

MD • S10EVAL-10

Esercizio 1. Un negoziante vende 22 tipi diversi di capsule di caffè, distinguibili per colore.

1. (3 p.) Per allestire una vetrina il negoziante posiziona in fila una capsula di ciascun colore disponibile. Quanti modi ha di farlo?

2. (4 p.) Un cliente vuole acquistare 4 capsule di colori diversi. Quante sono le scelte possibili?

3. (4 p.) Per promozione i primi 8 clienti ricevono una capsula in regalo a loro scelta. Quante sono le possibili successioni di scelte di queste capsule regalo?

$$1.a \quad 22^8$$

(Q) u

Esercizio 2. Consideriamo le seguenti due permutazioni di S_7 date come prodotto di cicli:

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

1. (p. 4) Determinare la decomposizione in cicli disgiunti di σ e τ .

2. (p. 3) Calcolare il periodo di σ , τ e $\sigma\tau$.

3. (p. 4) Stabilire se la funzione $f : \langle\sigma\rangle \rightarrow \mathbb{Z}_{18}$ definita ponendo $f(\sigma^k) = \bar{3}k$ per ogni $k \in \mathbb{Z}$ è ben definita, se è un omomorfismo, se è iniettiva e se è suriettiva.

1.a 22! modi di ri-ordinare gli elementi

$$1.b \quad \binom{22}{4}$$

possibilità

2.a

$$\sigma = (1\ 2\ 4\ 3\ 7\ 6)$$

$$\tau = (1\ 6\ 3\ 2)(4\ 5)$$

(Q) u

$$2.b \quad \text{Tipol}(\sigma) = 6 \quad P(\sigma) = 6, \quad \text{Tipol}(\tau) = (4, 2) \quad P(\tau) = \text{lcm}(4, 2) = 4$$

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

(Q) u

$$2.c \quad \langle\sigma\rangle = \{ \text{id}, \sigma, \sigma^2, \sigma^3, \sigma^4, \sigma^5 \} \quad \text{ovvero } \sigma^k \text{ per } k \geq 0 \wedge k \leq 5$$

Ma siccome $P(\sigma) = 6$ per 2b $n \in \mathbb{Z}_{18}$ sse $n = y + 18t$

$P(\sigma) \mid 18$ per cui ogni n di σ^k può essere rappresentata in $[\mathbb{Z}]_{18}$

$$\overline{3 \cdot k} = \overline{0} \quad \text{in } \mathbb{Z}_{18}$$

$$f(\sigma^k \cdot \sigma^{k'}) = f(\sigma^k) + f(\sigma^{k'})$$

$$\text{Kernel}(f) = \{k \in \mathbb{Z} \mid f(\sigma^k) = \overline{0}\}$$

$$\frac{f(\sigma^{k+k'})}{3 \cdot (k+k')} = \frac{\overline{3k} + \overline{3k'}}{3 \cdot (k+k')}$$

$$= \overline{4 \cdot 0}, \overline{6 \cdot 6}$$

$$\overline{6 \cdot 6} = \overline{0}$$

$$18 - P(\sigma) \neq 0 \quad \text{ovvero}$$

$$= \{ \overline{0} \} \leftrightarrow \underline{\text{f è iniettiva}}$$

(Q) u

il periodo di σ non è in grado di coprire tutto \mathbb{Z}_{18} . \leftrightarrow non è suriettiva

Esercizio 3. 1. (p. 4) Applicando l'algoritmo euclideo determinare MCD(57, 25) e realizzare l'identità di Bezout.

2. (p. 4) Calcolare il resto della divisione per 38 del numero 5^{561} .

3. (p. 3) Stabilire se il gruppo $\mathbb{Z}_9 \times \mathbb{Z}$ è ciclico o no.

$$\text{MCD}(57, 25) = 1$$

$$x \quad y$$

$$1 = 16 \cdot 25 - 7 \cdot 57$$

(6w)

$$3.1 \quad 57 = 2 \cdot 25 + 7 \quad \Delta \quad 1 = 2 \cdot 25 - 7 \cdot (57 - 2 \cdot 25) = 12 \cdot 25 - 7 \cdot 57 + 14 \cdot 25$$

$$25 = 3 \cdot 7 + 4 \quad 1 = 2 \cdot (25 - 3 \cdot 7) - 1 \cdot 7 \Rightarrow 2 \cdot 25 - 6 \cdot 7 - 1 \cdot 7 = 2 \cdot 25 - 7 \cdot 7$$

$$7 = 1 \cdot 4 + 3 \quad 1 = 4 - 1 \cdot (7 - 1 \cdot 4) \Rightarrow 4 - 1 \cdot 7 + 1 \cdot 4 \Rightarrow 2 \cdot 4 - 1 \cdot 7$$

$$4 = 1 \cdot 3 + 1 \quad 1 = 4 - 1 \cdot 3$$

$$3 = 3 \cdot 1 + 0 \quad 3 = 7 - 1 \cdot 4 \quad 4 = 2 \cdot 25 - 7 \cdot 7$$

$$7 = 57 - 2 \cdot 25$$

$$3.2 \quad \varphi(38) = \varphi(2 \cdot 19) = 18$$

$$\text{MCD}(18, 5) = 1$$

$$38 = 7 \cdot 5 + 3$$

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

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

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

$$561 = 31 \cdot 18 + 3 \Rightarrow 5^{561} \equiv 3^3 \pmod{38} \Rightarrow 125 \pmod{38}$$

