aplicar con
estos subcinos

$$= 5(3 \cdot 2^k - 2 \cdot 3^k) - 6(3 \cdot 2^{k-1} - 2 \cdot 3^{k-1})$$

PP 428 Discrete
Maths

Un conjunto "A" es finito (es decir que se puede contar la cantidad de elementos que tiene) y tiene cardinal "n" si existe una función $f: \{1, \dots, n\} \rightarrow A$, que sea biyectiva.

Cardinal de un conjunto.

El cardinal de un conjunto "A" es la cantidad de elementos de "A" y su notación es: $|A|$.

$$\text{Si } A = \{0, 7, -2, 9\}, |A| = 4$$

Principio de Adición

Pg. 54 Discrete Maths

Dadas dos actividades "X" e "Y", si ambas se pueden realizar de "n" y "m" formas distintas respectivamente, entonces la cantidad de formas diferentes de realizar ambas actividades es " $n + m$ ".

Si "A" y "B" son conjuntos finitos disjuntos, entonces:

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

Definición formal general

Sean A_1, \dots, A_n conjuntos finitos tales que $\underbrace{A_i \cap A_j = \emptyset}_{\text{Disjuntos}}$, $i \neq j$, entonces:

$$|A_1, \dots, A_n| = |A_1| + \dots + |A_n|$$

Disjuntos pg. 34

Si no son disjuntos:

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

cuando son disjuntos
esto es cero ya que
 $A \cap B = \emptyset$, $|\emptyset| = 0$

Principio de Multiplicación

PPS27

Discrete
Maths

Si una actividad consiste de "K" etapas, la primera etapa se puede hacer en " n_1 " maneras y la segunda en " n_2 " maneras*, entonces toda la actividad se puede realizar en " $n_1 \cdot n_2 \cdot \dots \cdot n_K$ " maneras. * independiente de n_1

Dado el producto cartesiano $A \times B = \{(a, b) : a \in A, b \in B\}$

$$|A \times B| = |A| \cdot |B| = n_1 \cdot n_2 \cdot \dots \cdot n_K$$

cada conjunto
es una etapa

suponiendo que hay K conjuntos

Selecciones Ordenadas CON Repetición

A través del principio de multiplicación, afirmamos que siendo " n " y " m " $\in \mathbb{N}$, Hay " n^m " formas posibles* de elegir ordenadamente una cantidad " m " de elementos de un conjunto que tiene " n " elementos.

- m y n se pueden pensar como cardinales de un conjunto.

Conjunto Potencia

pp 346 Discrete Maths
369

Una aplicación de la selección ordenada con repetición es el conjunto potencia.

Dado un subconjunto "X" de "n" elementos, podemos averiguar cuantas subconjuntos posibles puede tener.

Se denota " $P(X)$ " el conjunto formado por todos los subconjuntos de "X".

$$P(X) = \{\emptyset, \{1\}, \{2\}, \{1, 2\}\} \quad \text{si } X = \{1, 2\}$$

$$\text{Si } X \text{ es finito, } |P(X)| = 2^{|X|}$$

Ejemplo:

$$X = \{a, b, c\}$$

Sea $A \subseteq X : a \in A \vee a \notin A \rightsquigarrow 2 \text{ posibilidades}$

$b \in A \vee b \notin A \rightsquigarrow 2 \text{ posibilidades}$

$c \in A \vee c \notin A \rightsquigarrow 2 \text{ posibilidades}$

Entonces hay " $2 \cdot 2 \cdot 2$ " posibilidades. Es decir $2^{|X|} = 2^3$

Se puede pensar que a cada elemento le asigna un cero si no pertenece, y un uno si si pertenece. $C = \{0, 1\}$, $|C| = 2$

$$|A| = |C|^{|X|}$$

Selecciones Ordenadas sin Repetición.

