APPUNTI PER MATEMATICA DISCRETA

Definizione di sottoinsieme : un insieme B è un sottoinsieme si un insieme A se ogni elemento B è anche un elemento di A

Si scrive: B⊆A

Es. N⊆Z⊆Q⊆R⊆C

Z={numeri interi} -4 -3 -2 -1 0 1 2 3 4….

Q={numeri razionali} positivi e negativi e da tutti i numeri frazionali positivi e negativi (es: 1, -1, 1/2, ⅔

R={numeri reali} -5 , 4.5 5…

C={numeri complessi} 2i,−3i, √(5)i

Proprietà delle relazioni:

1. R è riflessiva se per ∀a∈A A è in relazione con A

Es. A={1,2,3,4}

R={(1,1),(2,2),(3,3),(4,4)}⊆AxA

R è riflessiva

R1={(1,2),(3,4)} non riflessiva

1. R è simmetrica se ∀a∈A , ∀a∈A

Se a è in relazione con b allora b è in relazione con a ovvero se(a,b)∈R allora(b,a)∈R

1. R è transitiva se per a,b,c ∈ A

Se a è in relazione con b e b è in relazione con c allora a è in relazione c

Una relazione è equivalente se R è

-riflessiva

-simmetrica

-transitiva

Per verificare che una corrispondenza sia una funzione:

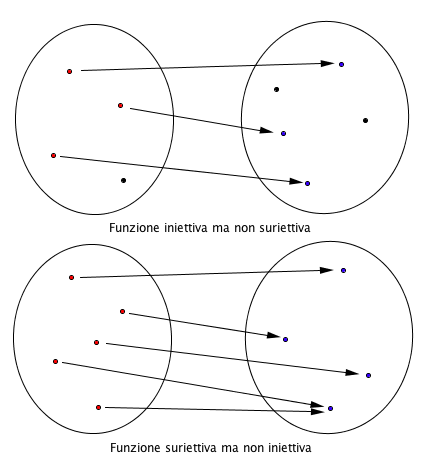
1) ogni elemento di A deve avere un immagine in B (BEN DEFINITA )

2) ogni elemento di A ha una sola immagine in B (DEFINIZIONE DI FUNZIONE )

Definiamo la suriettività: una funzione f:A→B è suriettiva se ogni b∈B ha una controimmagine

Iniettiva: se ogni elemento di B è immagine di più di un elemento di A

invertibile se iniettiva e suriettiva

 1 iniettiva ma non suriettiva 2 suriettiva ma non iniettiva

Regola generale per trovare tutte le congruenze :

Data la congruenza

Ax三b mod n

1. Calcolo d=(a,n)

Se d ∤ b non ci sono soluzioni

Se d/b ci sono soluzioni

In questo caso cerco le soluzioni pongo a1x三b1 mod n1n

Si ha (a1,n1)=1 allora a1 invertibile mod n1

Bèzout calcolo [a1]-1n1 =[c]n1

Moltiplico per c primo e secondo membro in a1x三b1 mod n1n

X三cb1 mod n1 pongo s=cb1

Modulo n le soluzioni sono:

X三s mod n

x=s+n1 mod n

X三s+2 n1 mod n

……….

x三s+(d-1)n1 mod n

Cioè

[s]n1 [s+n1]n [s+2n1]n….[s+(d-1)n1]n

Ci sono classi di resto mod n che sono soluzioni

Esempio:

Elencare le soluzioni in Z68 della congruenza 12x三8 mod 68

Soluzione:

mcd(12,68)=4 divide 8= ci sono soluzioni

Troviamole:

Divido per 4 trovo congruenza

3x三2 mod 17

Cerco [3]-117

Bezout

17=5\*3+2

3=2+1

1=3\*2=3-(17-5\*3)=6\*3-17

[3]-117 =[6]17

Moltiplico 3x三2 mod 17 per 6

6\*3x三2\*6 mod 17

Le soluzioni in Z68 sono:

[12],[12+17] [12+17] [12+34] [12+51]

Ovvero

[12] [29] [46] [63]

teorema di bezout

facciamo euclide tra (1147 1000)

1147=1000\*1+147

1000=147\*6+118

147=118\*1+29

118=29\*4+2

29=2\*14+1

2=1\*2+0

bezout

1=29-(14\*2) ovvero prendo l’ultimo passaggio con resto e sposto l’uguaglianza

1=29-14\*(118-4\*29) adesso il 2

1=29(1+14\*4)-14\*118

1=29\*57-14\*118 i resti sono i numeri che andranno sostituiti per esempio 29

1=(147\*1-118)\*57-14\*118

1=147\*1 -118(57+14)

1=147\*57-118\*71 devo riscrivere il numero come multipli di 147 e 118

1=147\*57-(1000-6\*147)\*71

1=147\*57-1000\*71 -6\*147\*71

1=147\*(57+6\*71)-1000\*71

1=147\*483-1000\*71

1=(1147-1000\*1)\*483-1000\*71

1=1147\*483-1000\*483-1000\*71

1=1147\*483-1000\*(483-71)

1=1147\*483-1000\*554 risultato

x=483 y=-554

periodo = il minimo intero n>0 t.c. σn=(1) (o l’mcd nei cicli disgiunti)

lagrange:

1)cardinalità sottogruppo divide cardinalità del gruppo

1. xcardinalità del gruppo =elemento neutro per ogni x appartenete al gruppo
2. xcardinalità<x>= elemento neutro per ogni x appartenete al gruppo

(<x> è il generatore)

Terminologia:

F:G1→G2 omomorfismo si dice:

-monomorfismo se è iniettivo

-epimorfismo se è surriettivo

-isomorfismo se è biettivo

-endomorfismo se G1=G2

-automorfismo se G1=G2 ed è biettivo

proposizione : F:G1→G2 omomorfismo

F iniettivo ⇔ ker F={eG1} (e elemento neutro)

isomorfismi :

Def: due gruppi G1,G2 si dicono isomorfi se esiste un isomorfismo F:G1→G2 (in questo caso F-1:G1→G2 isomorfismo )

Due gruppi isomorfi sono “moralmente” lo stesso gruppo ovvero hanno le stesse proprietà

Esempio importante!!!!!

Supponiamo m,n є N m,n>=2 t.c. n/m

Consideriamo la funzione:

F:Zm→Zn

[a]m→[a]n

È ben definita se non dipende dalla scelta del rappresentante cioè:

Se [a]m=[a1],⇒[a]n=[a1]n

Nota bene è essenziale che n/m

Se n/m:

Esempio:

m=45 n=9

F:Z45→Z9

[a]45 →[a]9

Ker F={[a]45|[a]9=[0]9}

={[a]45|9/a}

={[0]45,[9]45,[18]45,[27]45,[36]45}(tutti i multipli di 9 fino a 45)

sottogruppi : H<=G

Proprietà:

H⊆G è sottogruppo ⇔

1. H è stabile
2. H contiene e
3. X є H⇒x-1 є H

N=numero di oggetti

k= posti disponibili