$$\begin{array}{r} 25 \\ 125 \\ \hline 114 \\ \hline 11 \end{array} \quad \begin{array}{r} 18 \\ 36 \\ \hline 18 \\ \hline 0 \end{array}$$

$$\begin{array}{r} 18 \\ 36 \\ \hline 18 \\ \hline 0 \end{array} \quad \begin{array}{r} 18 \\ 36 \\ \hline 18 \\ \hline 0 \end{array}$$

$$\begin{array}{r} 11 \pmod{38} \\ 18 \\ \hline 18 \\ \hline 0 \end{array} \quad \begin{array}{r} 1 \\ 18 \\ \hline 18 \\ \hline 0 \end{array} \quad \begin{array}{r} 1 \\ 18 \\ \hline 18 \\ \hline 0 \end{array}$$

$$\begin{array}{r} 1 \\ 38 \cdot 3^8 \\ \hline 2 \\ \hline 76 \cdot 144 \end{array}$$

$$\begin{array}{r} 1 \\ 108 \\ \hline 18 \\ \hline 108 \\ \hline 0 \end{array}$$

3.3.

\mathbb{Z} è gruppo ciclico infinito
per cui $\mathbb{Z}_q \times \mathbb{Z}$ non può essere
ciclico in quanto \mathbb{Z}_q non è infinito

Esercizio 1. Un giardiniere ha a disposizione 12 tipi diversi di piante per adornare un giardino

1. (3 p.) Per una piccola aiuola deve scegliere 5 piante di tipo diverso. Quante possibili scelte ha dei 5 tipi?
2. (4 p.) In un'aiuola grande deve piantare 15 piante, però mettendo almeno una pianta per tipo. Quante sono le possibili scelte delle 15 piante?
3. (4 p.) Lungo uno dei muri di cinta deve mettere 24 piante, 2 per tipo. Quanti modi ha di farlo?

$$|P|=12$$

$$(a) \binom{12}{5}$$

1.b) $\downarrow \cdot \left(\frac{12+3-1}{3} \right) \downarrow \cdot \frac{12-1}{3!}$

\downarrow tipo per
pianta

1.c) ~~$12 \cdot 11 \cdot 10 \cdot 9 \cdot 8 \cdot 7$~~

equivalente ad
aumentare in cui
ogni parola è ripetuta
volte = $\frac{24!}{2^{12}}$

Esercizio 2. Consideriamo la seguente permutazione di S_9 :

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

1. (p. 4) Determinare la decomposizione in cicli disgiunti di σ , σ^{-1} e σ^2 .
2. (p. 3) Determinare tipo e parità di σ , σ^{-1} e σ^2 .
3. (p. 4) Stabilire se la funzione $f: \mathbb{Z}_{10} \rightarrow S_9$ definita ponendo $f(\bar{k}) = \sigma^{3k}$ per ogni $k \in \mathbb{Z}$ è ben definita, se è un omomorfismo, se è iniettiva e se è suriettiva.

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

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

2.2) $\text{Tipolo}(\sigma) = (2, 3, 3)$, $P(\sigma) = P + P + P$

$$\rightarrow \begin{matrix} \swarrow 4 \\ \searrow 5 \\ \swarrow 6 \\ \searrow 7 \end{matrix} \quad \begin{matrix} \swarrow 4 \\ \searrow 5 \\ \swarrow 6 \\ \searrow 7 \end{matrix}$$

$\begin{matrix} \swarrow 4 \\ \searrow 5 \\ \swarrow 6 \\ \searrow 7 \end{matrix}$ $\begin{matrix} \swarrow 4 \\ \searrow 5 \\ \swarrow 6 \\ \searrow 7 \end{matrix}$

2.3) $n \in \mathbb{Z}_{10}$ $n = q + 30t$

$$P(\sigma) = 6$$

$$[\alpha]_0 = [b]_{10} \rightarrow f([\alpha]_0) = f([b]_{10})$$

$$\begin{aligned} \sigma^a &= b \\ \text{s.t. } a - b &= 0 \\ \text{s.t. } 10 &\mid a - b \\ \text{s.t. } 3 &\mid a - b \end{aligned}$$

$$f(\bar{\alpha}) = \frac{3\alpha}{\sigma} = \frac{3(b+30)}{\sigma} = \frac{3b+30}{\sigma}$$

quindi è ben def.
 $\frac{3b}{\sigma} = f(b)$

$$f(\bar{\alpha} + \bar{b}) = f(\bar{\alpha}) \cdot f(\bar{b})$$

$$\begin{aligned} \frac{3(\alpha+b)}{\sigma} &= \frac{3\alpha}{\sigma} \cdot \frac{3b}{\sigma} \\ &= f(\bar{\alpha}) \cdot f(\bar{b}) \end{aligned}$$

$$\text{Kernel}(f) = \{ \bar{n} \mid \bar{\sigma}^n = \text{id} \} = \{ \bar{0}, \bar{1}, \dots \}$$

non è iniettiva

$$\begin{aligned} 30 &= 5 \cdot 6 + 0 \\ \bar{\sigma}^0 &= \text{id}_\sigma \end{aligned}$$

$$10 - P(\sigma) \neq 0$$

Non è suriettiva

Esercizio 3. 1. (p. 4) Scivere il numero $224_{[6]}$ (scritto in base 6) in notazione binaria.