Pp 533 Discrete Maths

Dada una "m" cantidad de selecciones ordenadas sin repetición de una cantidad "n" de elementos:

Si $n > m$



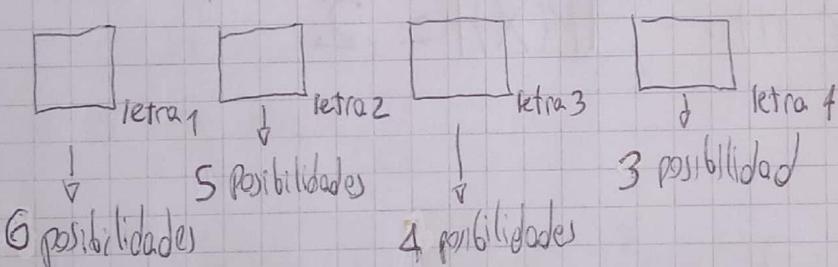
si $n < m$ es imposible no repetir

La cantidad de elecciones: $n \cdot (n-1) \cdot (n-2) \cdots (n-m+1)$ ó $\frac{n!}{(n-m)!}$

Ejemplo: ¿Cuántas palabras de 4 letras se pueden formar con $X = \{d, a, j, i, l\}$ sin repetir letras?

$$n=6$$

$$m=4$$



cantidad de factores

$$\frac{6 \cdot 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1}{2!}$$

$$\frac{6 \cdot (6-1) \cdot (6-2) \cdot (6-3)}{2!} = n \cdot (n-m+1)$$

Si $n=m$ → También cuando $n-m=1$, ya que $0!=1!$

$$\frac{n!}{(n-m)!} = \frac{n!}{0!} = n!$$

Definición de no Repetición

$A = \{a_{i_1}, a_{i_2}, \dots, a_{i_m}\}$, las selecciones son $a_{i_1} \cdot a_{i_2} \cdot a_{i_m}$ {donde $a_{i_j} \neq a_{i_k}$ si $i_j \neq k$ }

Selecciones Sin Orden Sin Repetición

Dado " $n=5$ " la cantidad de elementos de un conjunto "A", se precisa saber la cantidad de subconjuntos diferentes de " m " elementos del conjunto A.

Ejemplo: $A = \{1, 2, 3, 4, 5\}$, $|A|=n=5$

¿Cuántos subconjuntos de "A" con " m " elementos existen?

Si $m=3$, entonces:

$$\frac{n!}{(n-m)! \cdot m!} = \frac{5!}{2! \cdot 3!} = 10 = \binom{5}{3}$$

Se llaman sin orden porque precisamente el orden no altera los conjuntos. Elegir 321, es lo mismo que elegir 231, por lo tanto es un error contar los subconjuntos iguales.

Teorema

Sea " X " un conjunto de " n " elementos, entonces el número total de subconjuntos de " X " de " m " elementos es:

$$\frac{n!}{(n-m)! \cdot m!}$$

Número Combinatorio

pp. 238 Discrete Maths

Es una selección sin orden sin repetición.

Sean $n, m \in \mathbb{N}_0$, $n \geq m$:

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

Diagrama explicativo:

- Elementos totales del conjunto: n
- Elementos a elegir: m

Si $n=m$:

$$\binom{n}{m} = \frac{n!}{m!} = 1$$

Nros Combinatorios fácilmente calculables

$$\binom{n}{m} = 0 \quad \text{sii } m > n$$

$$\binom{n}{0} = \frac{n!}{(n-0)! 0!} = \frac{n!}{n! 0!} = \frac{n!}{n!} = 1$$

$$\binom{0}{0} = \frac{0!}{(0-0)! 0!} = \frac{1}{1 \cdot 1} = 1$$

$$\binom{n}{1} = \frac{n!}{(n-1)! 1!} = \frac{n!}{(n-1)!} = \frac{n \cdot (n-1) \cdot (n-2) \cdots}{(n-1) \cdot (n-2) \cdots} = n$$

$$\binom{n}{n-1} = \frac{n!}{(n-(n-1))! (n-1)!} = \frac{n!}{1! (n-1)!} = \binom{n}{1} = n$$

Ejemplo:

Dado 10 profesionales en el que 6 son mujeres & 4 son hombres, ¿cuántos comités pueden formarse con 4 mujeres & 2 hombres?

$$\text{Elegir 4 mujeres entre 6: } \binom{6}{4} = \frac{6!}{2!4!} = 15$$

$$\text{Elegir 2 hombres entre 4: } \binom{4}{2} = \frac{4!}{2!2!} = 6$$

Usando el principio de multiplicación:

$$\binom{6}{4} \cdot \binom{4}{2} = 15 \cdot 6 = 90$$

+ Simetría de número combinatorio:

$$\binom{n}{m} = \binom{n}{n-m} \quad m, n \in \mathbb{N}_0, \quad n \geq m$$

Demostración algebraica en el apunte pp. 33

+ Triángulo de Pascal

pp 593 Discrete Maths

$$\binom{n+1}{m} = \binom{n}{m-1} + \binom{n}{m} \quad m, n \in \mathbb{N}, \quad n \geq m$$

