Esercizio 1. 1. (Punti 3) Calcolare il numero degli anagrammi della parola

PARALLELEPIPEDO.

2. (Punti 4) Si consideri l'insieme $\mathcal{A} = \{A, B, C, D, E, F, 1, 2, 3, 4\}$ i cui elementi sono lettere e cifre. Calcolare il numero degli ordinamenti di $\mathcal{A}$ in cui compaiono solo cifre nei due posti centrali.

3. (Punti 4) Sia $\mathcal{A}$ l'insieme del punto precedente. Calcolare il numero dei sottoinsiemi di A costituiti da 2 lettere e 3 cifre.

1.1) $\Sigma = \{ \overset{3}{p}, \overset{2}{a}, \overset{1}{r}, \overset{3}{l}, \overset{3}{e}, \overset{1}{i}, \overset{1}{d}, \overset{1}{o} \}$ $|\omega| = 15$ $P = \dfrac{15!}{3! \cdot 2! \quad 1 \cdot 3! \cdot 3!}$ ok

1.2) Devo scegliere 2 cifre su 4: $4 \cdot 3$
l'insieme sarà di 8 elem in cui
$\cancel{(6 \cdot 5 \cdot 4) \cdot (4 \cdot 3) \cdot (3 \cdot 2 \cdot 1)}$
~~le prime 3 lettere~~ cifre centrali Ultime lettere

le 8 rimanenti possono essere ordinati a piacere
$8! \cdot 12$

1.3) $\binom{6}{2} \cdot \binom{4}{3}$ ok

Esercizio 2. Si considerino le seguenti permutazioni in S_8:

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

1. (Punti 3) Scrivere σ, τ, $(\sigma \circ \tau)^{-1}$ come prodotto di cicli disgiunti e determinarne il periodo.
2. (Punti 4) Scrivere $(\sigma \circ \tau)^{9074}$ come prodotto di cicli disgiunti.
3. (Punti 4) Dimostrare che $H = \{\alpha \in S_8 : \alpha \circ \sigma = \sigma \circ \alpha\}$ è un sottogruppo di S_8. Esibire un elemento in H diverso dall'identità e un elemento che non appartiene ad H.

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

$$\begin{array}{l} \\ \tau \\ \sigma \end{array} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 1 & 5 & 7 & 4 & 6 & 2 & 8 & 3 \\ 4 & 3 & 6 & 2 & 7 & 8 & 1 & 5 \end{pmatrix}$$

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

2.2) $\text{Tipo}(\sigma \circ \tau) = 8$ $P(\sigma \circ \tau) = 8$ $(\sigma \circ \tau)^{9074} = \cancel{(\sigma \circ \tau)^{\overset{1134}{8}}} \circ (\sigma \circ \tau)^2$

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

2.3) - Per def $id_{S_8} \in S_8 \wedge Id \in H$ per $\sigma \circ id = \sigma = id \circ \sigma$
- $h \circ h' = (h \circ \sigma) \circ (h' \circ \sigma)$ sse $(h \circ \sigma) \circ (\sigma \circ h')$ sse $h \circ h'$ verificata
- $\forall h \in H \ \exists h^{-1} = h^{-1} \circ \sigma$ è inverso sse $(h \circ \sigma) \circ (h^{-1} \circ \sigma)$ sse $(h \circ \sigma) \circ (\sigma \circ h^{-1})$ sse $(h \circ h^{-1})$ sse id verificato

Se $h \circ \sigma = \sigma \circ h$ è vera quando $h = \sigma^k$
es: $\sigma^2 \Rightarrow \sigma^2 \circ \sigma = \sigma \circ \sigma^2 = \sigma^3$ ok

Altrimenti se diverso come τ $\tau \circ \sigma \neq \sigma \circ \tau$

Esercizio 3. 1. (Punti 4) Solo una tra le classi $\bar{5}$, $\bar{6}$ e $\overline{14}$ è invertibile in $\mathbb{Z}_{28}$. Dire quale e calcolarne l'inversa.

2. (Punti 4) Calcolare il resto della divisione di 7^{530} per 32.

3. (Punti 3) Si considerino le seguenti funzioni $\mathbb{Z}\times\mathbb{Z} \to \mathbb{Z}$ e si dica quali sono omomorfismi di gruppo e quali no.

$$f(a,b) = 5a - 2b, \qquad g(a,b) = 2a + 3b - 1, \qquad h(a,b) = a^2 - 5b.$$

3.1) È invertibile se co-prima

$MCD(28,5) = 1$ $\quad$ $\bar{5}$ è inv $\qquad$ $MCD(6,28) = 2$

$28 = 5\cdot 5 + 3$

$5 = 1\cdot 3 + 2$

$3 = 1\cdot 2 + \underline{1}$

$2 = 2\cdot 1 + 0$

OW

3.2) $\varphi(32) = \varphi(2^5) = 2^4\cdot 1 = 16$

$MCD(7,32) = 1$ $\quad$ si può usare eulero

$32 = 4\cdot 7 + 4$ $\qquad$ $530 = 33\cdot 16 + 2 \to 7^{530} = \cancel{7}^{16\cdot 33}\cdot 7^2 = 7^2 \bmod 32$

$7 = 1\cdot 4 + 3$ $\qquad$ $49 \bmod 32$

$4 = 1\cdot 3 + \underline{1}$ $\qquad$ $17 \bmod 32$

$3 = 3\cdot 1 + 0$

$530 : 16 = 33$; 48; 50; 48; 2 $\qquad$ $16\cdot 3 = 48$ $\qquad$ OW $\qquad$ $49 - 32 = 17$