2. (p. 3) Tra i seguenti gruppi uno è ciclico. Dire quale e trovarne i generatori:

$$\mathbb{Z}_2 \times \mathbb{Z}_5, \quad \mathbb{Z}_2 \times \mathbb{Z}_6, \quad \mathbb{Z}_2 \times \mathbb{Z}_{10}.$$

3. (p. 4) Calcolare tutte le soluzioni della congruenza $14x \equiv 6 \pmod{20}$.

3.1

$$\begin{array}{r} 1 \\ 2 \quad 4 \\ 26+2 \cdot 6+4 \cdot 6 \\ = 72+12+4 = [88]_{20} \end{array}$$

(Q)

$$64 \quad 32 \quad 16 \quad 8 \quad 4 \quad 2 \quad 1$$

$$88 = 1011000$$

3.2

$\text{MCD}(2,5)=1$ $\mathbb{Z}_2 \times \mathbb{Z}_5$ è ciclico i generatori sono tutti i $(a,b) \in \mathbb{Z}_2 \times \mathbb{Z}_5$ tali che

$$\text{MCD}(a,2) = \text{MCD}(b,5) = 1$$

$$\text{MCD}(1,2) = 1, \quad \text{MCD}(3,5) = 1$$

$(\overline{1}, \overline{3})$ è generatore di $\mathbb{Z}_2 \times \mathbb{Z}_5$
 $(\overline{1}, \overline{1}), (\overline{1}, \overline{2}), (\overline{1}, \overline{4})$.

3.3

$\text{MCD}(14,20) = 2$ 14 non è invertibile in \mathbb{Z}_{20}

$$20 = 1 \cdot 14 + 6 \quad 2 \mid 6 \quad \text{per cui si può ridursi come}$$

$$\begin{aligned} 14 &= 2 \cdot 6 + 2 \\ 6 &= 3 \cdot 2 + 0 \end{aligned} \quad \begin{aligned} \frac{1}{7} \frac{1}{14} x &\equiv \frac{1}{2} \pmod{\frac{1}{2}} \\ \text{in } \mathbb{Z}_{10} \quad \frac{1}{7} x &\equiv 3 \pmod{10} \quad \text{Bezout} \end{aligned}$$

$$\begin{aligned} \overline{1} &= \overline{3 \cdot 7 - 2 \cdot 10} \quad \overline{7} \cdot \overline{10} = \overline{0} \quad \text{MCD}(7,10) = 1 \\ \overline{1} &= \overline{3 \cdot 7} \quad \overline{3} \text{ è inv.} \quad \overline{10} = \overline{1} \cdot \overline{7} + \overline{3} \end{aligned}$$

$$\begin{aligned} \text{di } \overline{7} \text{ in } \mathbb{Z}_{10} \quad \overline{7} &= 2 \cdot 3 + \overline{1} \\ 3 &= 3 \cdot 1 + 0 \end{aligned}$$

$$\overline{1} = \overline{3} \cdot \overline{7} - \overline{2} \cdot \overline{10}$$

$$\overline{1} = \overline{7} - \overline{2} \cdot (\overline{10} - \overline{3}) = \overline{7} - \overline{2} \cdot \overline{10} + \overline{2} \cdot \overline{3}$$

$$\overline{7} \cdot \overline{3} \cdot x = \overline{3} \cdot \overline{3} \pmod{10}$$

$$x = 9 \pmod{10} \rightarrow$$

$$= \{-21, -11, -1, 9, 19, 29, 7\}$$

$$\text{ovvero in } \mathbb{Z}_{20} = \{ 9, 19, 7 \}$$

Esercizio 1. 1. (4 p.) Contare gli interi compresi tra 1 e 4000 divisibili per 4 o per 10.

2. (4 p.) Contare gli anagrammi, anche privi di senso, della parola POLPETTONE.

3. (3 p.) Durante un gioco, 15 bambini devono mettersi in cerchio tenendosi per mano a gruppetti di 3 persone. In quanti modi lo possono fare?

$$1.2 \quad \sum = \{ p, o, l, e, t, n \} \quad |P| = 10 \quad \text{ANAGRAM} = \frac{10!}{2! \cdot 2! \cdot 1! \cdot 2! \cdot 2! \cdot 1!}$$

$$2.3 \quad |Q| = 15 \quad \binom{15}{3} \text{ i gruppi}$$

$$4. \quad X_u = \{x \in \mathbb{Z} \mid 4|x \wedge P(x)\} = \left\lceil \frac{4000}{4} \right\rceil = 1000$$

$$X_{10} = \{x \in \mathbb{Z} \mid 10|x \wedge P(x)\} = \left\lceil \frac{4000}{10} \right\rceil = 400$$

$$X_{u \cup 10} = \{x \in \mathbb{Z} \mid (20|x) \wedge (4|x \wedge P(x))\} = \{x \in \mathbb{Z} \mid 20|x \wedge P(x)\} = \left\lceil \frac{4000}{20} \right\rceil = 200$$

$$\frac{4 \cdot 10}{2} = 20$$

$$|X_u \cup X_{10}| = |X_u| + |X_{10}| - |X_{u \cup 10}| \\ = 1000 + 400 - 200 \\ = 1200$$

Esercizio 2. Consideriamo la seguente permutazioni di S_7 :

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

1. (p. 4) Determinare la decomposizione in cicli disgiunti di σ , τ , τ^2 , τ^3 e $\sigma\tau$.

