

MD • SOROLLA "f" - 1

Rispondere a ciascuna domanda, motivando adeguatamente le risposte. Per essere sufficiente un compito deve raggiungere almeno 18 punti.

Esercizio 1 (11 punti). Viene formato un gruppo di lavoro costituito da 15 informatici per un progetto europeo a cui partecipano Albania, Dalmazia, Grecia, Olanda e Spagna.

- Il gruppo di lavoro sarà indicato con una sigla formata dalle 5 iniziali A.D.G.O.S delle nazioni coinvolte. Quante sono le possibili sigle?

- Quante diverse distribuzioni per nazionalità può avere un tale gruppo se si richiede che sia presente almeno un membro per ciascuna nazione partecipante?

- Una volta scelto il gruppo dei 15 informatici, si procede ad assegnare i compiti: 7 di loro devono essere assegnati a 1, 5 al settore progetto, 2 ai rimanenti ricoprendo il ruolo di coordinatore tra i due progetti, di responsabile del budget e di responsabile della presentazione dei risultati. In quanti modi si possono attribuire i compiti?

$$f_1 f_2 f_3 f_4 f_5 = 1$$

$$3 \cdot \alpha \leq \{A, D, G, O, S\}^5, \alpha = \{A', D', G', O', S'\}$$

$$n_{SS} = \frac{S!}{3!1! \cdot 1! \cdot 1! \cdot 1!} = \frac{S!}{(3!)^1} \text{ OK}$$

1.b $|I| = 15$, se ne occupo già S delle rispettive nazionali devo solo scegliere i 10 componenti rimanenti.

$$\text{rimanenti sono } \frac{10 \cdot 9 \cdot 8 \cdot 7 \cdot 6 \cdot 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1}{A^7 D^5 G^1 O^1 S^1} = 10$$

Per ottenere le combinazioni dei 10 rimanenti, bisogna sceglierle a partire dalle S nazionalità in cui conta: ordine ma non contano ripetizioni per cui è una
Combinazione con ripetizione = $\binom{10+S-1}{S-1} = \binom{14}{4}$

1.c $|I| = 15$

$$\text{Sotto-progetto 1} = \binom{15}{7} = \frac{15!}{7! \cdot (15-7)!} = \frac{15!}{7!} = \left[\begin{array}{l} \text{totale} \\ \binom{15}{7} \cdot \binom{8}{8} \cdot 3! \\ \text{OK} \end{array} \right]$$

$$\text{Sotto-progetto 2} = \binom{8}{8} = \frac{8!}{8!}$$

$$3 \text{ ruoli rimanenti} = 3! \leftarrow \text{la rimanenza}$$

Esercizio 2 (11 punti). Si considerino le permutazioni di S_7 :

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 7 & 1 & 3 & 4 & 5 & 6 & 2 \end{pmatrix} \quad \tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 1 & 2 & 4 & 6 & 3 & 5 & 7 \end{pmatrix}$$

a) Determinare tipo e parità di σ e τ .

OU

2.c) $\text{Tipo}(\sigma) = 3, \text{Tipo}(\tau) = 4$

$$\sigma = (1, 7, 2) \quad \tau = (3, 4, 6, 5)$$

Parità (σ) = Pari, Parità (τ) = Disp.

b) Determinare le composizioni $\tau \circ \sigma$ e $\sigma \circ \tau$.

c) Verificare che l'insieme $H = \{\sigma^h \tau^k \mid h, k \in \mathbb{Z}\}$ è un sottogruppo di S_7 e che si tratta di un gruppo ciclico.

2.b)

$$\begin{aligned} \tau \circ \sigma &= \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 1 & 2 & 4 & 6 & 3 & 5 & 7 \\ 7 & 1 & 4 & 6 & 3 & 5 & 2 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 7 & 1 & 3 & 4 & 5 & 6 & 2 \end{pmatrix} \\ &= (1, 7, 2) \cdot (3, 4, 6, 5) \end{aligned}$$

$$\sigma \circ \tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 7 & 1 & 3 & 4 & 5 & 6 & 2 \\ 1 & 1 & 4 & 6 & 3 & 5 & 2 \end{pmatrix} \quad \text{OU} \quad (1, 7, 2) \circ (3, 4, 6, 5)$$

2.c)

S_7 è un gruppo ciclico $\Rightarrow \langle \pi \rangle = \{e, \pi, \pi^2, \pi^3, \dots, \pi^6\}$

Per def. $\sigma^h \in \langle \pi \rangle$ e $\tau^k \in \langle \pi \rangle$, definendo quindi

H , per essere sottogruppo

- $e \in H : \sigma^h \circ \tau^k$ con $h=0$ e $k=0$ SI
- $g^m * g^n \in H : (\sigma^{h_1} \circ \tau^{k_1}) * (\sigma^{h_2} \circ \tau^{k_2}) = \sigma^{h_1+h_2} \circ \tau^{k_1+k_2} \in H$ per $h_1, h_2, k_1, k_2 \in \mathbb{Z}$
- $\forall g^n \exists g^m \in H$ t.c. $e = g^n \circ g^m \Rightarrow (\sigma^{h_1} \circ \tau^{k_1}) \circ (\sigma^{h_2} \circ \tau^{k_2}) = e$
 $\sigma^{h_1+h_2} \circ \tau^{k_1+k_2} = e$
se $h_1 = -h_2$ e $k_1 = -k_2$
 $\sigma^{h_1-h_2} \circ \tau^{k_1-k_2} = \sigma^0 \circ \tau^0 = e$

È ciclico? periodo $(\sigma^{h_1} \circ \tau^{k_1}) = \text{lcm}(3, 4) = [2] = 12$ ciclico

DA MIGLIORARE :

- Dimostrazioni de un insieme sia sotto-gruppo di un altro
- Verificare de sia ciclico.

