Universidad Nacional de Córdoba
Facultad de Matemáticas, Astronomía, Física y Computación
FAMAF

Matemática Discreta I

Resúmen

Integrantes: Ayala Facundo
Bachmann Lautaro
Baudino Geremias
Canavesio Gonzalo
Collo Gastón
Lozano Benjamín

Profesor: Tiraboschi Leopoldo Alejandro

Índice de Contenidos

1. Números naturales **1**
1.1. Ordenando los enteros . . . 1
1.2. Definicion de cota inferior . . . 1
1.3. Definicion de minimo . . . 1
1.4. Axioma de buena ordenación(I12) . . . 1
1.5. Definiciones Recursivas . . . 2
1.5.1. Definición recursiva de sumatoria . . . 2
1.5.2. Definición recursiva de la productoria . . . 2
1.5.3. Definición recursiva de $n!$ . . . 2
1.5.4. Definición recursiva de x^n . . . 2
1.5.5. Propiedades de x^n . . . 3
1.6. El principio de inducción . . . 3
1.6.1. Enunciado del principio de inducción . . . 3
1.6.2. Enunciado del principio de inducción completa . . . 3

2. Conteo **4**
2.1. Definición del numero combinatorio . . . 4
2.2. Enunciado de la simetría del numero combinatorio . . . 4
2.3. Enunciado del Cálculo del número combinatorio por el triángulo de Pascal . . . 4
2.4. Enunciado del Teorema del Binomio . . . 5
2.5. Demostración $\sum_{i=0}^{n} \binom{n}{i} = 2^n$ . . . 5

3. Divisibilidad **6**
3.1. Enunciado del algoritmo de división . . . 6
3.2. 'Divide a' | . . . 6
3.2.1. Definición de 'divide a' . . . 6
3.2.2. Propiedades de 'divide a' | (con demostración, observación 3.2.2) . . . 6
3.3. Definición de máximo común divisor . . . 7
3.4. Definición de enteros coprimos . . . 8
3.5. Definición de mínimo común múltiplo . . . 8
3.6. Relación entre el Máximo Común Divisor y Mínimo Común Múltiplo (enunciado del Teorema 3.3.13) . . . 8
3.7. Definición de número primo . . . 9
3.8. Enunciado del criterio de la raíz (proposición 3.4.5) . . . 9
3.9. enunciado y demostración del Teorema 3.4.6.(a). . . . 9
3.10. Enunciado del teorema fundamental de la aritmética (enunciado del Teorema 3.4.7) . . . 10
3.11. Demostraciones: . . . 10
3.11.1. Demostración del Corolario 3.3.5 . . . 10
3.11.2. proposición 3.3.7, con demostraciones. . . . 11
3.11.3. Si a no nulo, entonces mcd(a, b) = mcd(a, b - a) (proposición 3.3.8) . . . 12

3.11.4. observación 3.4.3 . . . 12

4. Aritmética modular **13**
4.1. Definición de congruencia . . . 13
4.2. Propiedades de la congruencia ,enunciados y demostraciones . . . 13
4.2.1. Propiedad reflexiva . . . 13
4.2.2. Propiedad simétrica . . . 13
4.2.3. Propiedad Transitiva . . . 13
4.3. Enunciado sobre la existencia de soluciones en la ecuación lineal de congruencia (enunciado del Teorema 4.2.1) . . . 14
4.4. Teorema de Fermat (enunciado, teorema 4.3.2) . . . 14
4.5. Demostraciones . . . 15
4.5.1. Teorema 4.1.3 (a) . . . 15
4.5.2. Teorema 4.1.3 (b) . . . 15

5. Grafos **16**
5.1. Definición de grafo . . . 16
5.2. Definición de valencia . . . 16
5.3. Definición de caminata y camino . . . 16
5.4. Definición de ciclo . . . 16
5.5. Definición de ciclo hamiltoniano, caminata euleriana y circuito euleriano . . . 17
5.5.1. Ciclo hamiltoniano . . . 17
5.5.2. Caminata Euleriana y Circuito Euleriano . . . 17
5.6. Enunciado del teorema de existencia de caminatas eulerianas (enunciado del Teorema 5.4.7). 17
5.7. Definición de árbol . . . 18
5.8. Demostraciones . . . 18
5.8.1. La suma de las valencias de un grafo es dos veces el número de aristas (demostración del Teorema 5.3.1) . . . 18
5.8.2. Demostrar que el número de vértices impares de un grafo es par (demostración del Teorema 5.3.2) . . . 19

6. Complementario **19**
6.1. Conteo . . . 19
6.1.1. Principio de Adicion . . . 19
6.1.2. Principio de Multiplicacion . . . 20
6.1.3. Selecciones . . . 20
6.2. Divisibilidad . . . 21
6.2.1. Induccion en divisibilidad . . . 21
6.2.2. Euclides . . . 21
6.2.3. Combinacion Lineal Entera . . . 21
6.2.4. Como probar que un numero no es racional o que no existe un n tal que a·n^k=m^k 22
6.2.5. Resolver ejercicio de la forma 'Hallar el multiplo positivo mas pequeño de x! que es un cuadrado' . . . 22
6.3. Aritmetica Modular . . . 23

