Problema 1: In S10, si consideri la permutazione σ = (1 3 5 7 9)(1 2 3 4)

a) (Punti 4)

Scrivere σ come prodotto di cicli disgiunti, determinarne il tipo, il periodo e la parità.

(1 2 5 7 9) (3 4)

tipo (5, 2)

periodo= mcm tra (5 2)= 10

è dispari

b) (Punti 4) Determinare una permutazione π in S10 tale che σ5272 ◦ π = (1 2).

σ5272 trasformiamolo in mod 10 (ricavato dal periodo)

σ527 +σ2 = σ527 sarebbe e quindi sparisce e rimane σ2

σ2 = (1 5 9 2 7 ) ( 3 4 sparisce perchè un biciclo alla seconda scompare perchè diventa l’identità)

noi quindi sappiamo che σ2 ◦ π = (1 2).

questo implica

π=(σ2)-1 ◦ (1 2)

l’inverso di (1 5 9 2 7 ) sarà quindi (7 2 9 5 1 )

π=(7 2 9 5 1) ◦ (1 2)

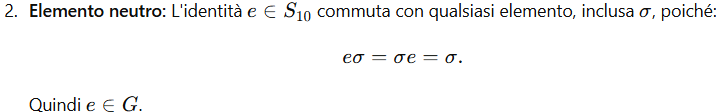
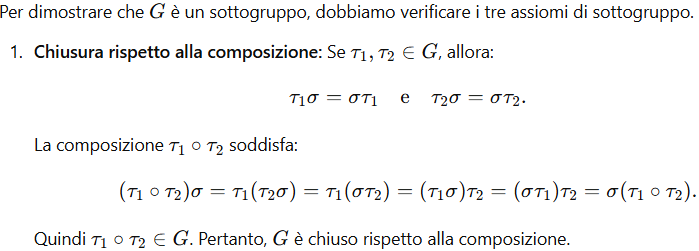
lo trasformo in prodotti di cicli

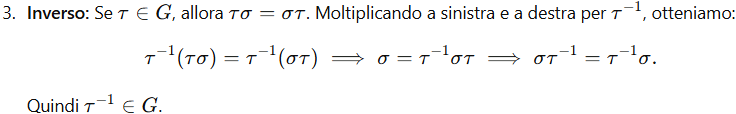
π=(1 9 5 ) (2 7)

c) (Punti 3) Si consideri l'insieme

G = {τ ∈ S10 | τ σ = στ}.

Dimostrare che G è un sottogruppo di S10 e determinare tre elementi distinti appartenenti a G





inoltre per essere sotto gruppo

1. G≠Ø

quindi dato che σ ∈ G, quindi G ≠ ∅

i 3 elementi posso essere l’identità(1), σ e σ2

Problema 2:

Siano N = 1147, M = 5

a) (Punti 4) Calcolare il massimo comune divisore di N e 1000 e esprimerlo mediante l'identità di Bézout.

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)

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

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

1=29\*57-14\*118

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

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

1=147\*57-118\*71

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

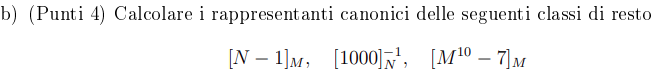
1=(1147-1000\*1)\*483-1000\*71

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

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

1=1147\*483-1000\*554

x=483 y=-554



[1147-1] mod 5

[1146] mod 5 三 1

il rappresentante canonico è 1

[1000]-1 mod 1147

1000x三 1 mod 1147

sapendo grazie a bezout che

1000\*(554)三 1 mod 1147

quindi ora facendo

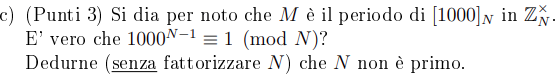
1147-554=593

[1000]-1 mod 1147=593

[m10-7]m ovvero [510-7]5

[510] mod 5 - [7] mod 5

[510] mod 5 = id - [7] mod 5 = -2 mod 5 ovvero 3 mod 5



5=periodo di [1000] mod 1147

10001147-1三 1 mod 5

10001146三 1 mod 5

dato che 5 non divide 1146 la congruenza non è valida

per il piccolo teorema di fermat n non può essere primo