Esercizio 3 (11 punti).

a) Determinare MCD e identità di Bézout dei numeri $m = 3973$ e $n = 1853$.

b) Determinare le ultime due cifre decimali del numero 41803^{1003} .

c) Determinare il numero di elementi invertibili dei due anelli prodotto $A = \mathbb{Z}_8 \times \mathbb{Z}_{15}$ e $R = \mathbb{Z}_{12} \times \mathbb{Z}_{10}$. Stabilire se $g: A \rightarrow R$ data da $g([h]_8, [k]_{15}) = ([3h]_{12}, [2k]_{10})$ è un omomorfismo di anelli e in caso affermativo determinare $\ker(g)$ e $\text{Im}(g)$.

$$3. a) \text{MCD}(3973, 1853) = 1$$

$$3973 = 2 \cdot 1853 + 264$$

$$1853 = 6 \cdot 264 + 251$$

$$264 = 1 \cdot 251 + 13$$

$$251 = 19 \cdot 13 + 11$$

$$13 = 1 \cdot 11 + 5$$

$$11 = 2 \cdot 5 + 1$$

$$5 = 1 \cdot 1 + 0$$

Bézout

$$1 = 11 - 2 \cdot 5 \quad S = 11 - 1 \cdot 11$$

$$1 = 11 - 2 \cdot (11 - 1 \cdot 11)$$

$$= 11 - 2 \cdot 11 + 2 \cdot 11 \quad 11 = 251 - 19 \cdot 13$$

$$= 3 \cdot 11 - 2 \cdot 13$$

$$1 = 3 \cdot (251 - 19 \cdot 13) - 2 \cdot 13$$

$$= 3 \cdot 251 - 45 \cdot 13 - 2 \cdot 13$$

$$= 3 \cdot 251 - 47 \cdot 13 \quad 13 = 264 - 1 \cdot 251$$

$$1 = 3 \cdot 251 - 47 \cdot (264 - 1 \cdot 251)$$

$$= 3 \cdot 251 - 47 \cdot 264 + 47 \cdot 251$$

$$= 50 \cdot 251 - 47 \cdot 264 \quad 264 = 1853 - 6 \cdot 251$$

$$1 = 50 \cdot (1853 - 6 \cdot 264) - 47 \cdot 264$$

$$= 50 \cdot 1853 - 300 \cdot 264 - 47 \cdot 264$$

$$= 50 \cdot 1853 - 347 \cdot 264$$

$$264 = 3973 - 2 \cdot 1853$$

$$1 = 50 \cdot 1853 - 347 \cdot (3973 - 2 \cdot 1853)$$

$$= 50 \cdot 1853 - 347 \cdot 3973 + 694 \cdot 1853$$

$$1 = \underbrace{347}_{x} \cdot 1853 - \underbrace{347}_{y} \cdot 3973$$

$$\begin{array}{r} 6 \\ 3973 \\ \hline 3706 \\ \hline 267 \end{array} \left| \begin{array}{l} 1853 \\ 2 \\ 12268 \end{array} \right.$$

$$\begin{array}{r} 11 \\ 1853 \\ \hline 2 \\ 3706 \\ \hline 267 \end{array}$$

$$\begin{array}{r} 1853 \\ \hline 3602 \\ \hline 251 \end{array} \left| \begin{array}{l} 264 \\ 6 \\ 12251 \end{array} \right.$$

$$\begin{array}{r} 44 \\ 264 \\ \hline 6 \\ 1602 \\ \hline 10 \end{array}$$

$$\begin{array}{r} 264 \\ \hline 251 \\ \hline 12 \\ 0 \end{array}$$

$$\begin{array}{r} 1 \\ 16 \\ \hline 1 \\ 16 \\ \hline 1 \end{array}$$

$$\begin{array}{r} 12 \\ 324 \\ \hline 16 \\ 144 \\ \hline 2 \end{array} \left| \begin{array}{l} 1 \\ 16 \\ 16 \\ 144 \\ \hline 144 \end{array} \right.$$

$$\begin{array}{r} 3 \\ 16 \\ \hline 16 \\ 16 \\ \hline 16 \\ 16 \\ \hline 0 \end{array} \left| \begin{array}{l} 3 \\ 16 \\ 16 \\ 16 \\ 16 \\ 16 \\ 16 \\ 0 \end{array} \right.$$

$$\begin{array}{r} 16 \\ 16 \\ \hline 16 \\ 16 \\ \hline 16 \\ 16 \\ \hline 0 \end{array} \left| \begin{array}{l} 16 \\ 16 \\ 16 \\ 16 \\ 16 \\ 16 \\ 16 \\ 0 \end{array} \right.$$