3.3) $f((a,b)) = 5a - 2b$ è ben definita se $(a,b) = (c,d) \to f((a,b)) = f((c,d))$

$f((a,b)+(c,d)) = f((a,b))\circ f((c,d))$ $\qquad$ sse $(a,b)-(c,d) = (0,0)$

$f((a+c, b+d)) = 5a - 2b + 5c - 2d$ $\qquad$ sse $5a - 2b - (5c - 2d)$

$5(a+c) - 2(b+d) = 5(a+c) - 2(b+d)$ $\quad$ OW $\quad$ sse $5a - 2b - 5c + 2d = 0$ Verificato

Omomorfismo Verificato

$g((a,b)) = 2a + 3b - 1$ $\quad$ Ben def. se $(a,b) = (c,d) \to f((a,b)) = f((c,d))$

$f((a,b)+(c,d)) = f((a,b)) + f((c,d))$ $\qquad$ sse $(a,b)-(c,d) = (0,0)$

$f((a+c, b+d)) = 2a + 3b - 1 + 2c + 3d - 1$ $\qquad$ sse $2a + 3b - 1 - (2c + 3d - 1)$

$2(a+c) + 3(b+d) - 1 = 2(a+c) + 3(b+d) - 2$ $\quad$ Non è omomorfismo $\quad$ sse $\cancel{2a} + 3b - 1 - \cancel{2c} - 3d + 1$

sse $2a - 2c + 3b - 3d = 0$ Verificato

$h(a,b) = a^2 - 5b$ $\quad$ Ben def se $(a,b) = (c,d) \to h((a,b)) = h((c,d))$

sse $(a,b)-(c,d) = (0,0)$

$h((a,b)+(c,d)) = h((a,b)) + h((c,d))$ $\qquad$ sse $a^2 - 5b - (c^2 - 5d)$

$h((a+c, b+d)) = a^2 - 5b + c^2 - 5d$ $\qquad$ sse $a^2 - 5b - c^2 + 5d$

$(a+c)^2 - 5(b+d) \neq a^2 + c^2 - 5(b+d)$ $\quad$ Non Omomorfismo $\quad$ sse $a^2 - c^2 - 5b + 5d = 0$ Verificata

Esercizio 1. 1. (Punti 3) In quanti modi diversi 4 persone possono sedersi in una fila di 10 sedie?

2. (Punti 4) Un allenatore di calcio ha nella sua squadra 3 portieri, 8 difensori, 8 centrocampisti e 6 attaccanti. In quanti modi diversi può scegliere 1 portiere, 4 difensori, 4 centrocampisti e 2 attaccanti?

3. (Punti 4) Ho 15 monete da 1 euro e 4 salvadanai. In quanti modi diversi posso mettere tutte le monete nei 4 salvadanai in modo che nessun salvadanaio sia vuoto?

1.1) $10 \cdot 9 \cdot 8 \cdot 7$ ok

1.2) $\binom{3}{1} \cdot \binom{8}{4} \cdot \binom{8}{4} \cdot \binom{6}{2}$ ok

Modi di scegliere portiere; difensori; Centro-campisti; Attaccanti

1.3) $\cancel{\binom{15}{1} \cdot \binom{14}{1} \cdot \binom{13}{1} \cdot \binom{12}{1} \cdot 4}$

Distribuire una moneta per ogni salvadanaio. I restanti 11 possono essere suddivisi usando le combinazioni con ripetizione.

$C^r_{4,11} = \binom{11+4-1}{4-1} = \binom{14}{3}$

Esercizio 2. 1. (Punti 3) Calcolare la decomposizione in cicli disgiunti della permutazione

$$\sigma = (2\ 8\ 3\ 5)(1\ 7\ 4\ 3)(2\ 7\ 6) \in \mathcal{S}_8.$$

2. (Punti 4) Determinare tipo, periodo e parità della permutazione σ^2 (con σ del punto precedente).

3. (Punti 4) Si considerino le permutazioni $\alpha = (1\ 3\ 5\ 6)(2\ 4)$ e $\beta = (1\ 5)(3\ 6)(2\ 7\ 4)$ in $\mathcal{S}_8$. Calcolare $\langle\alpha\rangle \cap \langle\beta\rangle$.

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

2.2) $\sigma^2 = (1,7,6,8,3)^2(2,4,5)^2$ $\quad$ Tipo$(\sigma^2) = (5,3)$ $\quad$ Periodo$(\sigma^2) = 15$ ok

$= (1,6,3,7,8)(2,5,4)$ $\quad$ Parità$(\sigma^2) = P+P=0$

2.3) Date le permutazioni, il sotto-gruppo ciclico di S_8 generato da una permutazione sono tutte le permutazioni elevate a l in cui la β

$\langle\alpha\rangle = \{id, \alpha, \alpha^2, \alpha^3\}$ $\quad$ $\langle\beta\rangle = \{id, \beta, \beta^2, \beta^3, \beta^4, \beta^5\}$

solo $(1\,5)(3\,6)$ appare sia in $\langle a\rangle$ che in $\langle b\rangle$ (oltre l'id)

quindi $= \{id, (1\,5)(3\,6)\}$

Esercizio 3. 1. (Punti 3) Si consideri il gruppo $\mathbb{Z}_{24} \times \mathbb{Z}_{30}$, determinare l'ordine di $\langle(6,5)\rangle$ e $\langle(5,6)\rangle$.