2. (p. 4) Determinare il periodo di σ , τ^2 , τ^3 e $\sigma\tau$.

3. (p. 3) Stabilire se la funzione $f : \mathbb{Z}_2 \times \mathbb{Z}_3 \rightarrow S_9$ definita ponendo $f(\bar{a}, \bar{b}) = \sigma^{3a-2b}$ per ogni $a, b \in \mathbb{Z}$ è ben definita, se è un omomorfismo e se è suriettiva.

$$\begin{aligned} G &= (1 \ 2 \ 3 \ 4 \ 5 \ 6) \\ J &= (6 \ 7) (1 \ 2 \ 3 \ 4 \ 5 \ 6) (6 \ 7) \\ &= (1 \ 2 \ 3 \ 4 \ 5 \ 7) \end{aligned}$$

$$2.1 \quad \sigma^2 = (1 \ 2 \ 3 \ 4 \ 5 \ 6)^2 \quad J^2 = (1 \ 2 \ 3 \ 5) (2 \ 4 \ 7) \\ = (1 \ 3 \ 5) (2 \ 4 \ 6) \quad J^3 = (1 \ 4) (2 \ 5) (3 \ 7)$$

(O)

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

$$2.2) \quad \text{Tp}(\sigma) = 6 \quad \text{P}(\sigma) = 6 \quad \text{Tp}(\tau^2) = (3, 3), \quad \text{P}(\tau^2) = 3 \quad \text{Tp}(\tau^3) = (3, 2, 2) \\ \text{P}(\tau^3) = 2 \quad \text{Tp}(\sigma\tau) = 7 \quad \text{P}(\sigma\tau) = 7 \quad \text{Tp}(\sigma\tau) = 7$$

(O)

Esercizio 2. Consideriamo la seguente permutazione di S_7 :

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

1. (p. 4) Determinare la decomposizione in cicli disgiunti di σ , τ , τ^2 , τ^3 e $\sigma\tau$.

2. (p. 4) Determinare il periodo di σ , τ^2 , τ^3 e $\sigma\tau$.

3. (p. 3) Stabilire se la funzione $f : \mathbb{Z}_2 \times \mathbb{Z}_3 \rightarrow S_9$ definita ponendo $f(\bar{a}, \bar{b}) = \sigma^{3a-2b}$ per ogni $a, b \in \mathbb{Z}$ è ben definita, se è un omomorfismo e se è suriettiva.

23) Ben def: è ben definita se per $\bar{a}, \bar{b} \in \mathbb{Z}_2 \times \mathbb{Z}_3$, allora

$$f((\bar{a}, \bar{b})) = f((\bar{c}, \bar{d})) \iff \bar{a} = \bar{c} \wedge \bar{b} = \bar{d}$$

Ovvero

$$f((\bar{a}, \bar{b})) = \sigma^{3a+6b-2c-3d} \\ = \sigma^{3c+6t-2d+6t_2}$$

$$\text{ste } \frac{3a-2b}{3c-2d} = \sigma$$

$$\text{ste } 2 \mid a - c \wedge 3 \mid b - d$$

$$\text{se } \exists t \text{ t.c. } a = c + 2t \wedge 3t_2 \text{ t.c. } b = d + 3t_2$$

Seppiaccino però che per il punto 2.2 Periodo(σ) = 6 quindi

$$\sigma^{6t} = \sigma^0 \text{ quindi}$$

$$\sigma^{3c+6t-2d+6t_2} \Rightarrow \sigma^{3c-2d} = f(\bar{c}, \bar{d})$$

Verificata \square

23

Omomorfismo? $f(g * g) = f(g) * f(g)$?

$$f((a, b) + (c, d)) = f((a, b)) \circ f((c, d))$$

$$f((a+c, b+d)) = \sigma^{3a+2b} \circ \sigma^{3c-2d}$$

$$\sigma^{3(a+c)-2(b+d)} = \sigma^{3a-2b+3c-2d} \text{ (raccordo 3) } \Rightarrow \sigma^{3(a+c)-2(b+d)} \text{ Verificato}$$

Suriettiva

$\mathbb{Z}_2 \times \mathbb{Z}_3$ sono ciclici con $\text{MCD}(2, 3) = 1$ che è uguale al periodo di σ per cui riempiono σ è suriettiva

Come stabilire se $\mathbb{Z}_n \times \mathbb{Z}_m \rightarrow \sigma^{\mathbb{Z}}$ è suriettiva

1. Calcolare $|\mathbb{Z}_n \times \mathbb{Z}_m| = |\mathbb{Z}_n| \times |\mathbb{Z}_m|$

2. Se $|\mathbb{Z}_n \times \mathbb{Z}_m| = (S_n)!$ allora è suriettiva

Ovvero la dim delle permutazioni

In questo caso:

$$|\mathbb{Z}_n \times \mathbb{Z}_m| = 2 \cdot 3 = 6 \quad \text{e} \quad 6 \neq 9! \quad \text{perciò non}$$

$\sigma \in S_9$ è suriettiva

Esercizio 3. 1. (p. 4) Calcolare il resto della divisione per 20 di $7^{401} + 3^{402}$.