$$\begin{array}{r} 16 \\ 16 \\ \hline 16 \\ 16 \\ \hline 16 \\ 16 \\ \hline 0 \end{array} \left| \begin{array}{l} 16 \\ 16 \\ 16 \\ 16 \\ 16 \\ 16 \\ 16 \\ 0 \end{array} \right.$$

$$\frac{50}{6}$$

$$\text{MCD}(41803, 600)$$

$$\begin{array}{r} 41803 \\ 400 \\ \hline 180 \\ 180 \\ \hline 0 \end{array}$$

$$\begin{array}{r} 347 \\ 2 \\ 694 \\ \hline 694 \\ 694 \\ \hline 0 \end{array}$$

3.b)

$$\varphi(100) = \varphi(s^4) \cdot \varphi(z^2) =$$

$$41803^{40 \cdot 25+3} \cdot (41803^{40})^3 = 27 \pmod{100}$$

$$\begin{array}{r} s \cdot 4 \\ 40 \\ \hline 100 \\ 100 \\ \hline 0 \end{array} \left| \begin{array}{l} z^2 \\ 27 \\ 27 \\ 27 \\ 27 \\ 27 \\ 27 \\ 0 \end{array} \right.$$

$$\pmod{100} = 27$$

le ultime 2 cifre
della sesta potenza

Esercizio 3 (11 punti).

- a) Determinare MCD e identità di Bézout dei numeri $m = 3973$ e $n = 1853$.
 b) Determinare le ultime due cifre decimali del numero 41803^{1003} .
 c) Determinare il numero di elementi invertibili dei due anelli prodotto $A = \mathbb{Z}_8 \times \mathbb{Z}_{15}$ e $R = \mathbb{Z}_{12} \times \mathbb{Z}_{10}$. Stabilire se $g: A \rightarrow R$ data da $g([h]_8, [k]_{15}) = ([3h]_{12}, [2k]_{10})$ è un omomorfismo di anelli e in caso affermativo determinare $\ker(g)$ e $\text{Im}(g)$.

3.C.1

Invertibili per A $\Rightarrow \mathcal{P}(\mathbb{Z}_8) \cdot \mathcal{P}(\mathbb{Z}_{15}) = \textcircled{32}$

$$\begin{matrix} \mathcal{P}(\mathbb{Z}^3) \cdot \mathcal{P}(\mathbb{Z}^5) \\ \mathcal{E} \cdot \mathcal{G} \end{matrix} = \mathcal{E} \cdot \mathcal{G}$$

Invertibili per B $\Rightarrow \mathcal{P}(\mathbb{Z}_{12}) \cdot \mathcal{P}(\mathbb{Z}_{10}) = \textcircled{36}$

$$\begin{matrix} \mathcal{P}(3 \cdot 2^2) \cdot \mathcal{P}(5 \cdot 2) \\ \mathcal{E} \cdot \mathcal{G} \end{matrix} = \mathcal{E} \cdot \mathcal{G}$$

3.C.2.1 $\Rightarrow g$ è un omorfismo? ^{ovvero} $\forall a, a' \in \mathbb{Z}_8 \quad g(a \cdot a') = g(a) \cdot g(a')$?

Per $[h]_8 \Rightarrow$ un numero h in \mathbb{Z}_8 è nella forma $n+8$. Per cui mappato in $[3n]_{12}$ sarebbe: $[3 \cdot (n+8)]_{12}$
 ovvero: $[3n+24]_{12}$ ma siccome $12 \mid 24$ allora è eq. a $[3n]_{12}$

Per $[k]_{15} \Rightarrow$ un num. K in \mathbb{Z}_{15} è nella forma $n+15$. Per cui mappato in $[2k]_{10}$ sarebbe: $[2 \cdot (n+15)]_{10}$
 ovvero: $[2n+30]_{10}$ ma siccome $10 \mid 30$, allora è eq. a $[2n]_{10}$

g è ben definita. Si verifica quindi la proprietà degli omomorfismi:

Per la somma: $\underbrace{g(([h]_8, [k]_8) + ([h']_8, [k']_8))}_{g([h+h']_8, [k+k']_8)} = g(([h]_8, [k]_8)) + g(([h']_8, [k']_8))$

$$g([h+h']_8, [k+k']_8) = ([3(h+h')]_{12}, [2(k+k')]_{10}) = ([3h]_8, [2k]_8) + ([3h']_8, [2k']_8) = \textcircled{51}$$

omomorfismo
gruppo
comm.