6.3.1. Encontrar los ultimos digitos . . . 23
6.3.2. Aplicacion de fermat . . . 23
6.3.3. Ecuacion lineal de congruencia . . . 24
6.4. Grafos . . . 25
6.4.1. Subgrafos . . . 25
6.4.2. Isomorfismo . . . 26
6.4.3. Como saber si dos grafos no son Isomorfos: . . . 26
6.4.4. Valencias . . . 27
6.4.5. Recorrido . . . 27
6.4.6. Circuito . . . 27
6.4.7. Conexidad . . . 27
6.4.8. Coloreo de vertices . . . 27

1. Números naturales

1.1. Ordenando los enteros

1.2. Definicion de cota inferior

Supongamos que X es un subconjunto de Z, entonces diremos que el entero b es una cota inferior de X si:

$$b \leq x \ para \ todo \ x \in X$$

1.3. Definicion de minimo

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

1.4. Axioma de buena ordenación(I12)

Es conocido como el axioma del buen orden o el principio de buena ordenacion.

El axioma dice que si X es un subconjunto de Z que no es vacio y tiene una cota inferior, entonces X tiene un minimo.

Ejemplo $10, 9, 8,$ **-7**, **-6**, $5, 4, 3, 2, 1, 0,$ **1**, **2**, **3**, $4, 5, 6, 7, 8, 9, 10$

Los elementos de nuestro conjunto están en negrita, el mínimo de nuestro conjunto es -7, pues $-7 < x$, $\forall x \in S$

1.5. Definiciones Recursivas

1.5.1. Definición recursiva de sumatoria

Sea n $\in$ N sean a_i para $1 \leq i \leq n$, una secuencia de números (reales, enteros, etc.). Entonces $\sum_{i=1}^{n} a_i$ denota la función recursiva definida

$$\sum_{i=1}^{1} = a_1,\ \sum_{i=1}^{n} a_i = \sum_{i=1}^{n-1} a_i + a_n (n \geq 2)$$

En este caso decimos que $\sum_{i=1}^{n}$ es la sumatoria de los a_i de i=1 a n.

1.5.2. Definición recursiva de la productoria

Sea n $\in$ N sean a_i para $1 \leq i \leq n$, una secuencia de números (reales, enteros, etc.). Entonces $\prod_{i=1}^{n} a_i$ denota la función recursiva definida

$$\prod_{i=1}^{1} a_i = a_1,\ \prod_{i=1}^{n} a_i = \prod_{i=1}^{n-1} a_i \cdot a_n\ (n \geq 2)$$

En este caso, decimos que $\prod_{i=1}^{n}$ es la productoria de los a_i de i=1 a n.

1.5.3. Definición recursiva de $n!$

Sea n $\in$ N, sean a_i para $1 \leq i \leq n$, una secuencia de números. En el caso de n! se puede definir como $\prod_{i=1}^{n}$ i, o bien como

$$0! = 1, \quad 1! = 1,\ n! = n \cdot (n-1)!\ (n \geq 2)$$

1.5.4. Definición recursiva de x^n

Sea x un número, si n $\in \mathbb{N}$, definimos

$$x^1 = x, \quad x^n = x \cdot x^{n-1}\ (n \geq 2)$$

1.5.5. Propiedades de x^n

Si n,m $\in$ N se cumplen las siguientes propiedades:

$$x^n \cdot x^m = x^{n+m}$$
$$(x^n)^m = x^{n \cdot m}$$

1.6. El principio de inducción

1.6.1. Enunciado del principio de inducción

Supongamos que S es un subconjunto de N que satisface las condiciones

a) 1 $\in$ S,

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

Entonces se sigue que S = N

1.6.2. Enunciado del principio de inducción completa

Supongamos que n_0 es cualquier entero (no necesariamente positivo) y sea $Z_{\geq n_0}$ el conjunto de enteros n tal que n $\geq$ n_0. Sea S un subconjunto de $Z \geq n_0$ que satisface las condiciones:

a) $n_0 \in S$

b) si h $\in$ S para todo h en el rango $n_0 \leq h \leq k$ entonces k+1 $\in$ S

Entonces se sigue que S = $Z_{\geq n_0}$

2. Conteo

2.1. Definición del numero combinatorio

Sean n,m $\in N_0$, m $\leq$ n. Definimos

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

y por razones que se verán mas adelante, se denomina el coeficiente binomial o numero combinatorio asociado al par n,m con m $\leq$ n.