Demostración algebraica: apunte pp. 34

$$\begin{array}{c}
 \binom{0}{0} = 1 \\
 \binom{1}{0} \\
 \binom{1}{1} \\
 \binom{2}{0} \quad \binom{2}{1} \\
 \binom{2}{1} \quad \binom{2}{2} \\
 \binom{3}{0} \quad \binom{3}{1} \quad \binom{3}{2} \\
 \binom{3}{1} \quad \binom{3}{2} \quad \binom{3}{3} \\
 \binom{4}{0} \quad \binom{4}{1} \quad \binom{4}{2} \quad \binom{4}{3} \\
 \binom{4}{1} \quad \binom{4}{2} \quad \binom{4}{3} \quad \binom{4}{4}
 \end{array}$$

Teorema del Binomio de Newton.

pp 596 Discrete Maths

Sea "n" un entero positivo. El coeficiente del término " $a^{n-i} \cdot b^i$ " en el desarrollo de $(a+b)^n$ es el número binomial $\binom{n}{i}$:

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

Teorema del Binomio y Conjunto Potencia.

$$\sum_{i=0}^n \binom{n}{i} = \binom{n}{0} + \binom{n}{1} + \binom{n}{2} + \dots + \binom{n}{n} = 2^n$$

15/04/21

- Notemos que " n " es el cardinal del conjunto.
- Cada término es la cantidad de subconjuntos con " i " elementos de un conjunto de " n " elementos.
- La unión de todos los subconjuntos de " m " elementos es igual al conjunto de n elementos

Algoritmo de división

pp 180, 218

Sean a y b números enteros con $b \in \mathbb{N}$, entonces q y $r \in \mathbb{Z}$ únicos tales que:

$$a = b \cdot q + r \quad \text{y} \quad 0 \leq r < b$$

$\begin{matrix} \downarrow & \downarrow \\ \text{dividendo} & \text{cociente} \end{matrix}$

$\begin{matrix} \downarrow & \downarrow \\ \text{divisor} & \text{resto} \end{matrix}$

- Si $a=0$, sabiendo que $b \in \mathbb{N}$, tiene que haber un $q=0$ y un $r=0$
- Si $b>a \Rightarrow q=0 \wedge r=a$

Teorema

Todo número natural "x" se puede escribir de forma única:

$$x = \Gamma_n \cdot 10^n + \Gamma_{n-1} 10^{n-1} + \dots + \Gamma_1 \cdot 10^1 + \Gamma_0 \cdot 10^0$$

\downarrow

$0 \leq \Gamma_i < 10$

$\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$

20/04/21
22/04/21

Divisibilidad

pp 170

Dados dos enteros x e y , se dice que y divide a x si:

$$x = y \cdot q \quad \text{para algún } q \in \mathbb{Z}$$

Observaciones

- Si $y|x$, existe algún $q \in \mathbb{Z}$ tal que $x = y \cdot q$, entonces por commutatividad $q|x$ si $x \neq 0$.
- Si $y|x \wedge y \neq 0$ entonces $\frac{x}{y}$ es el cociente de x dividido y .

Propiedades ($a, b, c \in \mathbb{Z}$)

- $1|a$, $a| \pm a$
- $a|0$
- Si $a|b$, entonces $a|b \cdot c$ para cualquier c .
- Si $a|b \wedge a|c$, entonces $a|(b+c)$
- Si $a|b \wedge a|c \Rightarrow a|(\gamma \cdot b + \varsigma \cdot c)$, $\gamma, \varsigma \in \mathbb{Z}$
- Si $a|b+c \wedge a|c \Rightarrow a|b$

Proposiciones

- Sean $a, b \in \mathbb{N}$

$$a \cdot b = 1 \Rightarrow a = 1 \wedge b = 1$$

- Sean $a, b, c \in \mathbb{N}$

- $a | a$ (reflexividad)

- $a | b \wedge b | a \Rightarrow a = b$ (antisimetría)

- $a | b \wedge b | c \Rightarrow a | c$ (transitividad)

MCD

Si "a" y "b" son enteros algunos de ellos no nulos, decimos que un entero positivo "d" es el máximo común divisor de "a" y "b" si:

a) $d | a$ y $d | b$

b) Si $c | a$ y $c | b$ entonces $c | d$

→ No hay divisor común mayor que "d"

→ Cualquier divisor de "a" y "b" divide a "d"

• Se denota $\text{mcd}(a, b)$ ó $\text{gcd}(a, b)$ → (greatest common divisor)

Teorema (mcd Únicos)

Dados $a, b \in \mathbb{Z}$, alguno de ellos no nulo, existe un único $d \in \mathbb{Z}$ que es mcd.