2. (p. 3) Calcolare gli elementi invertibili in $\mathbb{Z} \times \mathbb{Z}_{12}$ rispetto al prodotto componente per componente.

3. (p. 4) Risolvere l'equazione $2\bar{1}x = \bar{15}$ in \mathbb{Z}_{12} .

$$3.1) \quad \varphi(20) = \varphi(2 \cdot 5) = 2 \cdot 1 \cdot 4 = 8$$

$$\text{MCD}(7, 20) = 1 \quad \text{si può usare Euler}$$

$$20 = 2 \cdot 7 + 6$$

$$401 = 8 \cdot 50 + 1 \rightarrow 7 = 1 \cdot 7^1 \pmod{20} = 7 \pmod{20}$$

$$7 = 1 \cdot 6 + 1$$

$$6 = 6 \cdot 1 + 0$$

$$\text{MCD}(3, 20) = 1$$

si può usare Euler

$$20 = 6 \cdot 3 + 2$$

$$402 = 50 \cdot 8 + 2 \rightarrow 3 = 8 \cdot 3 \Rightarrow 3 \pmod{20}$$

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

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

$$\begin{array}{r} 401 \\ 40 \\ 50 \\ \hline 1 \end{array}$$

$$\begin{array}{r} 402 \\ 40 \\ 50 \\ \hline 2 \end{array}$$

Quindi

$$7+3 \pmod{20} \quad \text{OU}$$

$$16 \pmod{20}$$

3.2) Gli invertibili per $\mathbb{Z} \times \mathbb{Z}_2$ sono $\mathbb{Z} \times \mathbb{Z}_2^\times$ e sono equivalenti a $\mathbb{Z}^\times \times \mathbb{Z}_2^\times$ ovvero gli inv di \mathbb{Z} e \mathbb{Z}_2 . Per $\mathbb{Z}^\times = \{\pm 1\}$, per $\mathbb{Z}_2^\times = \{\bar{1}, \bar{5}, \bar{7}, \bar{11}\}$

a

b

$$\mathbb{Z}^\times \times \mathbb{Z}_2^\times = \{(\pm 1, \bar{1}), (\pm 1, \bar{5}), (\pm 1, \bar{7}), (\pm 1, \bar{11})\}$$

$$3.3) \quad 2\bar{1}x = \bar{15} \pmod{12}$$

$$\text{MCD}(2\bar{1}, 12) = 3 \quad 2\bar{1} \text{ non è invertibile in } \mathbb{Z}_2 \text{ ma}$$

$$2\bar{1} = \bar{1} \cdot 12 + q$$

$$3 \mid \bar{15} \text{ quindi } \bar{3}$$

$$12 = 1 \cdot q + 3$$

$$\bar{2}\bar{1}x = \bar{15} \pmod{12} \quad q$$

$$q = 3 \cdot 3 + 0$$

$$\bar{2}\bar{1}x = \bar{15} \pmod{12}$$

$$\bar{7}x = \bar{5} \pmod{4}$$

$$\text{MCD}(\bar{7}, 4) = 1$$

Bezout

$$\begin{array}{l} \bar{1} = 4 - 1 \cdot (\bar{7} - 1 \cdot 4) \rightarrow \bar{1} = 4 - 1 \cdot \bar{7} + 1 \cdot 4 \Rightarrow \bar{1} = 2 \cdot 4 - 1 \cdot \bar{7} \quad \bar{7} = 1 \cdot 4 + 3 \\ \bar{1} = 4 - 1 \cdot 3, \quad 3 = \bar{7} - 1 \cdot 4 \quad 4 = 1 \cdot 3 + 1 \\ \bar{3} = 3 \cdot 1 + 0 \end{array}$$

Quindi $\bar{1} = \bar{2} \cdot 4 - 1 \cdot \bar{7}$ in \mathbb{Z}_4 $\bar{4} = \bar{0}$

$$\bar{1} = -\bar{1} \cdot \bar{7} \text{ in } \mathbb{Z}_4 \rightarrow \bar{-1} \cdot \bar{7}x \equiv \bar{5} \cdot -1 \pmod{4}$$

$\bar{7} \pmod{4}$

$$x \equiv -5 \pmod{4}$$

Ovvero $4 \cdot \bar{-1} \cdot \bar{7}x \equiv \bar{5} \cdot -1$

$$x \equiv 3 \pmod{4}$$

$$\begin{array}{r} \bar{8} \\ \bar{4} \\ \bar{0} \\ \bar{4} \\ \bar{8} \\ \bar{0} \\ \hline \end{array}$$

$$-5 + 4 = -1 + 4 = 3$$

$$= \bar{7} \cdot \bar{3} \cdot \bar{1} \text{ in } \mathbb{Z}_{12}$$

$$\begin{array}{r} \bar{2} \\ \bar{4} \\ \bar{8} \\ \bar{0} \\ \hline \end{array}$$

Esercizio 1. 1. (4 p.) In una classe di una scuola materna ci sono 10 maschi ed 8 femmine. Per un gioco la maestra vuole scegliere un gruppetto di 4 facendo in modo che ci siano 2 maschi e 2 femmine. Quanti modi ha di farlo?