Definimos también

$$\binom{n}{m} = 0,\ si\ m > n$$

2.2. Enunciado de la simetría del numero combinatorio

Sean m,n $\in N_0$, tal que m $\leq$ n. Entonces

$$\binom{n}{m} = \binom{n}{n-m}$$

2.3. Enunciado del Cálculo del número combinatorio por el triángulo de Pascal

Sean m,n $\in$ N, tal que m $\leq$ n. Entonces

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

2.4. Enunciado del Teorema del Binomio

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

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

O escrito de una forma mas concisa:

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

2.5. Demostración $\sum_{i=0}^{n} \binom{n}{i} = 2^n$

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

Observar que $1 + 1 = 2$ (Artificio), luego por el teorema del binomio,

$$\begin{aligned} 2^n = (1+1)^n &= \sum_{i=0}^{n} \binom{n}{i} 1^{n-i}1^i \\ &= \sum_{i=0}^{n} \binom{n}{i} 1 \cdot 1 \\ &= \sum_{i=0}^{n} \binom{n}{i} \end{aligned}$$

3. Divisibilidad

3.1. Enunciado del algoritmo de división

Sean a y b números enteros cualesquiera con b ∈ N, entonces existen enteros únicos q y r tales que:

$$a = b * q + r \ y \ 0 \leq r < b$$

3.2. 'Divide a' |

3.2.1. Definición de 'divide a'

Dados dos enteros x e y, decimos que y es un divisor de x, y escribimos y|x, si:

$$x = y * q \text{ para algún q} \in Z$$

También decimos que y es un factor de x, que y divide a x, que x es divisible por y, y que es múltiplo de y. Cuando y|x podemos usar el símbolo $\frac{x}{y}$(o x/y) para denotar al entero q tal que x = y*q. Cuando y no es un divisor de x tenemos que asignar un nuevo significado a la fracción x/y, puesto que este numero no es un entero. Es importante recordar que x/y no es un elemento de Z a menos que y divida a xź.

3.2.2. Propiedades de 'divide a' | (con demostración, observación 3.2.2)

Sean a, b y c ∈ Z

a) 1|a , a|0 , a| ±a;

Demostración

a = 1.a $\implies$ 1 | a

0 = a.0 $\implies$ a | 0

a = a.1 $\implies$ a | a

-a = a.(-1) $\implies$ a | -a

b) Si a|b, entonces a|bc para cualquier c;

Demostración

a | b $\implies$ ∃ q / b = a.q , entonces a | bc $\implies$ ∃ m / bc = a.m.c = a(m.c) $\implies$ a|bc

c) Si a|b y a|c, entonces a|(b + c) para cualquier c

Demostración

Si a|b entonces b = a.q ∧ si a|c entonces c = a.q'

Entonces a|(b+c) $\implies$ b+c = aq + aq' = a(q + q') $\implies$ a|(b+c)

d) Si a|b y a|c, entonces a|(r.b + s.c) para cualquiera r, s $\in Z$

Demostración

a | b y a | c $\implies$ b = a.q y c = a.q'

Entonces r.b + s.c = (r.a.q) + (s.a.q') = a.(r.q + s.q') $\implies$ a |(**r**.b + **s**.c)

3.3. Definición de máximo común divisor

Si a y b son enteros alguno de ellos no nulo, decimos que un entero no negativo d es un máximo común divisor, o mcd, de a y b si:

a) d|a y d|b;

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

La condición a) nos dice que d es un común divisor de a y b y la condición b) nos dice que cualquier divisor común de a y b es divisor también de d.

Ejemplo: 6 es un divisor común de 60 y 84, pero no es el mayor divisor común, porque 12|60 y 12|84 pero $12 \nmid 6$ (El símbolo significa no divide)

Los divisores positivos comunes de 60 y 84 son 1, 2, 3, 6 y 12 luego aunque 6 es un divisor común, no satisface b) de la definición, pues 12|60 y 12|84 pero $12 \nmid 6$. En este caso, 12 claramente es el máximo común divisor

3.4. Definición de enteros coprimos

Que un entero sea coprimo con otro entero, significa que no comparten factores primos, es decir que el unico divisor comun que tienen es el 1 o el -1. Con esto podemos confirmar que si el mcd(a,b) = 1, entonces decimos que a y b son coprimos

3.5. Definición de mínimo común múltiplo

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:

a) a|m y b|m;

b) si a|n y b|n entonces m|n

La condición a) nos dice que m es múltiplo común de a y b, y la condición b) nos dice que cualquier otro múltiplo de a y b también debe ser múltiplo de m.

3.6. Relación entre el Máximo Común Divisor y Mínimo Común Múltiplo (enunciado del Teorema 3.3.13)

Sean a y b enteros no nulos, entonces:

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

En particular este resultado implica que si a y b son enteros coprimos, entonces mcm(a,b) = a*b

Ejemplo: Encontrar el mcm (8,14)

Solucion: Es claro que mcd(8,14)=2, luego mcm(8,14) = $\frac{8 \cdot 14}{2} = 56$

3.7. Definición de número primo

Se dice que un entero positivo p es primo si p $\geq$ 2 y los únicos enteros positivos que dividen p son 1 y p mismo

Luego si un entero m $\geq$ 2 no es un primo si y solo si existe m_1 divisor de m tal que $m_1 \neq 1, m$ y por lo tanto $1 < m_2 < m$. Concluyendo,

Un entero m $\geq$ 2 no es un primo si y sólo si m $= m_1 * m_2$ *donde* m_1 *y* m_2 son enteros estrictamente entre 1 y m.

IMPORTANTE: 1 NO ES PRIMO

3.8. Enunciado del criterio de la raíz (proposición 3.4.5)

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

3.9. enunciado y demostración del Teorema 3.4.6.(a).