Per il prodotto: $g(([h]_8, [k]_8) \cdot ([h']_8, [k']_8)) = g(([h]_8, [k]_8)) \cdot g(([h']_8, [k']_8))$?

$$g([zh \cdot h']_8, [ck \cdot k']_8) = ([3(zh \cdot h')]_{12}, [2(ck \cdot k')]_{10}) = ([3h]_8, [2k]_8) \cdot ([3h']_8, [2k']_8)$$

$$\neq ([e(h \cdot h')]_{12}, [e \cdot (k \cdot k')]_{10})$$

Non è un
omomorfismo
per gli: che si

MD • SUCCLAS "Z" - Z

Esercizio 1 (11 = 4 + 4 + 3 punti).

a) Una certa sigla alfamericana è formata da tre lettere (di un alfabeto di 21 lettere) seguite da tre cifre. Le cifre possono essere ripetute, le lettere no. Quante sono le possibili sigle in tutto?

b) Calcolare il numero degli anagrammi della parola SILLOGISMO.

c) Dire quanti sono i numeri tra 1 e 4200 non divisibili né per 2, né per 3 né per 7.

$$\text{lettere} \quad \text{Disposizioni semplici} = 21 \cdot 20 \cdot 19 \\ C_{21,3} = \binom{21+20}{20} = \binom{23}{20}$$

Possibili sigle sono \Rightarrow

$$1.b \quad c = \text{SILLOGISMO} = 10$$

$$= \frac{10!}{2! \cdot 2! \cdot 2! \cdot 2! \cdot 2! \cdot 1!} =$$

$$C_{10,3} = \binom{10}{3}$$

Ripetibili

Disp. con rip.

$$= 10 \cdot 10 \cdot 10$$

$$\frac{(23)!}{(20)!} \cdot \frac{10!}{(3)!} = 23! \cdot \frac{10!}{20! \cdot 3!} = \frac{10! \cdot 21 \cdot 20 \cdot 19 \cdot 18}{3! \cdot (7)!}$$

$$|S|=2 \text{ in } c \quad |I|=2 \text{ in } C \quad |2|=2$$

$$|O|=2 \quad |G|=1 \quad |W|=1$$

OU

2.c

$$P(n) \Rightarrow n \geq 1 \wedge n \leq 4200$$

$$Y = \{n \in \mathbb{N} \mid P(n) \wedge 3 \nmid n\} \quad Z = \{n \in \mathbb{N} \mid P(n) \wedge 7 \nmid n\}$$

$$(X \cap Y \cap Z) = ? \quad = |X| + |Y| + |Z| - |X \cap Y| - |X \cap Z| - |Y \cap Z|$$

$$+ |X \cup Y \cup Z|$$

$$|X| = 4200 / 2 = 2100, |Z| = \left[\frac{4200}{7} \right] = 600, |Y| = \left[\frac{4200}{3} \right] = 1400$$

$$|X \cap Y| = \{n \in \mathbb{N} \mid P(n) \wedge 6 \mid n\}$$

$$|X \cap Z| = \{n \in \mathbb{N} \mid P(n) \wedge 14 \mid n\}$$

$$|X \cap Y| = \left[\frac{4200}{6} \right] = 700$$

$$|Y \cap Z| = \{n \in \mathbb{N} \mid P(n) \wedge 21 \mid n\}$$

$$|X \cap Y \cap Z| = \left[\frac{4200}{42} \right] = 100$$

$$|X \cup Y \cup Z| = 2100 + 1400 + 600 - 700 - 300 - 200 + 2100$$

$$= 3500$$

No! Convienze fare il ragionamento = 2100 + 2000 - 1200 + 2100

al contrario! Ovvero contare $|X \cup Y \cup Z| = 6200 - 1200 = 5000$

e poi fare $4200 - |X \cup Y \cup Z|$ quindi

$$|X| = 2100, |Y| = 1400, |Z| = 600, |X \cap Y| = 700, |X \cap Z| = 300, |Y \cap Z| = 100$$

$$|X \cap Y \cap Z| = \left[\frac{4200}{42} \right] = 100 \quad \text{quindi}$$

$$|X \cup Y \cup Z| = 2100 + 1400 + 600 - 700 - 300 - 200 + 100$$

$$= 3500 - 100 - 500 + 100 = 3000$$

$$4200 - 3000 = \underline{\underline{1200}}$$

Esercizio 2 ($11 = 4 + 4 + 3$ punti). Si considerino i seguenti cicli in S_7 :

$$\sigma_1 = (2 \ 6 \ 1 \ 7 \ 5) \quad \sigma_2 = (1 \ 3 \ 6 \ 4).$$

- a) Calcolare la decomposizione in cicli disgiunti della composizione $\tau = \sigma_1 \circ \sigma_2$
b) Determinare tipo, parità e periodo di τ
c) Verificare che la funzione $f : \mathbb{Z}_{20} \rightarrow S_7$, con $f([k]) = \tau^k$ è ben definita, è un omomorfismo di gruppi da $(\mathbb{Z}_{20}, +)$ a (S_7, \circ) e determinarne esplicitamente il nucleo.

2.b = $\text{Tipo}(\tau) = (2, 5)$
 D_P

Periodo = $\text{mcm}(5, 2) = 10$

2.c.1

~~$[k]_{20} \rightarrow \tau^k$~~

siccome $k \in \mathbb{Z}$ allora k può essere
 ≥ 0 per cui τ^{k-1} non è effettuabile

No! Descrivere sempre gli elementi: $\sum_{i=0}^{n-1} k_i \tau^i$ è nella forma $k + z \alpha$
per cui $\tau^n = \tau^{(k+z\alpha)n} \Rightarrow \tau^n (\tau^{z\alpha})^n \Rightarrow \tau^n$
 $\tau = \tau$ siccome τ ha

Quindi è ben definita

Omomorfismo di gruppi: $f([k]_{20} + [k']_{20}) = f([k]_{20}) \circ f([k']_{20})$

$$f([k+k']_{20}) = \tau^k \circ \tau^{k'} = \tau^{k+k'}$$

Nucleo di omomorfismo: $\text{Kernel}(f) = \{ n \in \mathbb{Z}_{20} \mid f(n) = 0 \}$

$= \{ 0, 10 \}$ gli unici elementi
multipli del periodo
di τ tra 0 e 10.