2. (Punti 4) Determinare le soluzioni della congruenza $12x \equiv 16 \pmod{40}$ in $\mathbb{Z}_{40}$.

3. (Punti 4) Sia $(G,*)$ un gruppo ciclico di ordine 30 con generatore g, dimostrare che la seguente funzione è ben definita ed è un omomorfismo di gruppi

$$\varphi : G \longrightarrow \mathbb{Z}_{18}, \quad \varphi(g^k) = \overline{6k}.$$

Dire se si tratta di un omomorfismo iniettivo e/o suriettivo.

3.1)

3.2) $MCD(12,40)=4$

$40 = 3 \cdot 12 + \underline{4}$

$12 = 3 \cdot 4 + 0$

12 non è invertibile in $\mathbb{Z}_{40}$ ma $4 \mid 16$ per cui è semplificabile come

$3\cancel{\frac{12}{4}}x \equiv \cancel{\frac{16}{4}}_{4} \bmod \cancel{\frac{40}{4}}_{10}$

$MCD(3,10)=1$

$10 = 3 \cdot 3 + 1$

$3 = 3 \cdot 1 + 0$

ok

$\overline{1} = \cancel{\overline{10}} - 3 \cdot 3$

$\overline{1} = \overline{-3 \cdot 3}$ $\quad -3$ è inverso di 3 in $\mathbb{Z}_{10}$

$-3 \cdot 3x \equiv 4 \cdot -3 \bmod 10$

$x \equiv -12 \bmod 10$

$x \equiv 8 \bmod 10$

$[8]_{10} = \{\underset{-10}{-2}, \underset{0}{8}, \underset{10}{18}, \underset{20}{28} \dots\}$

Soluzioni $= \{\overline{8}, \overline{18}, \overline{28}, \overline{38}\}$ in $\mathbb{Z}_{40}$

3.3) $\underline{\text{Ben definito?}}$ $\quad g \in (G,*)$ può essere rappresentato come g^{k+30t} ← Periodo

dati $a, b \in (G,*) \wedge a=b \rightarrow a-b=0$

sse $a^{k+30t} - b^{k+30t} = 0$

sse $6(k+30t) - 6(k+30t) = 0$

sse $\overline{6k + 180t - 6k - 180t} = 0$ $\quad \overline{180t} = \overline{0}$ in $\mathbb{Z}_{18}$

sse $\overline{6k - 6k} = 0$ $\quad \underline{\text{ben definita}}$

Omomorfismo? Verificato

ok

$f(g^a * g^b) = f(g^a) + f(g^b)$

$f(g^{(a+b)}) = \overline{6a} + \overline{6b}$

$\overline{6(a+b)} = \overline{6(a+b)}$

$Kerrel(f) = \{g^k \in G \mid f(g^k) = \overline{0} \text{ in } \mathbb{Z}_{18}\}$

$= \{k \in \mathbb{Z} \mid 6k = \overline{18t} \text{ in } \mathbb{Z}_{18}\}$

$= \{0, 3, 6, 9, 12 \dots\}$ Non è iniettiva

$54 \mid 18$

$18 \cdot 2 = 36 \quad 18 \cdot 3 = 54$

$Im(f) = \{\overline{0}, \overline{6}, \overline{12}\} \neq \mathbb{Z}_{18}$

Non è suriettiva

Esercizio 1. I circoli di tennis "Laver" e "Rosewall" si sfidano su un match di 7 incontri: 4 singolari maschili, 2 singolari femminili ed un doppio misto. Il doppio misto è giocato da tennisti e tenniste già selezionate per i singoli.

1. Il circolo "Laver" ha 8 tennisti e 5 tenniste di buon livello tra cui selezionare la squadra. Quante sono le squadre possibili tra cui il "Laver" deve sceglierne una?
2. Formate le squadre, i partecipanti verranno accoppiati casualmente (tennisti con tennisti e tenniste con tenniste) per i 6 singolari e un tennista ed una tennista per squadra verranno sorteggiati per il doppio misto. Quanti sono teoricamente i possibili accoppiamenti fra le due squadre?
3. I sette incontri vengono disputati consecutivamente: prima i 4 singoli maschili, poi i 2 singoli femminili, poi il doppio. Quanti sono i possibili ordinamenti dei sette incontri?

1.1) $\binom{8}{4} \cdot \binom{5}{2}$ ok

1.2) Totale maschili = 4
escluso cuarcio
$4! \cdot 2! \cdot (2 \cdot 4)^2$

1.3) $4! \cdot 2! \cdot 1$ ok

Esercizio 2. 1. Risolvere la congruenza $15X \equiv 6 \bmod 33$ In $\mathbb{Z}_{33}$.

2. Verificare che il gruppo moltiplicativo $\mathbb{Z}_{11}^{\times}$ delle classi invertibili modulo 11 è ciclico e generato da $[2]_{11}$. Determinare tutti gli altri generatori.
3. Dimostrare che la funzione $f : \mathbb{Z}_{11}^{\times} \to \mathbb{Z}_{20}$, $f([2]_{11}^{k}) = [2k]_{20}$ è un omomorfismo iniettivo.