Sea p un numero primo:

a) Si p|xy entonces p|x o p|y

b) $x_1, x_2, ..., x_n$ son enteros tales que

$$p \mid x_1 x_2 ... x_n$$

entonces p|x_i para algun x_i (1 $\leq$ i $\leq$ n).

Demostración del a: Si p|x ya esta probado el resultado. Si p$\nmid$x entonces tenemos mcd(x,p) = 1. Por la proposición 3.4.4 (Si n>0 no es primo, entonces existe m>0 tal que m|n y m $\leq \sqrt{n}$) existen enteros r y s tales que rp + sx = 1. Por lo tanto tenemos

$$y = 1 \cdot y = (rp + sx)y = (ry)p + s(xy)$$

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

3.10. Enunciado del teorema fundamental de la aritmética (enunciado del Teorema 3.4.7)

La factorización en primos de un entero positivo ≥ 2 es única, salvo el orden de los factores primos

3.11. Demostraciones:

3.11.1. Demostración del Corolario 3.3.5

Para explicar esto necesitamos apoyarnos de la proposición 3.3.4, que dice "Sean a,b $\in$ Z, alguno de ellos no nulo. Entonces existen s,t $\in$ Z tal que

$$(a, b) = sa + tb$$

Corolario 3.3.5: Sean a y b enteros, b no nulo, entonces

$$(a, b) = 1 \iff \text{existen s, t} \in \text{Z tales que } 1 = \text{sa + tb}$$

Demostración($\Longrightarrow$) Es consecuencia trivial de la proposición 3.3.4. ($\longleftarrow$) sea d= (a,b), entonces d|a y d|b y por lo tanto d|sa + tb para cualesquiera s,t $\in$ Z. En particular, la hipótesis que implica d|1 y, en consecuencia d=1

3.11.2. proposición 3.3.7, con demostraciones.

La siguiente propiedad no es tan obvia y resulta muy importante:

$$Si\ a \neq 0,\ b \in Z,\ entonces\ mcd(a, b) = mcd(a, b - a)$$

Demostracion: Sea d= mcd(a,b), luego

(a)d|a y d|b y (b) si c|a y c|b, entonces c|d

Probemos que:

(a') d|a y d|b-a y (b') Si c|a y c|b-a $\longrightarrow$ c|d

Sean a,b enteros con a$\neq$ 0, entonces

1) mcd(b,a) = mcd(a,b) = mcd $(\pm a, \pm b)$,

Demostracion 1):por a) d|a y d|b $\longrightarrow$ d|ba $\longrightarrow$ (a')

2) Si a > 0, mdc(a,0) = a, y mcd(a,a) = a,

Demostracion 2): Si c|a, y c|b-a $\longrightarrow$ c|a+(b-a)=b $\longrightarrow$ c|d $\longrightarrow$ (b')

3) mcd(1,b) = 1

Demostración 3): Comprobamos que 1 cumple con la definición:

a) 1|1 y 1|b

b) Si c|1 y c|b entonces c|1

Propiedades que obviamente son verdaderas

3.11.3. Si a no nulo, entonces mcd(a, b) = mcd(a, b - a) (proposición 3.3.8)

Si a $\neq$0, b $\in$ Z, entonces mcd(a,b) = mcd(a,b-a).

Demostración. Sea d=mcd(a,b-a), luego

a) d|a y d|b-a;

b) si c|a y c|b-a, entonces c|d.

Ahora bien, como d|a y d|b-a, entonces d|a + (b-a) = b. Es decir, para recalcar

a') d|a y d|b.

Por el otro lado, si c|a y c|b, entonces c|b-a, luego por b) tenemos c|d. Es decir

b') Si c|a y c|b, entonces c|d

Luego, por definición de mcd, obtenemos que d = mcd(a,b).

3.11.4. observación 3.4.3

Sea a $\in$ Z y p primo. Entonces

a) p$\nmid$a, entonces mcd(a,p)=1

b) Si p y p' son primos y p|p' entonces p = p'.

Demostración:

a) Como los únicos divisores de p son p y 1, p $\nmid$a, el único divisor común de p y a es 1

p' es primo, por lo tanto tiene solo dos divisores positivos 1 y p'. Como p no es 1, tenemos que p=p'.

4. Aritmética modular

4.1. Definición de congruencia

Sean a y b enteros y m un entero positivo. Diremos que a es congruente a b módulo m, y escribimos

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

Si a-b es divisible por m

Observar que $a \equiv 0$ (mód m) si y sólo si m|a y que $a \equiv b$ (mód m) si y sólo si a-b $\equiv$ 0 (mód m)

4.2. Propiedades de la congruencia ,enunciados y demostraciones

4.2.1. Propiedad reflexiva

Es reflexiva, es decir x $\equiv$ x (mód m)

Demostracion: Esta propiedad se debe a que x-x es cero, por lo tanto es cero y eso implica que es divisible por m

4.2.2. Propiedad simétrica

Es simetrica, es decir si x $\equiv$ y (mód m), entonces y $\equiv$ x (mód m)

Demostracion: Esta propiedad se debe a que si x-y = k*m, entonces y-x = (-k)*m.