Esercizio 3 (11 = 4 + 4 + 3 punti).

a) Dopo aver verificato che $\text{MCD}(75, 1156) = 1$, calcolare l'inverso di 75 in \mathbb{Z}_{1156} .

b) Calcolare il numero degli elementi invertibili nell'anello $\mathbb{Z} \times \mathbb{Z}_{20}$.

c) Calcolare il resto della divisione di 1387^{34} per 60.

3.a) $\text{MCD}(75, 1156)$ tramite Algoritmo di Euclideo.

$$1156 = 15 \cdot 75 + 31$$

$$75 = 2 \cdot 31 + 13$$

$$31 = 2 \cdot 13 + 5$$

$$13 = 2 \cdot 5 + 3$$

$$5 = 1 \cdot 3 + 2$$

$$3 = 1 \cdot 2 + 1 \quad \text{MCD}$$

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

Quindi $I = \frac{1}{447 \cdot 75 - 29 \cdot 1156}$

$$= \frac{1}{447 \cdot 75}$$

$$= \frac{1}{33525}$$

$$1 = 12 \cdot 75 - 29 \cdot (1156 - 15 \cdot 75) \Rightarrow 12 \cdot 75 - 29 \cdot 1156 + 15 \cdot 75 \cdot 29 \Rightarrow 447 \cdot 75 - 29 \cdot 1156$$

$$1 = 12 \cdot (75 - 2 \cdot 31) - 29 \cdot 31 \Rightarrow 12 \cdot 75 - 24 \cdot 31 - 29 \cdot 31 = 12 \cdot 75 - 29 \cdot 31$$

$$1 = 2 \cdot 13 - 5 \cdot (31 - 2 \cdot 13) \Rightarrow 2 \cdot 13 - 5 \cdot 31 + 10 \cdot 13 \Rightarrow 12 \cdot 13 - 5 \cdot 31$$

$$1 = 2 \cdot (13 - 2 \cdot 5) - 5 \cdot 5 \Rightarrow 2 \cdot 13 - 4 \cdot 5 - 1 \cdot 5 \Rightarrow 2 \cdot 13 - 5 \cdot 5$$

$$1 = 3 - 1 \cdot (5 - 1 \cdot 3) \Rightarrow 3 - 1 \cdot 5 + 1 \cdot 3 \Rightarrow 2 \cdot 3 - 1 \cdot 5$$

$$2 = 3 - 1 = 2$$

$$2 = 5 - 1 \cdot 3$$

3.b) $\varphi(\mathbb{Z}_{20}) = \varphi(20) \Rightarrow \varphi(5 \cdot 2^2) \Rightarrow 4 \cdot 2 = 8 \quad \varphi(2) = 4 - 1 = 3$

3.c) $\varphi(60) = \varphi(5 \cdot 3 \cdot 2) = 16$ controllo $\text{MCD}(16, 1387)$

$$1387 = 23 \cdot 60 + 7$$

$$60 = 8 \cdot 7 + 4$$

$$7 = 1 \cdot 4 + 3$$

$$4 = 1 \cdot 3 + 1 \quad \text{OK}$$

$$3 = 3 \cdot 1 + 0$$

$$4 \cdot 2 \cdot 2$$

$$34 = 2 \cdot 16 + 2$$

$$34 \mid 16$$

$$\begin{array}{r} 32 \\ 2 \\ \hline 2 \\ \hline \end{array}$$

$$\begin{array}{r} 16 \\ 2 \\ \hline 2 \\ \hline \end{array}$$

$$(1387^{\frac{16}{2}}) \cdot 1387^2$$

$$\Leftrightarrow 7^2 = 1 \pmod{60}$$

$$(7^{\frac{16}{2}})^2 \equiv 49 \pmod{60}$$

MD • SICULA "LE" - 3

Esercizio 1. Alle semifinali olimpiche degli 800 metri piani sono ammessi i 24 atleti con i tempi migliori delle qualificazioni. Gli atleti sono poi distribuiti in tre semifinali da 8. Determinare il numero di modi in cui possono essere scelti gli atleti per la prima semifinale nei casi seguenti:

- a) non si richiede nessuna condizione, tutte le possibilità sono ammesse;
- b) in ciascuna semifinale devono essere presenti 2 dei 6 atleti coi tempi migliori;
- c) 8 atleti in semifinale sono europei (e 16 non europei) e in ciascuna semifinale devono essere presenti non più di 3 atleti europei.