2. (3 p.) Un'azienda produce palline da ping-pong bianche, gialle, arancioni e rosse. Le distribuisce in confezioni da 8 in cui i colori sono mischiati a caso. Quante confezioni diverse per distribuzione di colori possono esistere?

3. (4 p.) Un hacker scopre che una password d'accesso ad un sito è un anagramma di

AACEHHHPPRZ
.....

che non inizia per E. Quante sono le possibili password che deve tentare?

$$|M|=10 \quad |F|=8$$

$$G \subseteq M \times M \times F \times F \quad \text{OU}$$

$$\text{61. Dovendo scegliere 2 maschi} \\ \hookrightarrow \binom{10}{2} \cdot \binom{8}{2} \quad \& \quad 2 \in F$$

1.2 $|T|=4$ sono commesse ripetizioni
 $g, u, r = \text{arg} \rightarrow \text{ordine non conta}$

$$C_4^1 = \binom{8+4-1}{4-1}$$

$$= \binom{11}{3}$$

$$1.3 \sum = \{ \underset{\text{a}}{2}, \underset{\text{c}}{2}, \underset{\text{e}}{2}, \underset{\text{h}}{3}, \underset{\text{p}}{1}, \underset{\text{r}}{2}, \underset{\text{z}}{2} \} \quad \text{Tutte sono } \frac{4!}{2!3!2!}$$

Sottraendo tutte quelle che iniziano per 'e'

$$\frac{10!}{2!3!2!} - \frac{10!}{2!3!2!}$$

OU

Esercizio 2. 1. (p. 4) Sia

$$\sigma = (3\ 8\ 1)(2\ 4\ 8\ 5)(3\ 5\ 6\ 7)(2\ 1\ 6\ 4\ 3) \in S_8.$$

Calcolare la decomposizione in cicli disgiunti ed il periodo di σ e σ^{-1} .

2. (p. 4) Sia σ la permutazione del punto precedente. Dire per quali $k > 0$ la permutazione σ^k è un ciclo

3. (p. 3) Di una permutazione $\tau \in S_{11}$ sappiamo che ha periodo 10. Quali potranno essere i tipi di τ ?

2.2) σ^k è ciclo e σ^n è composto da solo 1 ciclo disgiunto

2.3) $P(\tau) = \text{lcm}(\text{Tipo}(\tau))$ ovvero $\pm 10 = \text{lcm}(\text{Tipo}(\tau))$
ovvero $\{(40), (2,5), (2,2,5)\}$

$$2.1) \sigma = (1, 7, 8, 5, 6)(2, 3, 4)$$

$$\text{Tipo} = (S_3) \quad P(\sigma) = \text{lcm}(S_3) = 15$$

$$\sigma^{-1} = (3, 7, 8, 5, 6)^{-1} \cdot (2, 3, 4)^{-1}$$

$$= (1, 6, 5, 8, 7) \cdot (2, 4, 3)$$

$$\text{Tipo}(\sigma^{-1}) = (S_3) \quad P(\sigma^{-1}) = \text{lcm}(S_3) = 15 \leq 4$$

Esercizio 3. 1. (p. 4) Determinare le due cifre finali del numero $49^{67681} - 3^{53483}$.

2. (p. 3) Convertire in base 8 il numero $4021_{(6)}$ scritto in base 6.

3. (p. 4) Dimostrare che la funzione

$$f : \mathbb{Z}_{15} \rightarrow \mathbb{Z}_{18}, \quad f([x]_{15}) = [6x]_{18}$$

è ben definita ed è un omomorfismo. Dire poi se f è iniettiva o suriettiva.

3.1) Per 2 cifre finali $\text{e}(100)$
 $= \varphi(s^2 \cdot 2^2) = 5 \cdot 4 \cdot 2 = 40$

$$\begin{aligned} 67681/40 &\Rightarrow 170 \cdot 40 + 1 \rightarrow 170 = \frac{67681}{40} = \frac{170 \cdot 40}{40} \mod 100 \\ 53483/40 &\Rightarrow 1338 \cdot 40 + 3 \rightarrow 3 = \frac{53483}{40} = \frac{1338 \cdot 40 + 3}{40} \mod 100 \end{aligned}$$

$$= 40 - 27 \mod 100 \rightarrow 22 \mod 100 = (22) \quad \textcircled{Ou}$$

$$\begin{aligned} 3.2) [4021]_{15} &\rightarrow 1 \cdot 6 + 2 \cdot 6 + 0 \cdot 6^3 + 4 \cdot 6^4 \\ &\rightarrow 1 + 12 + 0 + 864 = [877]_{10} \quad \textcircled{Ou} \end{aligned}$$

$$877 = 10 \cdot 8 + 5 \rightarrow [877]_{10} = [555]_8,$$

$$10q = 13 \cdot 8 + 5$$

$$13 = 1 \cdot 8 + 5$$

$$1 = 0 \cdot 8 + 1$$

$$\begin{aligned} 3.3) f : \mathbb{Z}_{15} &\rightarrow \mathbb{Z}_{18} \text{ è ben definita se dati } [a]_{15}, [b]_{15} \rightarrow \bar{a} = \bar{b} \rightarrow \\ &\rightarrow \text{con } x = 15t + a \\ &x, y \in \mathbb{Z}_{15} \quad g = 15t + b \\ &18 | 15t \text{ quindi} \\ &\bar{a} = \bar{b} \text{ in } \mathbb{Z}_{18} \end{aligned}$$