4.2.3. Propiedad Transitiva

Es transitiva, es decir, Si x $\equiv$ y (mód m) e y $\equiv$ z (mód m), entonces x $\equiv$ z (mód m)

Demostración: Esta propiedad se debe a que, puesto que x-y = k*m e y-z = l*m, tenemos que x-z = (x-y) + (y-z) = (k+1)*m

4.3. Enunciado sobre la existencia de soluciones en la ecuación lineal de congruencia (enunciado del Teorema 4.2.1)

Sean a,b números enteros y m un entero positivo y denotemos d= mcd(a,m). La ecuación:

$$ax \equiv b \ (mod\ m)$$

Admite solución si y solo si d|b, y en este caso dada x_0 una solución, todas las soluciones son de la forma

$$x = x_0 + kn, \ con\ k\ \in Z\ y\ n = \frac{m}{d}$$

4.4. Teorema de Fermat (enunciado, teorema 4.3.2)

Sea p un número primo y a un número entero. Entonces:

$$a^p \equiv a \ (mod\ p)$$

4.5. Demostraciones

4.5.1. Teorema 4.1.3 (a)

Enunciado: $x_1 + y_1 \equiv x_2 + y_2$ (mód m)

Demostración: 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.

4.5.2. Teorema 4.1.3 (b)

Enunciado: $x_1y_1 \equiv x_2y_2$ (mód m)

Demostración: por hipótesis tenemos que existen enteros x,y tales que x_1 - x_2 = mx e $y_1 - y_2$ = my.

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

Y por consiguiente el lado izquierdo es divisible por m, como buscamos demostrar

5. Grafos

5.1. 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.

5.2. Definición de valencia

La valencia o grado de un vértice v en un grafo G = (V,E) es el número de aristas de G que contienen v . Usaremos la notación δ(v) para la valencia de v, formalmente

δ(v) = | D_v |, donde $D_v = \{e \in E \mid v \in e\}$

5.3. Definición de caminata y camino

Una caminata en un grafo G es una secuencia de vértices

$$v_1, v_2, ..., v_k,$$

tal que v_i y v_{i+1} son adyacentes (Quiere decir que están conectados mediante una arista) $(1 \leq i \leq k-1)$. Si todos los vértices son distintos, una caminata es llamada camino.

Es decir una caminata especifica una ruta en G: del primer vértice vamos a uno adyacente, de este a otro adyacente y así siguiendo. En una caminata podemos visitar cualquier vértice varias veces, y en particular, podemos ir de un vértice x a otro y luego tomar la dirección contraria y regresar a x. Mientras que en un camino, cada vértice es visitado solo una vez

5.4. Definición de ciclo

Llamaremos ciclo a una caminata v_1,v_2,...,v_{r+1} con r $\leq$ 3 y cuyos vértices son distintos exceptuando los extremos, es decir que v_1,v_2,...,v_r es un camino de al menos tres vértices y $v_1 = v_{r+1}$. A menudo diremos que es un r-ciclo o un ciclo de longitud r en G

5.5. Definición de ciclo hamiltoniano, caminata euleriana y circuito euleriano

5.5.1. Ciclo hamiltoniano

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

5.5.2. Caminata Euleriana y Circuito Euleriano

Una caminata euleriana en un grafo G es un 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.

5.6. Enunciado del teorema de existencia de caminatas eulerianas (enunciado del Teorema 5.4.7).

Un grafo conexo con más de un vértice posee una caminata euleriana de v a w, con v≠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.

5.7. Definición de árbol

Diremos que un grafo T es un árbol si T es conexo y no hay ciclos en T

Si T = (V, E) es un grafo conexo con al menos dos vértices, entonces son equivalentes las siguientes propiedades y puede utilizarse para definir un árbol:

T1) T es un árbol (T es conexo y no hay ciclos en T)

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

Debemos demostrar que T1 $\iff$ T2 $\iff$ T3 $\iff$ T4

Pero solo con demostrar T1 $\longrightarrow$ T2 $\longrightarrow$ T3 $\longrightarrow$ T4 queda demostrado todo

5.8. Demostraciones

5.8.1. La suma de las valencias de un grafo es dos veces el número de aristas (demostración del Teorema 5.3.1)

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

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 colorario 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 el teorema de que la suma de los valores de las valencias tomados sobre todos los vértices v del grafo G = (V,E), es igual a dos veces el numero de aristas, tenemos que:

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

5.8.2. Demostrar que el número de vértices impares de un grafo es par (demostración del Teorema 5.3.2)

Existe un colorario de este resultado. Diremos que un vertice 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 vertices impares y pares respectivamente, luego $V = V_i \cup V_p$ es una particion de V. Por el teorema 5.3.1 (La suma de los valores de las valencias, tomados sobre todos los vertices v del grafo G=(V,E), es igual a dos veces el numero de aristas), tenemos que:

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

Ahora cada termino en la segunda suma es par, luego esta suma es un numero par. Puesto que el lado derecho tambien es un numero par, la primera suma tambien debe ser par. Pero la suma de numeros impares solo puede ser par si el numero de terminos es par. En otras palabras:

Un grafo en el cual todos los vertices tienen la misma valencia r se llama regular(Con valencia r), o r-valente, o de grado r. En este caso, el resultado del teorema 5.3.1 se traduce a:

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

6. Complementario

6.1. Conteo

6.1.1. Principio de Adicion

Se puede realizar una acción A de n formas distintas o, alternativamente, se puede realizar otra acción B de m formas distintas.

