**DOMANDE BRENTI**

- Prodotto Cartesiano:

è l’insieme di A x B di tutte le coppie ordinate (a, b) dove a appartiene ad A e b appartiene a B.

Le parti di A sono degli insiemi che a loro volta sono sottoinsiemi di A

- Cos'è una funzione:

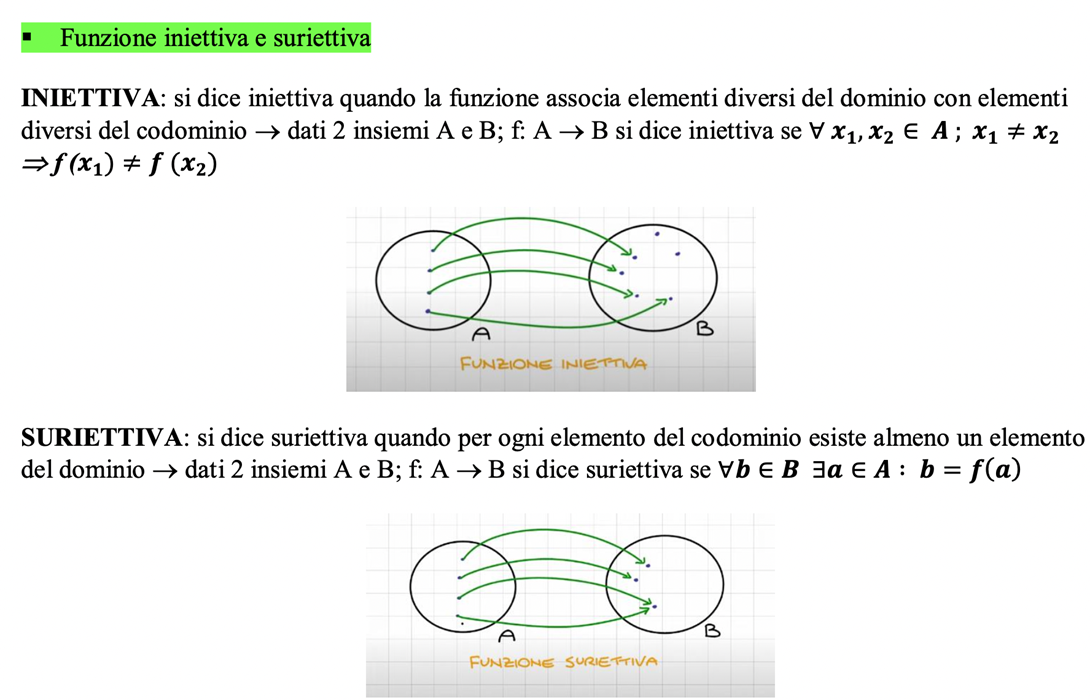
Siano A, B insiemi, una funzione f da A in B è un sottoinsieme f sottoinsieme di A x B, tale che ad ogni elemento di A associa uno e un solo elemento di B.

- Quando una funzione si dice suriettiva:

Per ogni elemento del codominio esiste almeno un elemento del dominio

- Quando una funzione si dice iniettiva:

f è suriettiva se x, y appartiene ad A e x diverso da y, quindi f(x) diverso f(y)



- Quando una funzione si dice biunivoca:

Quando f è sia iniettiva che suriettiva

- Cos'è l'immagine di una funzione:

?

- Cos'è la Controimmagine di una funzione:

?

-Cos’è la composizione di una funzione:

(g o f) (a): = g(f(a))

- Cos'è l'identità di una funzione:

è la funzione che associa ad ogni elemento l’elemento stesso

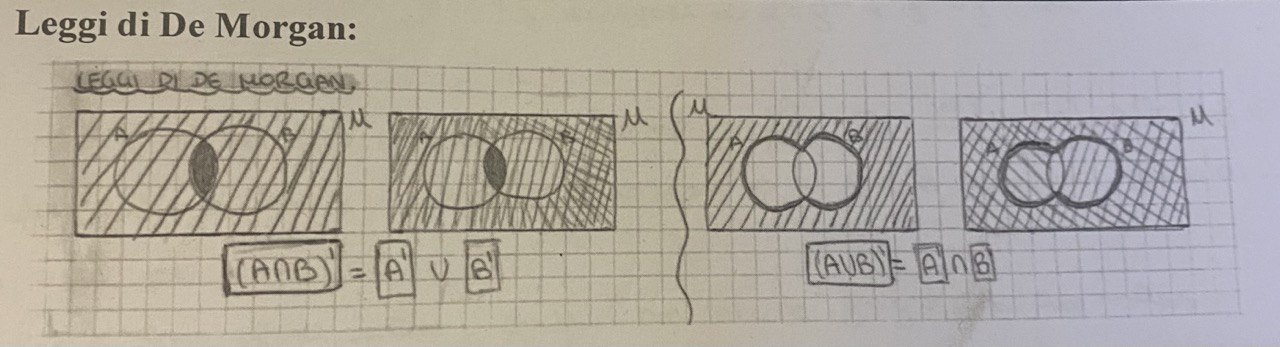
1 = 1

- Cos'è la funzione inversa:

f (a b)

f -1 (b a)

- Cosa sono le leggi di De Morgan



- Cosa sono le relazioni:

Una relazione tra A e B è un sottoinsieme r c a x b quindi scriviamo a R b

Se A = B si dice che r è una relazione su A

Una funzione f: A B è una relazione tra A e B

- Cos'è una partizione:

è un insieme (B) i cui elementi sono a loro volta insiemi (B sottoinsieme di A)

- Cos'è una proposizione?

È un’affermazione che può essere vera o falsa. Queste possono essere “proposizioni composte”, cioè più proposizioni collegate tra loro da connettivi logici

- Congiunzione di una proposizione:

P ∧ Q

- Disgiunzione di una proposizione:

P ∨ Q

- Disgiunzione esclusiva di una proposizione:

P x Q

- Implicazione di una proposizione:

P Q

- Equivalenza Logica di una proposizione:

P Q

- Cos'è un Predicato?

È una proposizione la cui verità o falsità dipende da una o più variabili

- Cos'è la dimostrazione diretta

Un ragionamento che mostra che se A è vero allora necessariamente è vera anche B

- Cos'è la dimostrazione per Assurdo

Si suppone vera A e (negato)B, deducendo una contraddizione

- Cos'è il principio di induzione matematico

È una tecnica di dimostrazione che consente di dimostrare la validità di una tesi attraverso 2 condizioni:

1. Passo Base o Passo 0
2. Passo Induttivo

- Cos'è il principio di induzione completo

Sia P(n) un predicato.

1) P(1) è vero;

2) Se n ∈ P allora ( P(1) ∧ P(2) ∧ … ∧ P(n) ) → P(n+1)

Allora P(n) è vero ∀ n ∈ P

- Cos'è il principio del buon ordinamento?

Ogni insieme di numeri naturali non vuoto contiene un numero che è più piccolo di tutti gli altri.

In altre parole, un qualsiasi sottoinsieme non vuoto dei numeri naturali ammette minimo.

WOP è falso per Z e per Q.

- Cosa sono i numeri primi?

Definiamo numero primo a, solo se a >= 2, e se è divisibile per uno e per se stesso.

Altrimenti a si dice composto

- Quando due numeri si dicono Coprimi?

I numeri Coprimi sono primi tra loro e l’unico numero che li divide è 1

- Quando un numero si dice perfetto?

Un numero si dice perfetto quando è uguale alla somma dei suoi divisori

- Cosa afferma il teorema dei numeri primi?

Lim pigreco(n) / (n/ln(n)) = 1

n +infinito

- Cos'è l'MCD?

Il Massimo Comune Divisore è il più grande divisore comune dei numeri considerati e viene calcolato mediante il metodo di composizione in fattori primi

- Cos'è l'algoritmo euclideo?