2.1) $MCD(15, 33) = \underline{3}$ Non è invertibile in $\mathbb{Z}_{33}$
$33 = 2 \cdot 15 + 3$ ma $3|6$ quindi
$15 = 5 \cdot 3 + 0$

ok

$-22 \quad -11 \quad 0 \quad 11 \quad 22 \quad 33$
$\Rightarrow \{ -15, -4, 7, 18, 29, 40 \ldots \}$
$\Rightarrow \{ \overline{7}, \overline{18}, \overline{29} \}$ in $\mathbb{Z}_{33}$

$\frac{15}{3} x \equiv \frac{6}{3} \bmod \frac{33}{3}$

$5x = 2 \bmod 11$ $\quad MCD(5, 11) = 1$
$\overline{1} = \overline{11 - 2 \cdot 5}$ $\quad 11 = 2 \cdot 5 + \underline{1}$
$\overline{1} = \overline{-2 \cdot 5}$ $\quad 5 = 5 \cdot 1 + 0$
$-2 \cdot 5 x \equiv 2 \cdot -2 \bmod 11$
$x \equiv -4 \bmod 11 \to 7 \bmod 11$

2.2) Elenco tutti gli elementi fino a n in $\mathbb{Z}_{11}$
$MCD(1, 10) = 1$ ✓ $\quad 11 = 11 \cdot \underline{1} + 0$
$MCD(2, 10) = 2$ ✗ $\quad \varphi(11) = 10$
$MCD(3, 10) = 1$ ✓ $\quad 10 = 3 \cdot 3 + 1$
$MCD(4, 10) \neq 1$
$MCD(5, 10) \neq 1$ $\quad \mathbb{Z}_{11} = \{ \overline{1}, \overline{3}, \overline{7}, \overline{9} \}$
$MCD(6, 10) \neq 1$
$MCD(7, 10) = 1$ Per elencare ~~gli invertibili di~~ $[2]_{11}$ bisognerebbe
$MCD(8, 10) \neq 1$ elencare 2^n in $\mathbb{Z}_{11}$
$MCD(9, 10) = 1$ $\Rightarrow \{$ $\quad 1, 2, 4, 8, 16, 32, 64, 128 \ldots$
$MCD(10, 10) \neq 1$ $\quad 1, 2, 4, 8, 5, 21, 53, 117 \ldots$

Sono i generatori tutti i n per $[2^n]_{11}$
t.c. $MCD(n, 11-1) = 1$
$\Rightarrow \{ 2, 13, 23, 43 \ldots \}$

Esercizio 2. 1. Risolvere la congruenza $15X \equiv 6 \bmod 33$ In $\mathbb{Z}_{33}$.

2. Verificare che il gruppo moltiplicativo $\mathbb{Z}_{11}^{\times}$ delle classi invertibili modulo 11 è ciclico e generato da $[2]_{11}$. Determinare tutti gli altri generatori.

3. Dimostrare che la funzione $f : \mathbb{Z}_{11}^{\times} \to \mathbb{Z}_{20}$, $f([2]_{11}^{k}) = [2k]_{20}$ è un omomorfismo iniettivo.

~~2.3 Ben Definita? Dati $a, b \in \mathbb{Z}_{11}^{\times}$~~ $a = b \to [2]_{11}^{h} = [2]_{11}^{k}$

~~sse $[2]_{11}^{h-k} = \overline{0}$ in $\mathbb{Z}_{11}$~~

~~sse $[2(h-k)]_{20} = \overline{0}$ in $\mathbb{Z}_{20}$~~

~~verificato~~

Spostata su MD1-Helper come caso d'uso

Esercizio 1. 1. (Punti 4) Verificare che $\mathrm{MCD}(142, 112) = 2$ e determinare la corrispondente identità di Bezout.

2. (Punti 4) Determinare l'inversa moltiplicativa di $\overline{56}$ in $\mathbb{Z}_{71}$.

3. (Punti 4) Elencare esplicitamente i generatori del gruppo additivo $(\mathbb{Z}_{18}, +)$.

1.1)

$142 = 1\cdot 112 + 30$ $\qquad 2 = \overset{x}{15}\cdot 142 - \overset{y}{19}\cdot 112$ $\qquad$ Bezout

$112 = 3\cdot 30 + 22$ $\qquad 2 = 15\cdot 30 - 4\cdot 112 \to 15\cdot(142 - 1\cdot 112) - 4\cdot 112 \to 15\cdot 142 - 15\cdot 112 - 4\cdot 112$

$30 = 1\cdot 22 + 8$ $\qquad 2 = 3\cdot 30 - 4\cdot 22 \to 3\cdot 30 - 4\cdot(112 - 3\cdot 30) \to 3\cdot 30 - 4\cdot 112 + 12\cdot 30$

$22 = 2\cdot 8 + 6$ $\qquad 2 = 3\cdot 8 - 1\cdot 22 \to 3\cdot(30 - 1\cdot 22) - 1\cdot 22 \to 3\cdot 30 - 3\cdot 22 - 1\cdot 22$

$8 = 1\cdot 6 + \underline{2}$ $\qquad 2 = 8 - 1\cdot 6 \to 8 - 1\cdot(22 - 2\cdot 8) \to 8 - 1\cdot 22 + 2\cdot 8$

$6 = 3\cdot 2 + 0$

$\mathrm{MCD}(142, 112) = 2$ $\qquad 6 = 22 - 2\cdot 8 \qquad 8 = 30 - 1\cdot 22 \qquad 22 = 112 - 3\cdot 30$

$30 = 142 - 1\cdot 112$

1.2) $\mathrm{MCD}(71, 56) = 1 \longleftrightarrow 56$ è invertibile in $\mathbb{Z}_{71}$

$71 = 1\cdot 56 + 15$ $\qquad 1 = 15\cdot 71 - 19\cdot 56 \to \bar{1} = \overline{\cancel{15\cdot 71} - 19\cdot 56}$ $\qquad \overline{-19\cdot 56} = \bar{1}$