Entonces el número de formas de realizar la acción A o B es n + m.

Ejemplo de cuando usar Adicion:

Supongamos que alguien quiere salir a dar una vuelta, y solo puede elegir un lugar donde pasear, como primer opcion tiene el cine, donde hay 3 peliculas, o como segunda opcion tiene el teatro donde hay 4 obras posibles.

Entonces, esta persona tendra un total de 3 (Cine) + 4 (Teatro) = 7 (Opciones totales) formas distintas de elegir el paseo. Recordemos solo puede elegir 1 opcion, no pueden ocurrir en simultaneo.

6.1.2. Principio de Multiplicacion

En este caso, supongamos que una actividad consiste de 2 etapas, la primer etapa podra ser realizada de n_1 maneras y la segunda etapa de n_2 maneras, independientemente de como sucedio la primer etapa.

Entonces toda la actividad puede ser realizada de $n_1 \cdot n_2$ formas distintas

Ejemplo: Ahora supongamos, que la persona anterior puede darse el gusto de ir a ambos lugares, primero al cine y luego al teatro. Entonces va a tener 3 (Formas de las que puede suceder ir al cine) · 4 (Formas de las que puede suceder ir al teatro) = 12 formas diferentes de hacer el paseo.

6.1.3. Selecciones

Seleccion Ordenada con repeticion

Supongamos que nos interesa el orden y que se pueda repetir los elementos, Entonces la formula es: $m \cdot m \cdot m \cdot m.....m = m^n$ con n las veces que se repita el elemento.

Ejemplo: Teniendo en cuenta que hay 26 letras y 10 dígitos, Una contraseña de longitud n es una palabra formada por n caracteres. Cuántas contraseñas de longitud 11 es posible hacer?

La solucion es (26 + 10 (cantidad total de elementos))^{11}, donde 11 es la cantidad de veces que se repiten los elementos.

Seleccion Ordenada Sin repeticion

Si n $\geq$ m entonces existen $\frac{n!}{(\mathrm{n}\ \ \mathrm{m})!}$ = n · (n 1)...(n (m 1)) selecciones ordenadas y sin repetición de m elementos de un conjunto de n elementos

Seleccion Sin orden y Sin repeticion

Sean n, m $\in N_0$, m $\leq$ n y supongamos que el conjunto X tiene n elementos. Entonces, la cantidad de subconjuntos de X con m elementos es $\binom{n}{m} = \frac{n!}{(\mathrm{n}\ \ \mathrm{m})! \cdot m!}$

Repeticiones

Se permutan todos los caracteres involucrados en la palabra que debemos ordenar y se divide por el factorial de la cantidad de repeticiones del elemento n_1 multiplicado por la cantidad de repeticiones del elemento n_2: $\frac{n!}{n_1! \cdot n_2! \cdot n_3!}$
Tomemos la palabra *ramanathan*, el número total de permutaciones es $\frac{10!}{4!\text{ů}2!}$

Mesa redonda

El número total de permutaciones se disminuye en n, ya que existen n repeticiones las cuales solo "giran"la mesa, pero a los lados las personas siguen teniendo a las mismas personas.

Entonces, las permutaciones con mesa redonda son $(n-1)!$

6.2. Divisibilidad

6.2.1. Induccion en divisibilidad

Cuando vayamos a hacer induccion sobre una propiedad de divisibilidad, tenemos que tener en cuenta las diferencias con la induccion normal. Nosotros sabemos que un entero b es divisible por a si ∃q tal que b = aq. Entonces nosotros tenemos que buscar que aq = b basicamente, y luego comprobar que existe un m tal que am = b evaluado en k+1.

Ejemplo: Supongamos que nos piden probar que $3^{2n+2} + 2^{6n+1}$ es multiplo de 11, nuestra H.I va a ser buscar que Existe un q tal que 11q = $3^{2(k)+2} + 2^{6(k)+1}$ y vamos a tener que demostrar en k+1: que existe un m tal que 11m=$3^{2(k+1)+2} + 2^{6(k+1)+1}$

6.2.2. Euclides

Supongamos que nos piden encontrar el mcd entre dos numeros, el algoritmo mas efectivo es el de euclides, en que consta? Vamos a dividir el mayor, por el menor, luego vamos a buscar el mcd entre el menor y el resto de la division, hasta llegar a un (a,0) Ejemplo:

(7469, 2464), La division es: 76469 = 2464 · 3 + 77, luego calculamos el mcd(2464,77) y asi hasta llegar a (a,0)

6.2.3. Combinacion Lineal Entera

Sean a, b ∈ Z, alguno de ellos no nulo. Entonces existen s, t Z tal que:

$$(a, b) = sa + tb$$

Partiendo del mcd, cambiando los valores de las formulas por los restos podemos llegar a la combinacion lineal sa + tb.