$f(\bar{a}) = f(\bar{b}) \quad \text{sce } [6a]_{18} = [6b]_{18}$
 $\Rightarrow [6(15t+a)]_{18} = [6(15t+b)]_{18}$
 $\Rightarrow [6 \cdot 15t + 6a]_{18} = [6 \cdot 15t + 6b]_{18}$
 $\Rightarrow [90t + 6a]_{18} = [90t + 6b]_{18}$
 $\Rightarrow [6a]_{18} = [6b]_{18} \quad \underline{\text{Verificare}}$

$$\begin{aligned} \text{Omorfismo} \leftrightarrow f(\bar{a} + \bar{b}) &= f(\bar{a}) \cdot f(\bar{b}) \quad \underline{\text{Verificata}} \\ f(\bar{a} + \bar{b}) &= [6a]_{18} \cdot [6b]_{18} \\ [6(a+b)]_{18} &= \sum [6(a+b)]_{18} \quad 12 \cdot 6 = 72 \quad 72 \cdot 18 = 126 \end{aligned}$$

$$\begin{aligned} \text{Iniettiva} \leftrightarrow \text{Kernel}(f) &= \{ e_n \} \quad \rightarrow 1, 2, 3, \dots, 12 \quad \textcircled{Ou} \\ &= \{ n \in \mathbb{Z}_{15} \mid 6n = \bar{0} \text{ in } \mathbb{Z}_{18} \} \\ &= \{ 0, 3, 6, 9, 12 \} \quad \text{non è iniettiva} \end{aligned}$$

$$\begin{aligned} \text{Suriettiva} \leftrightarrow \text{Im}(f) &= \mathbb{Z}_{18} \quad \text{ma } |\mathbb{Z}_{15}| < |\mathbb{Z}_{18}| \quad \text{F} \underline{\text{non è}} \\ &\underline{\text{suriettiva}} \end{aligned}$$

Esercizio 1. 1. (4 p.) Su 180 iscritti all'appello unificato di MDL sappiamo che 106 hanno sostenuto il parziale di MD e 138 il parziale di L. Quanti studenti hanno sostenuto solo MD? Quanti solo L?

2. (3 p.) Quante sono permutazioni di tipo (4, 3, 3, 2) in S_{12} ? Quante in S_{14} ?

3. (4 p.) In un barattolo ci sono 12 caramelle di colore diverso. Sapendo che Alessia, Beatrice e Carla ne hanno prese rispettivamente a , b e c svuotando il barattolo, quante sono le possibili terne (a, b, c) , includendo anche il caso che qualche ragazza non abbia preso alcuna caramella?

$$\text{es1) } |I| = 180 = |\text{MD UL}| \quad \text{OK}$$

$$|\text{MD}| = 106 \quad |\text{MD UL}| = |\text{MD}| + |L|$$

$$|L| = 138 \quad - |\text{MD UL}|$$

$$|\text{MD}| = 106 - 64 \quad |\text{MD UL}| = 106 + 138 - 180$$

$$|\text{MD}| = 42 \quad = 64$$

$$|\text{L}| = 138 - 64 = 74$$

$$\text{1.2) Per } S_{12} \rightarrow \frac{12 \cdot 11}{2} \cdot \frac{10 \cdot 9 \cdot 8}{3} \cdot \frac{7 \cdot 6 \cdot 5}{3} \cdot \frac{4 \cdot 3 \cdot 2 \cdot 1}{4}$$

$$= \frac{12!}{2 \cdot 3 \cdot 2 \cdot 4} \cdot \frac{1}{2!} \quad \text{OK}$$

$$\text{Per } S_{14} \rightarrow \frac{14 \cdot 13}{2} \cdot \frac{12 \cdot 11 \cdot 10}{3} \cdot \frac{9 \cdot 8 \cdot 7}{3} \cdot \frac{6 \cdot 5 \cdot 4 \cdot 3}{4} \cdot \frac{1}{2!}$$

1.3) Combinaz con ripetizione di elementi di un insieme di 3 elementi presi 12 volte (questa non l'ho capita)

$$\binom{3+12-1}{3-1} = \binom{14}{2} = 7 \cdot 3$$

Esercizio 2. 1. (p. 4) Sia

$$\sigma = (1\ 3)(7\ 5\ 1)(4\ 7)(1\ 5\ 7)(3\ 1\ 2\ 9)(1\ 3)(6\ 7\ 8) \in S_9.$$

Calcolarne la decomposizione in cicli disgiunti, il tipo, la parità ed il periodo.

2. (p. 3) Sia σ la permutazione del punto precedente. Individuare un numero $k > 0$ per cui la permutazione σ^k abbia periodo 4. Individuare un $s > 0$ per cui σ^s abbia periodo 3.