$56 = 3\cdot 15 + 11$ $\qquad 1 = 15\cdot 15 - 4\cdot 56 \to 15\cdot(71 - 1\cdot 56) - 4\cdot 56 \to 15\cdot 71 - 15\cdot 56 - 4\cdot 56$

$15 = 1\cdot 11 + 4$ $\qquad 1 = 3\cdot 15 - 4\cdot 11 \to 3\cdot 15 - 4\cdot(56 - 3\cdot 15) \to 3\cdot 15 - 4\cdot 56 + 12\cdot 15$

$11 = 2\cdot 4 + 3$ $\qquad 1 = 3\cdot 4 - 1\cdot 11 \to 3\cdot(15 - 1\cdot 11) - 1\cdot 11 \to 3\cdot 15 - 3\cdot 11 - 1\cdot 11$ $\qquad -19$ è inverso

$4 = 1\cdot 3 + \underline{1}$ $\qquad 1 = 4 - 1\cdot 3 \to 4 - 1\cdot(11 - 2\cdot 4) \to 4 - 1\cdot 11 + 2\cdot 4$ $\qquad$ di $56 \bmod 71$

$3 = 3\cdot 1 + 0$ $\qquad 3 = 11 - 2\cdot 4 \qquad 4 = 15 - 1\cdot 11$ $\qquad \underline{-19 \bmod 71}$

$11 = 56 - 3\cdot 15 \qquad 15 = 71 - 1\cdot 56$ $\qquad 52$

1.3

generatori $= \{\bar{1}, \bar{5}, \bar{7}, \overline{11}, \overline{13}, \overline{17}\}$

$\mathrm{MCD}(1, 18) = 1$ $\quad \langle 1 \rangle_{18}$ generatore

$\mathrm{MCD}(2, 18) = 2$ $\quad \langle 2 \rangle$ non è generatore

$\mathrm{MCD}(3, 18) = 3$ $\quad \langle 3 \rangle$ non è ger.

$\mathrm{MCD}(4, 18) = 2$ $\quad \langle 4 \rangle$ non è

$\mathrm{MCD}(5, 18) = 1$ $\quad \langle 5 \rangle$ si

$\mathrm{MCD}(6, 18) = 6$ $\quad \langle 6 \rangle$ NO

$\mathrm{MCD}(7, 18) = 1$ $\quad \langle 7 \rangle$ si

$\mathrm{MCD}(8, 18) = 2$ $\quad \langle 8 \rangle$ no

$\mathrm{MCD}(9, 18) = 9$ $\quad \langle 9 \rangle$ no

$\mathrm{MCD}(10, 18) = 2$ $\quad \langle 10 \rangle$ NO

$\mathrm{MCD}(11, 18) = 1$ $\quad \langle 11 \rangle$ si

$\mathrm{MCD}(12, 18) = 6$ $\quad \langle 12 \rangle$ NO

$\mathrm{MCD}(13, 18) = 0$ $\quad \langle 13 \rangle$ no

$\mathrm{MCD}(14, 18) = 0$

$\vdots$

$\mathrm{MCD}(14, 17) = 1$

Esercizio 2. Consideriamo la permutazione $\pi = (3\ 7\ 8)(2\ 3\ 5)(1\ 4\ 5\ 6\ 9)(7\ 9) \in \mathcal{S}_9$

1. (Punti 4) Determinare tipo, periodo e parità di π.
2. (Punti 4) Qual è il più piccolo $k > 0$ tale che π^k è un ciclo?
3. (Punti 4) Dimostrare che la funzione $f : \langle\pi\rangle \to \mathbb{Z}_8$, $f(\pi^t) = \overline{2t}$ è un omomorfismo ben definito. È iniettiva? È suriettiva?

ok

2.1) $\pi = (1,4,2,7)(3,5,6,9,8)$ Tipo$(\pi) = (4,5)$ Parità$(\pi) = D+P \Rightarrow D$

Periodo$(\pi) = \text{mcm}(4,5) = 20$

2.2) Per definizione $\pi^k = C_4^k \cdot C_5^k$ quindi k deve essere tale da:

$k \mid 4 \vee k \mid 5$

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

ok

$= (3,8,9,6,5)$

2.3) Ben def?

dati $a,b \in \mathbb{Z}$ con $a=b \to \pi^a = \pi^b \longrightarrow f(\pi^a) = f(\pi^b)$

sse $\pi^{a-b} = id_{S_9}$

ok

sse $P(\pi) \mid a-b$

sse $20 \mid a-b$

sse $40 \mid 2(a-b)$

sse $40 \mid \underbrace{2a}-2b$

↳ è nella forma di f

Omomorfismo?

$f(\pi^a \circ \pi^b) = f(\pi^a) + f(\pi^b)$

$f(\pi^{a+b}) = \overline{2a} + \overline{2b}$

$\overline{2(a+b)} = \overline{2(a+b)}$ verificata

$\text{Kernel}(f) = \{\pi^t \mid f(\pi^t) = \overline{0} \text{ in } \mathbb{Z}_8\}$

Ovvero tutti i t tali che $2t = 18x \mod 8$

$= \{\overline{0}, \overline{8} \ldots\} \neq \{\overline{0}\} \longleftrightarrow$ non è iniettiva

$\text{Im}(f) = \{\overline{0}, \overline{2}, \overline{4}, \overline{6}\} \neq \{\overline{0}, \overline{1}, \overline{2}, \overline{3} \ldots\}$ Non è suriettiva

Turno 1, Problema 1: Una ditta associa ad ogni impiegato un codice numerico di 6 cifre. Calcolare il numero dei codici possibili in ciascuno dei casi seguenti.