6.2.4. Como probar que un numero no es racional o que no existe un n tal que a$\cdot n^k$=m^k

Aca nosotros lo que tenemos que buscar, si nos dan una raiz, primero es hacer que esa raiz sea una ecuacion de la forma a$\cdot n^k = m^k$, luego de eso, tenemos que descomponer todo en primos, para ver si la descomposicion es igual o no, es decir, si n tiene un exponente no divisible por k, entonces por el teorema fundamental de aritmetica que dice que la factorizacion en primos es unica, sabemos que no existe tal numero.

En otras palabras, si la factorizacion en primos de la izquierda tiene exponentes diferentes o no divisibles por k, no existe tal numero, ya que por el TFA, sabemos que la descomposicion es unica.

6.2.5. Resolver ejercicio de la forma 'Hallar el multiplo positivo mas pequeño de x! que es un cuadrado'

Bueno, en este tipo de ejercicios hay un truquito, a simple vista no se nota, supongamos que buscamos el multiplo positivo mas pequeño de 5! que a su vez, es un cuadrado. Bueno, este numero es 120, por lo que nosotros tenemos que buscar un x tal que 120*x=y^2.

Si descomponemos el 120, tenemos que $120 = 2^3 \cdot 3 \cdot 5$, £Que podemos notar de la ecuacion anterior ahora que sabemos esto? Que si descomponemos a y^2, todos sus primos tienen exponentes cuadrados, entonces lo que deberiamos hacer, es que nuestra x nos lleve a que nos queden todos exponentes cuadrados en la descomposicion de la izquierda.

Entonces: $2^3 \cdot 3 \cdot 5 \cdot 2 \cdot 3 \cdot 5 = y^2$.

6.3. Aritmetica Modular

6.3.1. Encontrar los ultimos digitos

Para encontrar los ultimos dos digitos, lo que tenemos que hacer es ir desmenuzando la potencia del numero en cuestion, hasta llegar al numero buscado, por ejemplo:

$2^{338} \equiv 2^{330} \cdot 2^8 \ (mod\ 100)$

$2^{330} \cdot 2^8 \equiv (2^{22})^{15} \cdot 2^8 \equiv (4)^{15} \cdot 2^8 \equiv (2^2)^{15} \cdot 2^8 \ (mod\ 100)$

$2^{30} \cdot 2^8 \equiv 2^{22} \cdot 2^{16} \equiv 4 \cdot 2^{16} \equiv 2^2 \cdot 2^{16} \equiv 2^{18} \ (mod\ 100)$

$2^{18} \equiv (2^9)^2 \equiv (512)^2 \equiv (500+12)^2 \equiv 12^2 \ (mod\ 100)$

$12^2 \equiv 144 \equiv (100+44) \equiv 44 \ (mod\ 100)$

Entonces, los ultimos dos digitos son 44.

6.3.2. Aplicacion de fermat

Como aplicar fermat? Bueno, primero tenemos que ver que p (primo del mod) no divida a a, y ahi podemos aplicar que $a^{p-1} \equiv 1$. Pero para que nos serviria esto? Bueno, nos ahorra muchisimos pasos y nos hace tener una referencia. Aca dejo un ejemplo de como usar el Corolario.

Encontrar el resto de 3^{3490} por 17 mediante fermat.

1)Veamos que 3 y 7 son coprimos, lo cual es verdad ya que son primos.

2)Aplicamos el corolario de fermat $3^{16} \equiv 1(17)$

3)Descomponemos el 3490 en una div por 16

$$3490 = 16 \cdot 218 + 2$$

4)Con la ayuda del corolario y la descomposicion, podemos resolverlo una congruencia normal.

$$3^{3490} \equiv (3^{16})^{218} \cdot 3^2 \equiv 1^{218} \cdot 3^2 \equiv 3^2 \equiv 9\ (17)$$

Entonces el resto de la division es 9.

6.3.3. Ecuacion lineal de congruencia

Existe un metodo general para encontrar soluciones de la ecuacion lineal de congruencia

$$ax \equiv b \ (mod \ m)$$

con mcd(a,m)|b

a) Encontrar, usando el algoritmo de Euclides, r,s tales que

$$\text{d = mcd(a,m) = ra + sm}$$

b) Como d|b, tenemos que b = td y multiplicamos la ecuacion anterior por t:

$$dt = (rt)a + (st)m$$

c) b = dt = (rt)a + (st)m ≡ (rt)a (mod m). Luego x_0 = rt es solucion de la cuacion lineal de congruencia.

d) Toda solucion de la ecuacion lineal de congruencia es x = x_0 + k($\frac{m}{d}$) con k ∈ Z

Ejemplo: Hallemos las soluciones de la ecuacion $13x \equiv 7 \pmod{15}$ con $0 \leq x < 15$.

a) Usando Euclides obtenemos el mcd(13,15).