A = atleti: $|A| = 24$

1.a.b $|A_1| = 6 \quad A_{1-24}$

2.c

$$\frac{16 \cdot 15 \cdot 14 \cdot 13 \cdot 12}{3!} \quad \text{atleti non eu}$$

$16 + 8 = 14$ atleti tra europei e non

Loco 1 semifinale delle 8 atleti

Combinazioni

$$C_{24,8} = \binom{24}{8} = \frac{24!}{8! \cdot 16!} = \frac{24 \cdot 23 \cdot 22 \cdot 21 \cdot 20}{8!} \quad \text{OK}$$

1.a.b $|A_1| = 6 \quad A_{1-24}$

Per la prima semif.

$$\frac{6 \cdot 5}{2!} \cdot \binom{22}{6} = 6 \cdot 5 \cdot \frac{22!}{6! \cdot 16!} \quad \text{OK}$$

(OK)

Esercizio 2. Si considerino i seguenti cicli in S_8 :

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 7 & 6 & 8 & 4 & 2 & 1 & 5 & 3 \end{pmatrix} \quad \tau = (1 \ 7 \ 5 \ 2 \ 6).$$

a) Calcolare la decomposizione in cicli disgiunti di σ , σ^2 e $\sigma \circ \tau$

b) Fornire esempi di elementi di S_8 con periodo 6, 10, 13, oppure spiegare perché tali elementi non esistono.

c) Verificare che la funzione $f: S_{10} \rightarrow S_8$ con $f([k]) = \tau^{3k}$ è ben definita ed è un omomorfismo di gruppi da $(\mathbb{Z}_{10}, +)$ a (S_8, \circ) . Elencare tutti gli elementi nucleo.

$$\sigma \circ \tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 7 & 6 & 3 & 4 & 2 & 1 & 5 & 8 \\ 5 & 1 & 8 & 4 & 6 & 7 & 2 & 3 \end{pmatrix} \quad \text{OK} = (1, 5, 6, 7, 2) \cdot (3, 8)$$

2.b Periodo 6 $\Rightarrow \pi \in S_8$ composte da cicli con $\text{mcm}(\text{Tipo}(\pi)) = 6$
 es: $\pi = (1, 2, 3, 4, 5, 6) \quad \text{mcm}(\pi) = 6$

Periodo 10 $\Rightarrow \pi \in S_8 \Leftrightarrow \text{mcm}(\text{Tipo}(\pi)) = 10$ Per def.

il periodo è il numero di applicaz. della permutazione per ritrovare l'identità. Ma siccome dopo 18 il ciclo si ripete, allora il periodo di 10 non esiste o bensì è equivalente al periodo di 2.
 $\pi = (1, 2)$ in S_8

Periodo 13 \Rightarrow In maniera analoga periodo di π in S_8 NON esiste
 per cui è eq. a $13-8=5$

$$\pi = (1, 2, 3, 4, 5)$$

2.c) f ben def? $[k]_{10}$ è nella forma $k+10n$, per cui $f(k+10n) = \tau^{3(k+10n)} = \tau^k \cdot \tau^{30n} \Rightarrow \tau^k \cdot (\tau^3)^{10n}$ Verificato

τ ha periodo 6

omomorfismo sic

$$f([k]_{10} + [k']_{10}) = f([k]_{10}) \cdot f([k']_{10}) \quad \text{Verificato}$$

$$f\left(\frac{[k+k']_{10}}{3^{(k+k')/10}}\right) = \tau^k \cdot \tau^{3 \cdot k'} = \tau^{k+3 \cdot k'} = f([k+k']_{10})$$

~~$\text{Kernel}(f) = \{k \in \mathbb{Z}_{10} \mid f(k) = 1\}$~~

~~$\frac{10}{1} / 2 = \{0, 5, 10\}$~~

Il Kernel si trova tramite l'ordine di σ

$\sigma = \text{mcm}(S_2) = 10$ ovvero $\sigma^0 = \text{Id}$ e nella funzione σ^{3k} quando $3k \neq 0$

In \mathbb{Z}_{10} , k è multiplo di 10 quando $k=0$ oppure multiplo $\frac{10}{\text{mcd}(10, 3)} = \frac{10}{1} = 10$ da cui

Esercizio 3. a) Calcolare la cifra finale del numero $7^{777} + 3^{333}$.

b) Risolvere la congruenza $40x \equiv 3 \pmod{1183}$.

c) Determinare il numero degli elementi invertibili nell'anello $\mathbb{Z} \times \mathbb{Z}_2 \times \mathbb{Z}_2$.

3.c. Uso l'ω per l'ultima cifra

$$\varphi(10) = \varphi(5 \cdot 2) = 4 \cdot 1 = 4$$

494

$$7^{777} = 194 \cdot 4 + 1 \rightarrow 7^{183} \Rightarrow (\cancel{7}) \cdot 7 \Rightarrow 7 \pmod{10} \quad \omega \pmod{10}$$
$$3^{333} = 83 \cdot 4 + 1 \rightarrow (3^4)^{83} \cdot 3^1 \Rightarrow 3 \pmod{10} \quad \text{OK} \quad \boxed{0}$$