1. (Punti 3) Un codice deve alternare cifre pari a cifre dispari e non può contenere cifre ripetute.
2. (Punti 4) Un codice non può cominciare con la cifra 0 ed inoltre la somma delle cifre che lo compongono deve essere pari.
3. (Punti 4) Un codice non può contenere la cifra 0 più di due volte.

1.1) $|N| = 10 \quad N = \{0, 1, \dots 9\} \quad |P| = 5 \quad |D| = 5$

$10 \cdot \binom{5}{1} \cdot \binom{4}{1} \cdot \binom{4}{1} \cdot \binom{3}{1} \cdot \binom{3}{1} = 7200$ DW

1.2) $|N \setminus \{0\}| = 9$ Affinché la somma sia pari ci deve essere 1 dispari e il resto pari

$\cancel{9 \cdot 4 \cdot \binom{5}{4}}$

~~scelgo 1 altro dispari~~

$\cancel{9 \cdot \binom{5}{5}}$

$9 \cdot \underbrace{10 \cdot 10 \cdot 10 \cdot 10 \cdot 10}_{} \cdot 5 = 450000$

Le possibilità senza lo 0

Da cui posso scegliere 10 elementi ripetibili

elemento pari o elemento dispari a seconda dei casi

1.3) $9 \cdot \cancel{9 \cdot 9 \cdot 9 \cdot 9} = 9^5$

~~Possibilità di scegliere 5 elementi~~

Ci sono 3 casistiche

- Lo 0 non c'é mai $\rightarrow |N \setminus \{0\}| = 9$ quindi 9^6 sono 6 cifre tra le 9
- Lo 0 appare 1 volta $\rightarrow 9^5 \cdot 6$ ovvero le prime 5 cifre e le possibilità di ri-collocare lo 0
- Lo 0 appare 2 volte $\rightarrow 9^4 \cdot \binom{6}{2}$ le prime 4 cifre moltiplicate per le possibilità di scegliere 0 in 2 posizioni su 6

Il Totale è:

$9^6 + 9^5 \cdot 6 + 9^4 \binom{6}{2}$

$= 984150$

Turno 1, Problema 2: Si consideri in S_9 la permutazione $\sigma = (15782)(2496)$.

1. (Punti 3) Si scriva σ come prodotto di cicli disgiunti e si calcoli σ^{-1}.
2. (Punti 4) Si calcoli il periodo di σ^{98}.
3. (Punti 4) Dimostrare che la funzione

$$f : \langle\sigma\rangle \to \mathbb{Z}_{12}, \quad \sigma^t \mapsto \overline{3t}$$

è ben definita. f è iniettiva? f è suriettiva?

1.1 $\sigma = (1,5,7,8,2,4,9,6)$ ok

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

1.2) Tipo $(\sigma) = 8$ Periodo $(\sigma) = 8$ $\quad 98 = 12\cdot 8 + 2$ quindi $\sigma^{98} = \sigma^{12\cdot 8+2} \Rightarrow \overset{id}{\cancel{\sigma^{12\cdot 8}}} \cdot \sigma^2$

$\sigma^2 = (15782496)^2 \Rightarrow (1724)(5896)$ $\quad$ Tipo$(\sigma^2) = (4,4)$ $\quad P(\sigma^2) = 4$ ok

1.3) Ben definita? Dati $\sigma^a, \sigma^b \in S_9$ $\quad \sigma^a = \sigma^b \to f(\sigma^a) = f(\sigma^b)$ $\forall a,b \in \mathbb{Z}$

sse $\sigma^a = \sigma^b$ sse $\sigma^{a-b} = id_{S_9}$

sse $P(\sigma) \mid a-b$

sse $8 \mid a-b$

sse $24 \mid 3a-3b$

= def. di f Verificata

Omomorfismo?

$f(\sigma^a \cdot \sigma^b) = f(\sigma^a) + f(\sigma^b)$

$f(\sigma^{a+b}) = \overline{3a} + \overline{3b}$ ok

$\overline{3(a+b)} = \overline{3(a+b)}$ Verificato

Iniettiva? $\longleftrightarrow$ Kernel$(f) = \{\overline{0}\}$ in $\mathbb{Z}_{12}$

Kernel$(f) = \{\sigma^t \in S_9 \mid f(\sigma^t) = 0\}$ ovvero $\{t \in \mathbb{Z} \mid 3\cdot t \equiv \overline{0} \bmod 12\}$

$= \{\sigma^0, \sigma^4\} \neq \{\sigma^0\}$ $\to$ Non è iniettiva

Suriettiva? $Im(f) = \{\underset{0}{\overline{0}}, \underset{1}{\overline{3}}, \underset{2}{\overline{6}}, \underset{3}{\overline{9}}, \underset{4}{\overline{12}}, \underset{5}{\overline{15}}, \underset{6}{\overline{18}}, \underset{7}{\overline{21}}\}$

$= \{\overline{0}, \overline{3}, \overline{6}, \overline{9}\} \neq \mathbb{Z}_{12}$ $\quad$ Non è suriettiva

Turno 2, Problema 1: Svolgere i punti seguenti.

1. (Punti 3) Determinare l'inverso di $\overline{72}$ in $\mathbb{Z}_{125}$.
2. (Punti 4) Elencare le soluzioni in $\mathbb{Z}_{68}$ della congruenza $12X \equiv 8 \bmod 68$.
3. (Punti 4) Dire quante sono le classi $\overline{x} \in \mathbb{Z}_{11}$ tali che $\overline{5}^k = \overline{x}$ per qualche $k \in \mathbb{N}$.