$$15 = 3 \cdot 1 + 2$$

$$13 = 2 \cdot 6 + 1$$

$$2 = 1 \cdot 2 + 0$$

Luego 1= mcd(13,15). Como 1 divide a cualquier numero, en este caso la ecuacion tiene solucion. Del algoritmo de Euclides deducimos la Combinacion Lineal

$$1 = 13 - 2 \cdot 6 = 13 - (15 - 13) \cdot 6$$

$$= 13 \cdot 7 - 15 \cdot 6$$

Es decir, $1 = 13 \cdot 7$ - $15 \cdot 42$

b) Multiplicando la ecuacion obtenida por 7, obtenemos

$$7 = 13 \cdot 49 - 15 \cdot 42$$

Luego $13 \cdot 49 \equiv 7$, es decir 49 es solucion de la ecuacion.

d) Todas las soluciones son de la forma x = 49 + 15k

Para encontrar las soluciones en el intervalo $0 \leq x < 15$ se hace tanteando (por prueba y error) Hasta encontrar las soluciones, no hay un algoritmo ni nada. En este caso la unica x que cumple es 4, y su k es -3.

6.4. Grafos

6.4.1. Subgrafos

Sea G = (V, E) un grafo. Se dice que G' = (V', E') es subgrafo de G = (V, E) si V' $\subset$ V, E' $\subset$ E y todos los vértices que son extremos de las aristas de E' están en V'

• Un vertice solito es un subgrafo

• Con dibujitos uno no se confunde, pero con pares y listas de adyacencias es más fácil meter la pata y que el subgrafo no sea realmente un grafo debido a que algún vértice que participe en las aristas de del subgrafo no se encuentre entre los vértices incluidos en el subgrafo.

6.4.2. Isomorfismo

Si G_1 y G_2 son isomorfos, existe una función $f : v_1 \to v_2$ biyectiva, tal que

• Si $\{x, y\}$ es una arista de $G_1 \Rightarrow \{f(x), f(y)\}$ es una arista de G_2

•Recíprocamente, si $\{z, w\}$ es una arista de $G_2 \Rightarrow \{f^1(z), f^{-1}(w)\}$ es una arista de G_1, Esto porque es una función biyectiva y existe la inversa

Vamos a considerar que G_1 y G_2 son isomorfos si cambiando el nombre de los vértices de G_2 por el de los vértices de G_1, en cierto orden, obtenemos G_1.

Equivalentemente, diremos que f es un isomorfismo si es una biyección entre el conjunto de vértices de G_1 y el conjunto de vértices de G_2 tal que por cada $\{z, w\}$ arista de G_2, existe una y solo una $\{x, y\}$ arista de G_1 tal que $\{f(x), f(y)\} = \{z, w\}$

Si dos grafos son isomorfos, diremos que son el mismo grafo.

6.4.3. Como saber si dos grafos no son Isomorfos:

Para mostrar que dos grafos no son isomorfos, debemos demostrar que no hay una biyección entre el conjunto de vértices de uno con el conjunto de vértices de otro, que lleve las aristas de uno en las aristas del otro.

• Si G_1 y G_2 tienen diferente número de vértices, no son isomorfos

• Si G_1 y G_2 tienen diferente número de aristas, no son isomorfos

• Si hay un subgrafo en G_1 el cual no tiene un subgrafo isomorfo G_2, entonces G_1 y G_2 no son isomorfos

• Si la cantidad de vértices con valencia k en G_1 no es igual a la cantidad de vertices con valencia k en G_2 entonces G_1 y G_2 no son isomorfos

•Si el grafo complemento de G_1 no es isomorfo al grafo complemento de G_2, entonces G_1 y G_2 no son isomorfos

• Si el grafo complemento de G_1 no es isomorfo al grafo complemento de G_2, entonces G_1 y G_2no son isomorfos

• No hay ningún criterio general eficiente para determinar si dos grafos son isomorfos: la única manera de demostrarlo es con la definición, lo que significa encontrar una función biyectiva entre sus vértices

6.4.4. Valencias

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

• En lista de adyacencias, sería la cantidad de elementos que tiene la columna de ese vértice

• Diremos que un vértice de G es impar si su valencia es impar, y par si su valencia es par.

6.4.5. Recorrido

• Un recorrido es una caminata que puede repetir vértices pero no repite aristas

• Un recorrido maximal es un recorrido que no es posible continuar sin repetir aristas (Quedas "trabado.ªl final del recorrido)

• Un recorrido maximal es un recorrido que no es posible continuar sin repetir aristas (Quedas "trabado.ªl final del recorrido)

6.4.6. Circuito

Un circuito es un ciclo pero que si puede repetir vértices y aristas

6.4.7. Conexidad

Sea G grafo, diremos que es conexo si x y para cualesquiera x, y vértices en G (es un grafo en que todos sus vértices están conectados con los otros vertices por un camino)

Sea G grafo, diremos que es conexo si x y para cualesquiera x, y vértices en G (es un grafo en que todos sus vértices están conectados con los otros vertices por un camino)

6.4.8. Coloreo de vertices

Esto se basa en que los vértices que son adyacentes en el grafo deben tener diferentes colores

Sea G grafo. Diremos que G es bipartito si (G) = 2(G)=2. Es decir, si se puede colorear con dos colores (Su número cromático es 22)