Proposición (combinación lineal entera)

Sean $a, b \in \mathbb{Z}$, algunos de ellos no nulos, entonces existen $s, t \in \mathbb{Z}$ tal que:

$$\text{mcd}(a, b) = d = s \cdot a + t \cdot b$$

- El mcd de a, b es combinación lineal entera de a, b

Corolario (combinación lineal entera) (propiedad de coprimos)

Dados $a, b \in \mathbb{Z}$, $b \neq 0$ entonces:

$$(a, b) = 1 \iff \exists s, t \in \mathbb{Z} / 1 = s \cdot a + t \cdot b$$

Definición (coprimos)

Si $(a, b) = 1$ decimos que a, b son coprimos.

• En la factorización prima, los coprimos no tienen primos en común.

Proposiciones:

Proposición: $a, b \in \mathbb{Z}$ con $a \neq 0$:

- $\text{mcd}(a, b) = \text{mcd}(b, a) = \text{mcd}(\pm a, \pm b)$
- Si $a > 0$, $\text{mcd}(a, 0) = a$ y $\text{mcd}(a, a) = a$
- $\text{mcd}(1, b) = 1$

Propiedad (Importante)

Si $a \neq 0, b \in \mathbb{Z}$ entonces:

$$\text{mcd}(a, b) = \text{mcd}(a, b-a)$$

Proposición

Sean $a, b \in \mathbb{Z}$ no negativos y $b \neq 0$ entonces:

$$a = b \cdot q + r \Rightarrow \text{mcd}(a, b) = \text{mcd}(b, r)$$

Algoritmo de Euclides

Teorema

Sean a y $b \in \mathbb{Z}$ con $b > 0$, entonces el mcd es el último resto no nulo obtenido con el algoritmo de Euclides.

Para calcular el mcd de enteros a y b con $b > 0$ definimos q_i y r_i de la siguiente manera:

$$r_0 = a$$

$$r_1 = b$$

$$r_0 = r_1 \cdot q_1 + r_2 \quad (0 < r_2 < r_1)$$

$$r_1 = r_2 \cdot q_2 + r_3 \quad (0 < r_3 < r_2)$$

$$r_2 = r_3 \cdot q_3 + r_4 \quad (0 < r_4 < r_3)$$

...

$$r_{i-1} = r_i \cdot q_i + r_{i+1} \quad (0 < r_{i+1} < r_i)$$

$$r_{k-2} = r_{k-1} \cdot q_{k-1} + r_k \quad (0 < r_k < r_{k-1})$$

$$r_{k-1} = r_k \cdot q_k + 0$$

$$\Rightarrow r_k = \text{mcd}(a, b)$$

Mínimo Común Múltiplo

Si a y b son enteros decimos que un entero no negativo m es el mínimo común múltiplo de a y b si:

- a) $a|m$ y $b|m$ \rightarrow Es múltiplo común
- b) Si $a|n$ y $b|n$ entonces $m|n$ \rightarrow es múltiplo de m

Teorema

Sean a y b enteros no nulos:

$$\text{mcm}(a,b) = \frac{a \cdot b}{\text{mcd}(a,b)}$$

• Si son coprimos entonces $\text{mcm}(a,b) = a \cdot b$

Proposición

Sean n, a, b enteros no nulos entonces:

$$\text{mcd}(n \cdot a, n \cdot b) = n \cdot \text{mcd}(a, b)$$

Número Primo

Un entero positivo p mayor igual que dos es primo si los únicos enteros que dividen a p son 1 y p mismo.

P es primo si y solo si:

$$P = m_1 \cdot m_2 \Rightarrow m_1 = 1, m_2 = p \quad \text{o} \quad m_1 = p, m_2 = 1$$

M no es primo si:

• existen $m_1 > 1, m_2 < M$ tales que $M = m_1 \cdot m_2$

Teorema

Todo entero mayor que 1 es producto de números primos.