MCD$(125,72) = 1$ $\quad \overline{72}$ è invertibile

$125 = 1\cdot 72 + 53$ | $\overline{1} = \overline{33\cdot 72 - 14\cdot 125}$ $\quad 125\cdot t = \overline{0}$ in $\mathbb{Z}_{125} \to \overline{1} = \overline{33\cdot 72}$ inverso di $\overline{72}$ è $\overline{33}$ in $\mathbb{Z}_{125}$

$72 = 1\cdot 53 + 19$ | $1 = 14\cdot 72 - 19\cdot 53 \to 14\cdot 72 - 19\cdot(125 - 1\cdot 72) \to 14\cdot 72 - 19\cdot 125 + 19\cdot 72$

$53 = 2\cdot 19 + 15$ | $1 = 14\cdot 19 - 5\cdot 53 \to 14\cdot(72 - 1\cdot 53) - 5\cdot 53 \to 14\cdot 72 - 14\cdot 53 - 5\cdot 53 \to$

$19 = 1\cdot 15 + 4$ | $1 = 4\cdot 19 - 5\cdot 15 \to 4\cdot 19 - 5\cdot(53 - 2\cdot 19) \to 4\cdot 19 - 5\cdot 53 + 10\cdot 19$

$15 = 3\cdot 4 + 3$ | $1 = 4\cdot 4 - 1\cdot 15 \to 4\cdot(19 - 1\cdot 15) - 1\cdot 15 \to 4\cdot 19 - 4\cdot 15 - 1\cdot 15$

$4 = 1\cdot 3 + \underline{1}$ | $1 = 4 - 1\cdot 3 \to 4 - 1\cdot(15 - 3\cdot 4) \to 4 - 1\cdot 15 + 3\cdot 4$

$3 = 3\cdot 1 + 0$ | $\quad 3 = 15 - 3\cdot 4 \quad 4 = 19 - 1\cdot 15$

$15 = 53 - 2\cdot 19 \quad 19 = 72 - 1\cdot 53 \quad 53 = 125 - 1\cdot 72$

Turno 2, Problema 1: Svolgere i punti seguenti.

1. (Punti 3) Determinare l'inverso di $\overline{72}$ in $\mathbb{Z}_{125}$.
2. (Punti 4) Elencare le soluzioni in $\mathbb{Z}_{68}$ della congruenza $12X \equiv 8 \bmod 68$.
3. (Punti 4) Dire quante sono le classi $\overline{x} \in \mathbb{Z}_{11}$ tali che $\overline{5}^k = \overline{x}$ per qualche $k \in \mathbb{N}$.

1. Verifico se 'c'è' è invertibile con MCD(12, 68)

$68 = 5 \cdot 12 + 8$

$12 = 1 \cdot 8 + \underline{4}$

$8 = 2 \cdot 4 + 0$

12 non è invertibile in $\mathbb{Z}_{68}$ ma $4 \mid 8$ per cui si può risolvere dividendo per 'u'

$3 \frac{\cancel{12}x}{4} \equiv \frac{\cancel{8}^{2}}{4} \bmod \frac{\cancel{68}\,17}{4}$

$3x \equiv 2 \bmod 17$

$6 \cdot 3x \equiv 2 \cdot 6 \bmod 17$

$x \equiv 12 \bmod 17$

Elencandole: $\{ \overline{12}, \overline{29}, \overline{46}, \overline{63} \}$

MCD(3, 17) = 1

$17 = 5 \cdot 3 + 2$

$3 = 1 \cdot 2 + \underline{1}$

$2 = 2 \cdot 1 + 0$

$1 = 3 - 1 \cdot (17 - 5 \cdot 3)$

$1 = 3 - 1 \cdot 2$

$2 = 17 - 5 \cdot 3$

$1 = 3 - 1 \cdot 17 + 5 \cdot 3 \rightarrow \overline{1} = \overline{6 \cdot 3 - 1 \cdot 17}$

$\overline{1} = \overline{6 \cdot 3}$ in $\mathbb{Z}_{17}$

OK

1.3)

$\overline{5}^0 = \overline{1} \bmod 11$, $\overline{5}^1 = \overline{5} \bmod 11$ $\overline{5}^2 = \overline{25} \bmod 11 = \overline{14} \bmod 11$ $\overline{5}^3 = 125 \bmod 11$ $4 \bmod 11$

$\overline{5}^4 = a \bmod 11$

OK

Turno 2, Problema 2: Sia G un gruppo ciclico di ordine 30 con generatore g.

1. (Punti 3) Dire se le seguenti funzioni sono ben definite e sono omomorfismi di gruppi:

$$f : G \to \mathbb{Z}_{20}, \quad h : G \to \mathbb{Z}_{20}$$

definite da $f(g^k) = \overline{3k}$ e $h(g^k) = \overline{4k}$ per ogni $k \in \mathbb{Z}$

2. (Punti 4) Determinare nucleo e immagine di h.
3. (Punti 4) Determinare i generatori di un sottogruppo ciclico di G di ordine 10.