3.b) Controllo se invertibile \Rightarrow

$$1 = 7 \cdot (1183 - 207 \cdot 40) - 4 \cdot 40 \Rightarrow 7 \cdot 1183 - 207 \cdot 40 - 4 \cdot 40 \Rightarrow$$

$$\uparrow 1 = 3 \cdot 23 - 4 \cdot (40 - 1 \cdot 23) \Rightarrow 3 \cdot 23 - 4 \cdot 40 + 4 \cdot 23 \Rightarrow 7 \cdot 23 - 4 \cdot 40$$

$$1 = 3 \cdot (23 - 1 \cdot 17) - 1 \cdot 17 \Rightarrow 3 \cdot 23 - 3 \cdot 17 - 1 \cdot 17 \Rightarrow \underline{3 \cdot 23 - 4 \cdot 17}$$

$$1 = 6 - 1 \cdot (17 - 2 \cdot 6) \Rightarrow 6 - 1 \cdot 17 + 2 \cdot 6 \Rightarrow \underline{3 \cdot 6 - 1 \cdot 17}$$

$$\underline{1 = 6 - 1 \cdot 5} \quad S = 17 - 2 \cdot 6$$

$$1183 = 29 \cdot 40 + 23$$

$$40 = 1 \cdot 23 + 17$$

$$23 = 1 \cdot 17 + 6$$

$$17 = 2 \cdot 6 + 5$$

$$6 = 1 \cdot 5 + 1 \rightarrow \text{Invertibile}$$

$$S = 5 \cdot 1 + 0$$

$$\underline{1 = 7 \cdot 1183 - 207 \cdot 40 \Rightarrow -207 \cdot 40}$$

$$\cancel{-207 \cdot 40} \cdot \cancel{40} \times \underline{\underline{1}} \equiv \underline{\underline{1}} \cdot \cancel{-207 \cdot 40} \pmod{1183}$$

OK

3.c)

$$\varphi(\mathbb{Z}) \cdot \varphi(\mathbb{Z}_2) \cdot \varphi(\mathbb{Z}_2) =$$

4

\mathbb{Z} ha un numero inf. di elementi invertibili. tutte le
combinazioni sono delle forme $(x, \underbrace{y_1, \dots, y_n}_{\text{OK}})$

MP • SIMULIA "17"-4

Esercizio 1 (3+3+4). Un florista vende rose di 5 colori diversi (rosa, rosse, gialle, bianche e azzurre).

- Volendo acquistare un mazzo bicolore, quanti sono i possibili abbinamenti di colore?
- Di quante rose deve essere costituito un mazzo per essere sicuri che ve ne siano almeno 5 dello stesso colore?
- Quanti mazzi distinti di 12 rose si possono formare se si vuole che tutti i colori siano presenti?

$$|\text{Colori}| = 5$$

a) Scegliere 2 colori : ~~$S \cdot 4$~~

~~1 rosa tra 5 colori~~

~~Nope! Usare Combinazioni~~
 $C_{S,2} = \frac{S!}{2!(S-2)!} = \frac{S \cdot (S-1) \cdot (S-2) \cdots 1}{2 \cdot 1 \cdot (S-2) \cdots 1} = \frac{S(S-1)}{2 \cdot 1} = \frac{S(S-1)}{2}$

b) Se ci sono S per ogni colore si ha bisogno di un totale di

$$\underbrace{S \cdot S}_{\substack{\text{S rose del} \\ \text{primo colore}}} \cdot \underbrace{S \cdot 4}_{\substack{\text{S rose del 2^o} \\ \dots}} \cdot S \cdot 3 \cdot S \cdot 2 \cdot S \cdot 1 \Rightarrow S^5 \cdot S! \quad \text{Nope! Il Testo chiede} \\ \text{che almeno 1 colore abbia} \\ S \text{ elementi, non tutte le } S.$$

Se ne sceglie 1 per colore avrà $4 \cdot S = 20$
 se ne aggiungo 1, allora almeno 1 colore avrà S elem.

c) ~~$S \cdot 4 \cdot 3 \cdot 2 \cdot 1$~~ $\circ \binom{18}{14} = S! \cdot \frac{18!}{14! \cdot 4!} \quad \text{Nope!}$

~~S Fiori di
 S colori diff.~~

~~$18 - S = 7$ le rimanenti~~

$$S \circ \binom{7+S-1}{S-1} = \frac{7+S-1!}{(S-1)!} = \frac{14!}{4! \cdot 7!} = \frac{14 \cdot 13 \cdot 12 \cdot 11 \cdot 10 \cdot 9 \cdot 8 \cdot 7 \cdot 6}{4! \cdot 7!} \Rightarrow 330$$

Sono le rose
 di ogni mazzo

7 sono le rimanenti, ma il
 restrittivo calcolato su S de sono i
 colori, non su ~~12~~

Esercizio 2 (3+3+4). a) Determinare mediante l'algoritmo euclideo il massimo comune divisore d e il minimo comune multiplo D dei due numeri $a = 1377$ e $b = 1071$.

b) Determinare le ultime due cifre decimali (decine e unità) del numero 4597^{1003} .