Propiedades

Dados $a \in \mathbb{Z}$ y p primo:

- Si $p \nmid a$ entonces $\text{mcd}(a, p) = 1$
- Si $p \nmid p'$ son primos y $p \mid p'$ entonces $p = p'$

Lema

Si $n > 0$ no es primo, entonces existe $m > 0$ tal que $m \mid n$ y $m \leq \sqrt{n}$

Proposición

Sea $n \geq 2$, si $\nexists m$ tal que $1 < m \leq \sqrt{n}$ se cumple que $m \nmid n$, entonces n es primo.

Corolario

Sea $n \geq 2$, si $\nexists p$ primo tal que $1 < p \leq \sqrt{n}$ se cumple que $m \nmid n$, entonces n es primo

Teorema

Sea P primo:

- a) Si $P|x, y$ entonces $P|x$ ó $P|y \rightarrow$ Solo ^{fuerza para} primos
- b) Dados $x_1, x_2, x_3, \dots, x_n$ enteros tales que $P|x_1 \cdot x_2 \cdot x_3 \cdots x_n$ entonces $P|x_i$ para algún $x_i (1 \leq i \leq n)$

Teorema

La factorización en primos de un entero positivo $n \geq 2$ es única, salvo por el orden de los factores.

$$n = p_1 \cdot p_2 \cdots p_n$$

No existen otros p_j primos que sean factores de n .

Congruencia

definición

Sean " a " y " b " enteros y " m " un entero positivo. Decimos que " a " es congruente a " b " módulo " m :

$$a \equiv b \pmod{m} \Leftrightarrow m | a - b$$

Notemos que:

- $a \equiv 0 \pmod{m} \iff m \mid a$
- $a \equiv b \pmod{m} \iff a - b \equiv 0 \pmod{m}$

Proposición:

Dado $a \in \mathbb{Z}, m \in \mathbb{Z}^+$:

$$a \equiv r \pmod{m} \iff a = m \cdot q + r$$

Propiedades

I) $a \equiv a \pmod{m}$ Reflexiva

II) $a \equiv b \pmod{m} \Rightarrow b \equiv a \pmod{m}$ Simétrica

III) $a \equiv b \pmod{m} \wedge b \equiv c \pmod{m} \Rightarrow a \equiv c \pmod{m}$ Transitiva

Teorema:

$$\text{Si } x_1 \equiv x_2 \pmod{m} \wedge y_1 \equiv y_2 \pmod{m}$$

Entonces:

a) $x_1 + y_1 \equiv x_2 + y_2 \pmod{m}$

b) $x_1 \cdot y_1 \equiv x_2 \cdot y_2 \pmod{m}$

c) Si $x \equiv y \pmod{m} \Rightarrow x^j \equiv y^j \pmod{m}, j \in \mathbb{N}$

Ecuación Lineal de Congruencia

$$a \cdot X \equiv b \pmod{m}, \quad x \in \mathbb{Z}$$

- Notemos que si $a \nmid b$, no hay solución.
- Si $a \mid b$, hay infinitas soluciones.
- Si X_0 es solución, entonces: $\boxed{X = X_0 + k \cdot m}, k \in \mathbb{Z}$

Teorema

Sean $a, b \in \mathbb{Z}$ y $m \in \mathbb{Z}^+$ y con $d = \text{mcd}(a, m)$ entonces:

$a \cdot X \equiv b \pmod{m}$ admite solución si $d \mid b$

y dado la solución X_0 , todas las soluciones son de la forma $X = X_0 + k \cdot n$ con $k \in \mathbb{Z}$ y $n = \frac{m}{d}$

11/05/21
13/05/21

Proposición:

Sean $a, b \in \mathbb{Z}$ y $m \in \mathbb{Z}^+$, $d > 0 / \text{dla, dlb, dlm}$:

$$ax \equiv b \pmod{m} \iff \frac{a}{d}x \equiv \frac{b}{d} \pmod{\frac{m}{d}}$$

Proposición

Dado: $a = m \cdot q_1 + r_1$, $a, q \in \mathbb{Z}$, $0 \leq r_1 < b$
 $b = m \cdot q_2 + r_2$, $b, q \in \mathbb{Z}$, $0 \leq r_2 < b$