3. (p. 4) Stabilire se la funzione $f : (\sigma^2) \rightarrow \mathbb{Z}_{12} : \sigma^{2k} \mapsto \overline{3k}$ è ben definita, un omorfismo, iniettiva e suriettiva.

2.1) OK

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

$$\text{Tipo}(\sigma) = (4, 2, 3) \quad \text{Parità}(\sigma) = \Delta + \Delta + P = P = \Delta + D = P$$

$$\text{Periodo}(\sigma) = \text{mcm}(4, 2, 3)$$

$$= \text{mcm}(4, 6) = 12$$

2.2) Periodo(σ^k) = 4 \Leftrightarrow Periodo($C_q^k \cdot C_q^k \circ C_q^k$) = 4 \Leftrightarrow $k \mid 12 \vee k \mid 3$

$$\text{Esempio con } k=3 : \sigma^3 = (1, 3, 2, 9)(4, 5)^3(6, 7, 8)^3$$

$$= (1, 3, 2, 9)(4, 5) \quad \text{Tipo}(\sigma^3) = (4, 2) \quad P(\sigma^3) = 4$$

Per avere $P(\sigma^k) = 3 \rightarrow k \mid 4$

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

$$= (6, 7, 8)$$

$$\forall a, b \in \mathbb{Z}$$

OK

2.3) Ben definita? $a = b \rightarrow f(\sigma^{2a}) = f(\sigma^{2b})$ OK

OK

applicando

$$\begin{aligned} & \text{sse } \sigma^{2a} = \sigma^{2b} \\ & \text{sse } \sigma^{2a-2b} = \text{id} \text{ sse} \\ & \text{sse } P(\sigma) \mid 2a - 2b \\ & \text{sse } \frac{12}{2} \mid 2a - 2b \\ & \text{sse } 6 \mid a - b \\ & \text{sse } 18 \mid 3a - 3b \\ & \text{Non ben def!} \end{aligned}$$

Esercizio 3. 1. (p. 4) Verificare che $\text{MCD}(11907, 1625) = 1$ e determinare la corrispondente identità di Bezout.

2. (p. 3) Dire quali delle seguenti funzioni che hanno \mathbb{Z} come dominio e codominio (pensato come gruppo additivo) sono omomorfismi:

$$f(n) = n^2 - n, \quad g(n) = -4n, \quad h(n) = |n|.$$

3. (p. 4) Calcolare il resto della divisione per 13 del numero 3^{780338} .

$$\begin{aligned} 3.1) \quad 11907 &= 7 \cdot 1625 + 532 \\ 1625 &= 3 \cdot 532 + 29 \\ 532 &= 18 \cdot 29 + 10 \\ 29 &= 2 \cdot 10 + 9 \\ 10 &= 1 \cdot 9 + 1 \\ 9 &= 9 \cdot 1 + 0 \end{aligned}$$

$$\begin{aligned} 3.2) \quad f(a+b) &= f(a) + f(b) \\ (a+b)^2 - (a+b) &\neq (a^2 - a) + (b^2 - b) \\ \text{Non è omomorfismo} \\ g(a+b) &= g(a) + g(b) \\ -u(a+b) &= -ua + ub \quad \text{S1} \\ -ua - ub &= -ua - ub \\ h(a+b) &= h(a) + h(b) \end{aligned}$$

$$|ab| = |a| + |b| \quad \text{No per es con } 5, -3$$

$$3.3) \quad \varphi(13) = 12$$

$$\text{MCD}(13, 3) = 1 \quad \text{Si pos oxire Eulero}$$

$$13 = 4 \cdot 3 + 1$$

quindi

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

$$3 = \frac{780338}{13} = 59268 \cdot 3^2$$

$$3 \mod 13$$

(C)

$$\text{MCD}(11907, 1625) = 1$$

Bezout

x y

$$\begin{aligned} 1 &= 1231 \cdot 1625 + 168 - 11907 \\ 1 &= 168 \cdot 532 - 55 \cdot 1625 \Rightarrow 55 \cdot 1625 + 168 - 11907 = 116 \cdot 1625 \\ 1 &= 3 \cdot 532 - 55 \cdot 29 \Rightarrow 3 \cdot 532 - 55 \cdot (1625 - 3 \cdot 532) = 3 \cdot 532 - 55 \cdot 1625 + 165 \cdot 532 \\ 1 &= 3 \cdot 10 - 1 \cdot 29 \Rightarrow 3 \cdot (532 - 18 \cdot 29) - 1 \cdot 29 = 3 \cdot 532 - 54 \cdot 29 + 29 \\ 1 &= 10 - 1 \cdot 9 \Rightarrow 1 = 10 - 1 \cdot (29 - 2 \cdot 10) = 10 - 1 \cdot 29 + 2 \cdot 10 \\ 9 &= 29 - 2 \cdot 10, \quad 10 = 532 - 18 \cdot 29, \\ 29 &= 1625 - 3 \cdot 532 \quad 532 = 11907 - 7 \cdot 1625 \end{aligned}$$

$$\begin{array}{r} 468 \\ 7 \\ \hline 1176 \\ 1176 \\ \hline 0 \end{array}$$

(C)

$$\begin{array}{r} 7 \\ 14, 21, 28, 35, 42, \\ 49, 56 \end{array}$$

$$\begin{array}{r} 1176 \\ 55 \\ \hline 1221 \end{array}$$