È un procedimento algebrico che permette di calcolare il massimo comun divisore tra due numeri interi attraverso un numero finito di passi basati sul calcolo di alcune divisioni

- Cos'è l'identità di Bezout?

Afferma che se a e b sono interi (non entrambi nulli) e il loro massimo comune divisore è d, allora esistono due interi x e y tali che:

ax + by = d

- Cosa afferma il teorema fondamentale dell'aritmetica?

Afferma che ogni numero naturale n>=1 o è un numero primo si può scrivere come prodotto di numeri primi.

Nel secondo caso la rappresentazione è unica a meno dell’ordine con cui compaiono i fattori

- Cosa sono le equazioni Diofantee lineari?

Un’equazione diofantea è un’equazione in una o più incognite con coefficienti interi di cui si ricercano le soluzioni intere

- Cosa sono le classi di resto?

Sia a ∈ Z la classe di congruenza di a mod n è la classe di equivalenza di a rispetto A ≡ n.

Quindi [a]n := {b ∈ Z : a ≡ mod n di b}

Si chiama anche classe di resto di a modulo n

- Cos'è l'inversa moltiplicativa?

Avendo due classi di resto [a]n e [b]n l’inversa moltiplicativa sarà: [a]n x [b]n = [1]n

- Cos'è una relazione di congruenza?

È una relazione di equivalenza compatibile con alcune operazioni algebriche

- Cos'è la funzione di Eulero?

È una funzione definita, per ogni intero positivo n, come il numero degli interi compresi tra 1 e n che sono coprimi con n

- Teorema di Eulero?

In matematica, Il Teorema di Eulero afferma che se n è un intero positivo ed a è coprimo rispetto ad n, allora:

a funzione phi di Eulero = la relazione di congruenza modulo n

a (n) congruente 1 mod n

- Piccolo teorema di Fermat?

Siano k, p appartenenti a N, p primo, tali che p x k

Allora

K elevato a p-1 è congruente a 1 (mod p)

- Codice RSA?

1) Prep

n = p \* q, dobbiamo prima calcolare n

ɸ (n) = (p-1) \* (q-1), trovare phi (n)

MCD (e, ɸ(n)) = 1, trovare il numero tale che l’mcd di questi 2 valori sia 1

Trovare inversa moltiplicativa [d] base ɸ(n) di [e] con base ɸ(n)

2) Codifica

Prendiamo un messaggio m ∈ P, che sia 1 <= m <= n tale che l’mcd (n, m) sia 1

Calcolare ([ḿ] base n) = ([m^^e] base n)

Scomponi l’inversa moltiplicativa

3)Decodifica

[ḿ^^d] mod n

- Numeri in base diversa?

Siano n, b ∈ P, con b >= 2.

Allora esistono da b0, …, bk ∈ N tale che 0 <= b, <= b-1 ∀ i = 0, …, k e n = bk \* b^^k + bk-1 \* b^^k-1+ … + bi \*b^^i + b0

Dove k := max { i ∈ N : b^^i <= N}. Tali b0 fino a bk sono unici.

- Cos'è la cardinalità?

È il numero degli elementi di un insieme.

- Problema fondamentale della combinatoria enumerativa?

Data una sequenza di insiemi finiti, calcolare la successione della cardinalità

- Proprietà di base (principio di inclusione esclusione ed altri)?

Siano A e B due insiemi e f : A B, f biunivoca. Allora

|A| = |B| \*\*A ha lo stesso numero di elementi di B

|AxB| = |A| x |B|

|A alla B| = |A| elevato alla |B|

|AUB| = |A| + |B| - |A intersecato B|

- Coefficiente Binomiale?

Il coefficiente binomiale n su k rappresenta il numero di sottoinsiemi di k elementi che si possono estrarre da un insieme di n elementi.

Il coefficiente binomiale n su k rappresenta il numero di sottoinsiemi di k elementi che si possono estrarre da un insieme di n elementi.