Entonces:

$$a \equiv b \pmod{m} \iff r_1 = r_2$$

Lema

Sea p un número primo entonces:

a) $p \mid \binom{p}{r}$ con $0 < r < p$

b) $(a+b)^p \equiv a^p + b^p \pmod{p}$

Pequeño Teorema de Fermat

Sea p un número primo y $a \in \mathbb{Z}$ entonces:

$$a^p \equiv a \pmod{p}$$

Teorema

Sea a y p coprimos con p primo :

$$a^{(p-1)} \equiv 1 \pmod{p}$$

Grafo

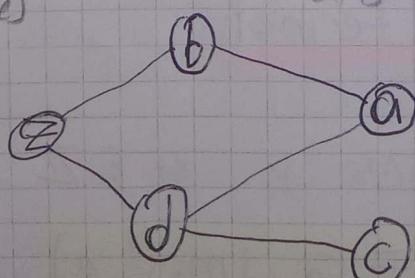
Definición (Grafo)

Un grafo G de un conjunto finito V , cuyos miembros son llamados vértices y un conjunto de elementos "2-subconjuntos" de V , cuyos miembros son llamados aristas.

Denotamos $G = (V, E)$

Ejemplo:

$$V = \{a, b, c, d, z\} \quad E = \left\{ \begin{array}{l} \{\underline{a}, \underline{b}\}, \{\underline{a}, \underline{d}\}, \{\underline{b}, \underline{z}\}, \{\underline{c}, \underline{d}\}, \{\underline{d}, \underline{z}\} \\ \text{arista} \quad \text{arista} \quad \text{arista} \quad \text{arista} \quad \text{arista} \end{array} \right\}$$



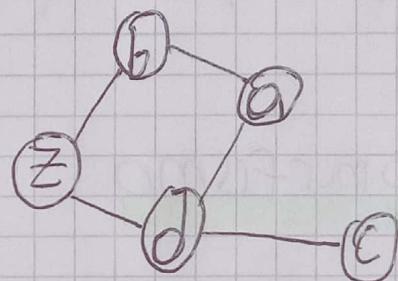
$$\circledast \quad \{a, b\} = \{b, a\}$$

Adyacencia

Dijemos que x e y de un grafo son adyacentes cuando $\{x, y\}$ es una arista.

Lista de adyacencia

a	b	c	d	z	Vertice
b	a	d	a	b	adyacencias
d	z	c	z	d	



Definición

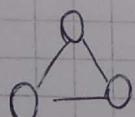
Definimos el grafo completo K_n , $n \in \mathbb{N}$, como el grafo con n vértices en el cual cada par de vértices es adyacente.

- K_1 ○

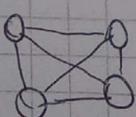
$$\text{Total Aristas} = \frac{K(K-1)}{2}$$

- K_2 ○—○

- K_3



- K_4



No importa el dibujo de un grafo ni el nombre de sus vértices para ver su equivalencia. La propiedad característica de los grafos es la manera en que los vértices están conectados.

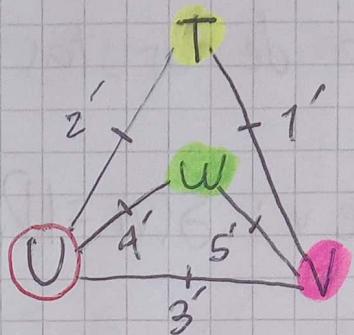
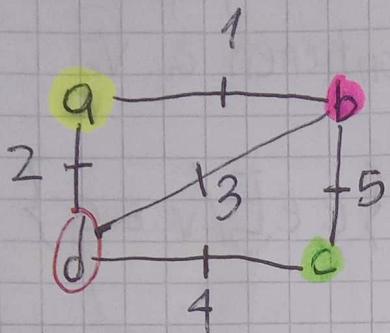
Es decir que dos grafos G_1 y G_2 son "iguales" si cambiando el nombre de los vértices de G_2 por el de los vértices de G_1 , en un cierto orden, obtenemos G_1 .

Isomorfismo

Dos grafos G_1 y G_2 se dicen que son isomorfos cuando existe una biyección α entre el conjunto de vértices de G_1 y el conjunto de vértices de G_2 tal que:

- Si $\{x, y\}$ es una arista de $G_1 \Rightarrow \{\alpha(x), \alpha(y)\}$ es una arista de G_2 y ...
- Si $\{z, w\}$ es una arista de $G_2 \Rightarrow \{\alpha^{-1}(z), \alpha^{-1}(w)\}$ es una arista de G_1 .