c) Determinare tutte le soluzioni di ciascuna delle due congruenze lineari

- $38x \equiv 25 \pmod{42}$
- $25x \equiv 38 \pmod{42}$

$$2.a) \quad \text{MCD}(1377, 1071) = 153$$

$$1377 = 1 \cdot 1071 + 306$$

$$1071 = 3 \cdot 306 + 153$$

$$306 = 2 \cdot 153 + 0$$

$$2.b) \quad P(100) = P(S^2 \cdot 2^2) = 5 \cdot 4 \cdot 2 \cdot 1 = 40$$

$$1603 \mid 40 \Rightarrow 1603 = 4 \cdot 40 + 3$$

$$4 \cdot 40 + 3$$

$$4597 \Rightarrow (4597 \cdot 40) \cdot 4597^3 \Rightarrow 4597^3 \Rightarrow 4597^3 \pmod{100} = -3 \pmod{100}$$

le ultime 2 cifre non cambiano

$$\widehat{1603} \mid 40$$

$$160 \mid 40$$

$$3 \mid 40$$

$$45^3 \pmod{100} \rightarrow (47-100)^3 \pmod{100}$$

è corretto

$$-3^3 \rightarrow -27$$

OK

2.c) - Det. de inv.

$$42 \mid 38 \rightarrow 1 \cdot 38 + 4$$

$$38 \mid 4 \rightarrow 4 \cdot 4 + 0 \rightarrow \text{MCD}$$

$$4 \mid 2 \rightarrow 2 \cdot 2 + 0$$

$$45^3 \pmod{100} \rightarrow (47-100)^3 \pmod{100}$$

è corretto

$$-3^3 \rightarrow -27$$

OK

dlb? $25 \mid 12 \notin \mathbb{Z}$ Non Risolvibile

- Det. de inv.

$$42 \mid 25 \rightarrow 1 \cdot 25 + 17$$

$$25 \mid 17 \rightarrow 1 \cdot 17 + 8$$

$$17 \mid 8 \rightarrow 2 \cdot 8 + 1 \rightarrow \text{MCD inv.}$$

$$8 \mid 1 \rightarrow 1 \cdot 1 + 0$$

$$\text{Bezout} \rightarrow I = \overline{3 \cdot 42 - 5 \cdot 25}$$

l'inverso di 25 in \mathbb{Z}_{42} è -5

OK

$$1 = 3 \cdot (42 - 1 \cdot 25) - 2 \cdot 25 \rightarrow 3 \cdot 42 - 3 \cdot 25 - 2 \cdot 25 = \overline{3 \cdot 42 - 5 \cdot 25}$$

$$1 = 17 - 2 \cdot (25 - 1 \cdot 17) = 17 - 2 \cdot 25 + 2 \cdot 17 = 3 \cdot 17 - 2 \cdot 25$$

$$1 = 17 - 2 \cdot 8$$

$$17 = 42 - 3 \cdot 25$$

$$8 = 25 - 1 \cdot 17$$

Esercizio 3 (3+3+4). Sia σ la seguente permutazione di S_9 :

$$\sigma = (1\ 6\ 7\ 2)(3\ 5\ 9\ 4)(8\ 6).$$

a) Scrivere la decomposizione in cicli disgiunti di σ , σ^2 e di σ^3 .

b) Determinare il numero di elementi del sottogruppo ciclico $H := \langle \sigma \rangle < S_9$.

c) Si consideri l'applicazione $f : H \rightarrow S_9$ data da $f(\sigma^k) = \sigma^{9k}$. Si dimostri che f è un omomorfismo dei gruppi (H, \circ) e (S_9, \circ) e si determini il suo nucleo. Si verifichi che $Im(f)$ coincide con H stesso.

Soluzione.

④ $\sigma^3 = (1, 8, 2, 6, 7)(3, 9)$
 $(4, 5)$
 $\sigma^3 = (1, 7, 6, 2, 8)(3, 4, 9, 5)$

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 6 & 1 & 5 & 3 & 9 & 8 & 2 & 7 & 4 \\ 8 & 6 & 9 & 5 & 4 & 7 & 1 & 2 & 3 \\ 7 & 8 & 4 & 9 & 3 & 2 & 6 & 1 & 5 \end{pmatrix} \xrightarrow{\sigma^3}$$

3.b) $|H| = C_a =$ il periodo di $\langle \sigma \rangle = 20$

3.c) Determino se è valida H è sotto-gruppo ciclico di S_9 descrivibile come $\{id, \sigma, \sigma^2, \dots, \sigma^9\}$ per cui la sua mappa è rappresentabile come: σ^x

$$f(\sigma^x) = \sigma^{3 \cdot x} \quad \text{deve appartenere a } S_9. \text{ Verificato}$$

$$f(h^u \circ h^v) = f(h^u) \circ f(h^v)$$
$$f(h^u h^v)^{3m} = h^{3u} \cdot h^{3v}$$
$$(h^u h^v)^{3m} = h^{3u + 3v} \quad \underline{\underline{\text{SI}}}$$

$$\text{Kernel}(f) = \{x \mid f(x) = 0\}$$

$$\text{Kernel}(f) = \sigma^{3m} = 1$$

in cui $3m$ è multiplo di 20

$$m = 20t \quad (\sigma^{3t})^{20} = 1_{S_9} = 1_S$$
$$3 \cdot 20 \cdot t \quad f \text{ è iniettiva}$$

se così si mappa su H allora $20 = 20$

$$Im(f) = H$$