Se k < n si svolge il coefficiente con la seguente formula

Se k > n il coefficiente è nullo

- Coefficiente Multinomiale → Il coefficiente multinomiale è un numero che indica in quanti modi un insieme di oggetti può essere suddiviso in un certo numero di sottoinsiemi di dimensioni specifiche. In altre parole, il coefficiente multinomiale rappresenta il numero di modi in cui è possibile suddividere un insieme di n oggetti in k sottoinsiemi di dimensioni n1, n2, ..., nk, rispettivamente.

-Il principio di inclusione/esclusione?

|AUB| = |A| + |B| - |A⋂B|

Se A e B sono insiemi finiti

Siano A B C insiemi finiti:

|A U B U C| = |AUB| + |C| - |(AUB)⋂C|

- Cos'è una composizione debole?

Una composizione debole è una sequenza però >= 0.

A differenza di una composizione normale in cui i numeri della sequenza devono essere >= 1.

- Cos'è una composizione?

Una composizione di n in k parti è una sequenza di k numeri positivi a1, a2, …, ak tale che la loro somma è uguale a n

- Cos'è una permutazione?

È un ordinamento lineare degli elementi di un insieme

Es. sia m = {1^^1, 2^^2, 3^^1} = {1,2,2,3}

S(m) = {2213, 2231, 2123, …. tutte le possibili combinazioni dei 4 numeri

- Ruffini?

Sia P(x) ∈ R[x] e L ∈ C. Allora p(L) = 0 se e solo se (x-L) | P(x)

DIM.

( A(x) | B(x) ↔ ∃ c(x) ∈ R [x] tale che B(x) = A(x)^^c(x) )

- Somma Geometrica?

Serve per calcolare un esponenziale in cui varia l’esponente

- Somma Polinomiale?

Per calcolarla bisogna trovare una formula chiusa g(x) tale che il DEG di g(x) <= DEG di f(x) + 1

- Somma non polinomiale?

Sia f:R → R, f continua e monotona in R base >0. Allora f(1) + ∫ da 1 ad n f(x) dx <= ∑ f(i) <= f(n) + ∫ f(x) dx ∀ n ∈ N.

Cambia i segni per la decrescente

- Asintoticamente Equivalente?

Avendo 2 funzioni f(x) e g(x) si dicono Asintoticamente Equivalente se il Lim x → ∞ di f(x) fratto g(x) fa 1

- o-piccolo?

Avendo 2 funzioni f(x) e g(x) si ha f = o(g) se il Lim di x → ∞ di f(x) fratto g(x) è uguale a 0

- O-grande?

Avendo 2 funzioni f(x) e g(x) si ha f = O(g) se |f(x)| <= c(g(x))

- Omega?

Avendo 2 funzioni f(x) e g(x) si ha f = Ω(g) se f(x) >= C(|g(x)|)

- Cos'è un grafo?

- Cos'è un Cammino?

- Cos'è un cammino chiuso?

- Cos'è un ciclo?

- Cos'è un sentiero?

- Cos'è un grafo vuoto?

- Cos'è un grafo completo?

- Cos'è un grafo connesso?

- Cos'è un grafo a foresta?

- Cos'è un grafo ad albero?

- Cos'è un grafo indipendente?

- Cos'è un grafo completo?

- Cos'è il grado di un grafo?

- Quando due grafi si dicono isomorfi?

- Cos'è un accoppiamento tra due grafi?

- Cos'è un grafo bipartito?

- Accoppiamento da V1 a V2?

- Cos'è un grafo regolare?

- Cos'è una Colorazione?

- Cos'è il numero cromatico?

- Cos'è una ricorsione? → La ricorsione in matematica discreta è un modo per definire una sequenza o una funzione in cui il valore della funzione dipende dal valore della funzione stessa in un punto precedente. In altre parole, una funzione ricorsiva è definita utilizzando se stessa.

- Cos'è un grafo diretto?

- Cos'è il grado interno di un grafo diretto?

- Cos'è il grado esterno di un grafo diretto?

- Cos'è una rete di comunicazione?

- Cos'è lo smistamento?

- Cos'è un accoppiamento?

- Cosa dice il teorema di hall?