Ejemplo:



bijeción dada por: $\alpha(a)=T, \alpha(b)=V, \alpha(c)=W, \alpha(d)=U$

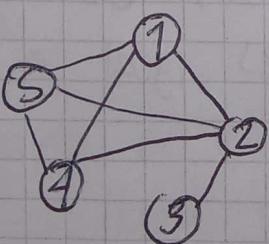
Subgrafo

Sea $G=(V,E)$ un grafo, se dice $G'=(V',E')$ es un subgrafo de G si:

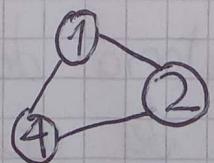
G' es un grafo y $V' \subseteq V, E' \subseteq E$

Ejemplos:

$G:$



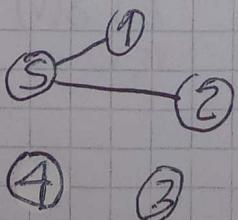
$G_1:$



$G_2:$



$G_3:$



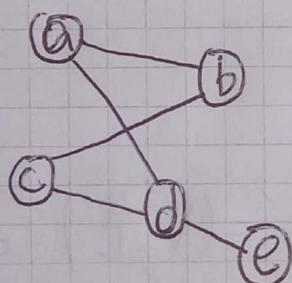
Valencias ó grado

pp 634

La valencia de un vértice v en un grafo $G = (V, E)$ es el número de aristas de G que contienen a v .

Valencia de v : $\delta(v) = |D_v|$ donde $D_v = \{e \in E / v \in e\}$

cardinal
conjunto formado por los
conjuntos aristas de un
vertice v .
conjunto de aristas
arista



$$\begin{aligned}\delta(a) &= 2 \\ \delta(b) &= 2 \\ \delta(c) &= 2 \\ \delta(d) &= 3 \\ \delta(e) &= 1\end{aligned}$$

Teorema

La sumatoria de las valencias $\delta(v)$ de todos los vértices v del grafo $G = (V, E)$ es igual a dos veces el número de aristas.

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

cardinal.
Lo conjunto de aristas

Teorema

El número de vértices impares, es par

explicación:

Un vértice es impar si su valencia es impar.

Denotando V_i , V_p tenemos que $V = V_i \cup V_p$ es una partición de V .

Luego:

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

$$\Rightarrow \underbrace{\sum_{v \in V_i} d(v)}_{\text{Par}} = 2|E| - \underbrace{\sum_{v \in V_p} d(v)}_{\text{Par}} \quad \text{Par} - \text{Par} = \text{Par} \Rightarrow \text{Par es par}$$

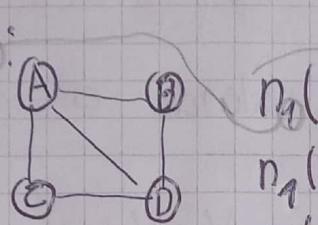
Observación

Un grafo en el cual todos sus vértices tienen la misma valencia Γ se llama regular con valencia Γ :

$$\Gamma |V| = 2|E|$$

Proposición (valencia y isomorfismo)

Sean G_1 y G_2 grafos isomorfos. Para cada $K \geq 0$ sea $n_i(K)$ el número de vértices de G_i que tienen valencia K (tomando $i=1,2$), entonces $n_1(K) = n_2(K)$

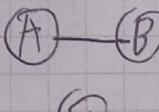
No Isomorfos: G_1 :  (cuanto tienen valencia 0?)

$$n_1(0) = 0$$

$$n_1(1) = 0$$

$$n_1(2) = 2$$

$$n_1(3) = 2$$

G_2 : 

$$n_2(0) = 1$$

$$n_2(1) = 2$$

$$n_2(2) = 0$$

Caminata

Una caminata en un grafo G es una secuencia de vértices

$$v_1, v_2, \dots, v_k$$

Tal que v_i y v_{i+1} son adyacentes ($1 \leq i \leq k-1$)

v_k no tiene un vértice adyacente que le sucede, si no que le precede.

Camino

Es una caminata en la que no se repiten los vértices. (consecutivamente temporalmente no se repite aristas)

Círculo

Es una caminata que empieza y termina en el mismo vértice.

11/06/21

Recorrido

Es una caminata donde todas las aristas son distintas.

