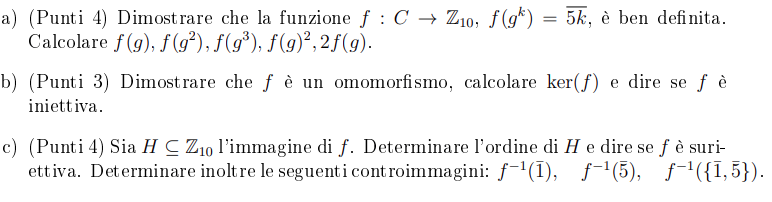
Sia C = ⟨g⟩ un gruppo ciclico con 32 elementi



1. dimostriamo che f(gk)=5k mod 10 è ben definita (ovvero che dipende solo da gk ):

gk+32=gk

per ogni k ∈ Z Perciò, due esponenti k e l che differiscono di un multiplo di 32, cioè k−l=32m rappresentano lo stesso elemento in C

verichiamo che f(gk) non cambia se k e l sono congruenti in 32

se gk=gl allora k-l=32m

f(gk)=5k mod 10 e f(gl)=5l mod 10

Ora, consideriamo la differenza:

5k-5l =

5(k-l)=

5\*32m=160m

160m Ξ 0 mod 10

quindi: gk=gl  quindi la funzione è ben definita

calcoliamo i valori richiesti:

f(g)=5\*1= 5 mod 10 ovvero 5

f(g2)=5\*2= 10 mod 10 ovvero 0

f(g3)=5\*3= 15 mod 10 ovvero 5

f(g)2 =52 = 25 mod 10 ovvero 5

2\*f(g)= 2\*5=10 mod 10 ovvero 0

1. f(gk)=5k mod 10 è omomorfismo se per ogni gk gl abbiamo:

f(gk⋅gl)=f(gk)+f(gl) mod10.

f(gk)+f(gl)=(5k mod 10)+(5l mod 10)= 5k+5l mod 10

f(gk⋅gl)=5(k+l) = 5k+5l

notiamo che sono uguali quindi è omomorfismo

Il kernel di un omomorfismo è l'insieme degli elementi del dominio che vengono mandati all'elemento neutro del codominio. Nel nostro caso, il codominio è Z10 e l'elemento neutro è 0. Dunque:

ker⁡(f)={gk∈C ∣ f(gk)=0}

f(gk)=0 = 5 k mod 10 =0

k=2

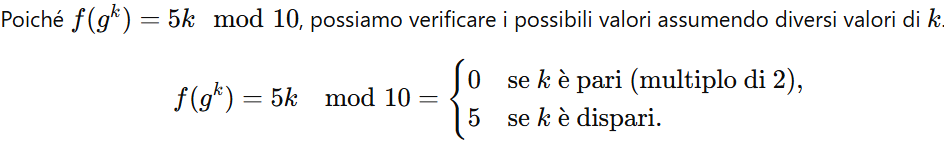
g2 = {0,2,4,6,…,30} ( perchè ⟨g⟩ un gruppo ciclico con 32 elementi)

il ker è generato da g2 che ha cardinalità=16

ker f = {g k | 10|5k} = {g k | 2|k} = {e, g2 , g4 , . . . g15}

Un omomorfismo è iniettivo se e solo se il suo kernel contiene solo l'elemento neutro del dominio. Nel nostro caso, il kernel ha 16 elementi (ker⁡(f)=⟨g2⟩ , quindi f **non è iniettiva**.

c)L'**immagine** di f, denotata con H, è l'insieme di tutti i valori in Z​10 che sono raggiunti da f(gk)quando k varia in {0,1,…,31}



H={0,5} ed ha ordine 2 (ordine e cardinalità sono la stessa cosa )

non contiene tutti gli elementi di Z​10  quindi non è suriettiva

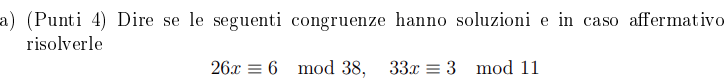
contro immagini:

f-1(1)= impossibile perché la funzione assume come valori 0 o 5 (∅)

f-1(5) =5 k mod 10 = 5 kΞ1 mod 2 (k dispari) vero

f-1({1 5}) solo per k dispari ovvero la funzione è sempre vera quando k∈{1,3,5,…,31}

PROBLEMA 2



mcd(26 38)= 2

2 divide 6 quindi ci sono 2 soluzioni

13xΞ3 mod 19

l’inverso di 13 mod 19 è:

eulero(19 13)=

19=13\*1+6

13=6\*2+1

6=2\*3+0

bezout:

1=13-6\*2

1=13-(19-13\*1)\*2

1=13\*3-19\*2

quindi 3 mod 19 è l’inverso di 13 mod 19

3\* 13xΞ3\*3 mod 19

quindi xΞ9 mod 19

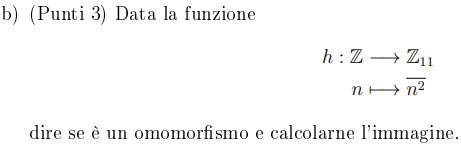
xΞ9 mod 38 prima soluzione

xΞ9+19 mod 38 ovvero xΞ28 mod 38

33xΞ3 mod 11

mcd(33 11)=11

3 non divide 11 quindi non ci sono soluzioni



#### **Verifica se h è un omomorfismo**

Una funzione tra gruppi è un omomorfismo se preserva l'operazione del gruppo. Qui il dominio Zè un gruppo abeliano rispetto alla somma , mentre Z11​ è un gruppo ciclico di ordine 11 rispetto alla somma modulo 11. Quindi, dobbiamo verificare se:

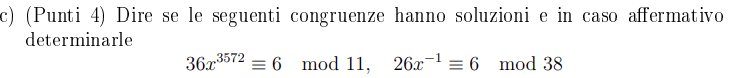
h(a+b)≡h(a)+h(b) mod 11,∀a,b∈Z.

h(a+b)=(a+b)2

h(a)+h(b)= a2+b2

ad occhio vediamo che non sono uguali quindi non è omomorfismo perchè non preserva la somma

l’immagine è: 



36x3572 ≡ 6 mod 11

36/11= 3 resto 3

quindi 36≡3 mod  11

ordine di 11=ᵩ(11)=10

quindi x3572 ≡ x3572 mod 11

Per il **Teorema di Eulero**, x10 ≡ 1 mod  11 + per ogni x invertibile modulo 11

x3572 ≡ x2 mod 11

3x2≡ 6 mod 11

calcoliamo l’inverso di 3

euclide (11 3)

11=3\*3+2

3=2\*1+1

2=1\*2+0

bezout

1=3-2\*1

1=3-(11-3\*3)\*1

1=3\*4-11\*3

4\* 3x2≡ 6 \* 4mod 11

x2≡ 6 \* 4 mod 11

x2≡24 mod 11

x2≡2mod11

x2 mod 11 per x∈{0,1,…,10}

Nessun valore di x2 mod  11 = 2 **Quindi, la congruenza non ha soluzioni (come si è visto al punto b), 2 non è un quadrato modulo 11)**

mcd(26 38)=2

quindi diventa

13x−1≡3mod19

euclide (19 13)

19=13\*1+6

13=6\*2+1

6=1\*6+0

bezout

1=13-6\*2

1=13-(19-6)\*2

1=13\*3-19\*2

3 \* 13x−1≡3 \* 3mod19

x−1≡9 mod 19

26x−1 ≡ 6 mod 38 si riduce a:

x≡ 17 mod 19

che dà x ≡ 17 mod 19.