Ciclo

Un ciclo es una caminata $V_1, V_2, \dots, V_k, V_1$ con V_1, V_2, \dots, V_k camino y $k \geq 3$. Es $V_i \sim V_{i+1}$, $i \in \mathbb{N}$

No se repiten vértices

Lema

Sea G un grafo, entonces x e y vértices pueden ser unidos por una caminata \Leftrightarrow pueden ser unidos por un camino.

Observación

$x \sim y$ significa que x e y pueden ser unidos por un camino en G con $x \neq y$. Es decir que existe un camino V_1, V_2, \dots, V_k en G con $x = V_1$ y $y = V_k$.

Definición (conexo)

Sea G grafo, diremos que es conexo si $x \sim y$ para cualesquiera x, y vértices en G

Proposición

Sea G grafo con x, y, z vértices de G :

(1) $x \sim x$ (reflexiva)

(2) Si $x \sim y \Rightarrow y \sim x$ (simétrica)

(3) Si $x \sim y \wedge y \sim z \Rightarrow x \sim z$ (transitividad)

Definición

Grados conexos

Un ciclo hamiltoniano es un ciclo que contiene a todos los vértices del grafo.

Una caminata euleriana es una caminata que usa todas las aristas del grafo exactamente una vez.

Un círculo euleriano es una caminata euleriana que empieza y termina en el mismo vértice.

Teoremas

- Un grafo conexo con más de un vértice tiene un círculo euleriano \Leftrightarrow todos los vértices del grafo tienen grado par
- Un grafo conexo con más de un vértice posee una caminata euleriana de V_1 a V_2 con $V_1 \neq V_2 \Leftrightarrow V_1 \wedge V_2$ son los

03/06/2021
08/06/21

Únicos vértices de grado impar.

Árbol

Un grafo T es un árbol si cumple que es conexo y no hay ciclos en T .

Lema

Sea $G = (V, E)$ un grafo conexo, entonces $|E| \geq |V| - 1$

Teorema

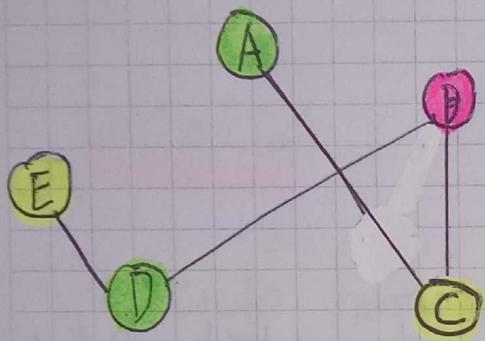
Sea T un grafo conexo con $|V| \geq 2$ las siguientes son equivalentes:

- I) T es un árbol
- II) Para cada par x, y de vértices existe un único camino de x a y en T .
- III) Al remover una arista cada componente es un árbol
- IV) $|E| = |V| - 1$

Cobreo

Una coloración de vértices de un grafo $G = (V, E)$ es una función $c: V \rightarrow \mathbb{N}$ con la siguiente propiedad:

$$c(x) \neq c(y) \quad \text{si } \{x, y\} \in E$$



Colores: $1 = \text{green}$, $2 = \text{red}$, $3 = \text{yellow}$

Función c

$$c(A) = c(D) = 1$$

$$c(B) = 2$$

$$c(C) = c(E) = 3$$

Número Cromático

Un número cromático de un grafo G , se denota como $\chi(G)$, es el mínimo entero K para el cual existe una coloración de vértices de G usando K colores.

Es decir que $\chi(G) = K \iff$ existe una coloración de vértices c la cual es una función de $V \rightarrow \mathbb{N}_K$ donde K es el mínimo entero con esta propiedad.

Observaciones:

- Sea G un grafo completo, entonces $K = |V|$

- Un ciclo con cantidad par de vértices $K=2$.
- Un ciclo con cantidad impar de vértices $K=3$.
- Sea G' un grafo completo de n vértices que es subgrafo de G , entonces $X(G) \geq n$.

Teorema

Si G es un grafo con valencia máxima K , entonces:

$$\text{I}) X(G) \leq K+1$$

$$\text{II}) \text{ Si } G \text{ es conexo no regular, } X(G) \leq K$$

Se utiliza el algoritmo de greedy para su demostración

Grafo Bipartito

Sea G grafo, es bipartito si $X(G)=2$

Teorema

Un grafo es bipartito \Leftrightarrow no tiene ciclos de longitud impar.

 tendría 3 colores.