2.1) Ben definita? (f)

$g^k = g^{k+30t}$, Dati $a, b \in G$, se $a = b$ allora

$a - b = 0$

sse $a^k - b^k = 0$

sse $a^{k+30t} - b^{k+30t} = 0$

sse $\overline{3 \cdot (k+30t)} - (\overline{3 \cdot (k+30t)})$

sse $\overline{3k + 90t - 3k - 90t}$

sse $20 \nmid 3k + 90t - 3k - 90t$

f non è ben definita, per cui non è omomorfismo

OK

$\mathrm{Im}(h) = \{ \overline{0}\ \overline{4}\ \overline{8}\ \overline{12}\ \overline{16}\ \cancel{\overline{20}}\ \cancel{\overline{24}}\ \cancel{\overline{28}} \}$

$0, 1, 2, 3, 4, \cancel{5}, \cancel{6}, \cancel{7}, 8$

Ben def? (h) SI $4 \cdot 10$ Dati $a, b \in G$ se $a = b$ allora

$a - b = 0$

sse $a^k - b^k = 0$

sse $a^{k+30t} - b^{k+30t} = 0$

sse $\overline{4 \cdot (k+30t)} - \overline{4 \cdot (k+30t)}$

sse $4 \cdot k + 120t - 4k - 120t$

sse $20 \mid 4k + 120t$ verificata

Omomorfismo?

$h(g^k * g^{k'}) = h(g^k) + h(g^{k'})$

$h(g^{k+k'}) = \overline{4k} + \overline{4k'}$

$\overline{4(k+k')} = \overline{4(k+k')}$ Verificata

OK

$120 \mid 20$, $120 \quad 6$

$\mathrm{Kernel}(h) = \{ g^k \in G \mid h(g^k) = \overline{0} \in \mathbb{Z}_{20} \}$

$= \{ g^0, g^5, g^{10}, g^{15}, g^{20}, g^{25} \}$

Turno 2, Problema 2: Sia G un gruppo ciclico di ordine 30 con generatore g.

1. (Punti 3) Dire se le seguenti funzioni sono ben definite e sono omomorfismi di gruppi:

$$f : G \to \mathbb{Z}_{20}, \quad h : G \to \mathbb{Z}_{20}$$

definite da $f(g^k) = \overline{3k}$ e $h(g^k) = \overline{4k}$ per ogni $k \in \mathbb{Z}$

2. (Punti 4) Determinare nucleo e immagine di h.
3. (Punti 4) Determinare i generatori di un sottogruppo ciclico di G di ordine 10.

no

no

2.3) $\langle g \rangle = \{e, g, g^1, g^2, g^3, g^4, g^5, g^6, g^7, g^8, g^9\}$ $\quad \langle g^4 \rangle = \{e, g^4, g^8, g^{\overset{2}{\cancel{12}}}, g^{\overset{6}{\cancel{16}}}, g^{\overset{e}{\cancel{20}}}\}$

$\langle g^2 \rangle = \{g^k \mid k = 2t \in \mathbb{Z}\} \neq 6$ no $\quad \langle g^5 \rangle = \{e, g^5\}$ no

$\langle g^3 \rangle = \{g^k \mid k = 3t \in \mathbb{Z}\} = \{e, g^3, g^6, g^9, g^{\overset{2}{\cancel{12}}}, g^{\overset{5}{\cancel{15}}}, g^{\overset{8}{\cancel{18}}}, g^{\overset{1}{\cancel{21}}}, g^{\overset{4}{\cancel{24}}}, g^{\overset{7}{\cancel{27}}}\}$

$\langle g^6 \rangle = \{e, g^6, g^{\overset{2}{\cancel{12}}}, g^{\overset{8}{\cancel{18}}}, g^{\overset{4}{\cancel{24}}}\}$ no $\quad g^7 = \{e, g^7, g^{\overset{4}{\cancel{14}}}, g^{\overset{1}{\cancel{21}}}, g^{\overset{8}{\cancel{28}}}, g^{\overset{5}{\cancel{35}}}, g^{\overset{2}{\cancel{42}}}, g^{\overset{9}{\cancel{49}}}, g^{\overset{6}{\cancel{56}}}, g^{\overset{3}{\cancel{63}}}\}$

$g^8 = \{e, g^8, g^{\overset{6}{\cancel{16}}}, g^{\overset{4}{\cancel{24}}}, g^{\overset{2}{\cancel{32}}}\} \neq \langle g \rangle$ $\quad g^9 = \{e, g^9, g^{\overset{8}{\cancel{18}}}, g^{\overset{7}{\cancel{27}}}, g^{\overset{6}{\cancel{36}}}, g^{\overset{5}{\cancel{45}}}, g^{\overset{4}{\cancel{54}}}, g^{\overset{3}{\cancel{63}}}, g^{\overset{2}{\cancel{72}}}, g^{\overset{1}{\cancel{81}}}\} = \langle g \rangle$

Quindi sono $\langle g \rangle, \langle g^3 \rangle, \langle g^7 \rangle, \langle g^9 \rangle$

Problema 1: Sia $C = \langle g \rangle$ un gruppo ciclico con 48 elementi.

1. (Punti 4) Dimostrare che la funzione $f : C \to \mathbb{Z}_{60}$, $f(g^k) = \overline{5k}$, è un omomorfismo ben definito e decidere se è iniettivo e/o suriettivo.
2. (Punti 3) Sia $H < \mathbb{Z}_{60}$ l'immagine di f. Dire quanti generatori ha H.
3. (Punti 4) Calcolare il rappresentante tra 0 e 59 di $(f(g^7))^{18}$.

1.1) Ben definito? $\quad$ ogni $g \in C$ può essere rappr. come g^k $\forall k \in \mathbb{Z}$

Dati $a, b \in C \to a = b$ sse $a - b = 0$

sse $a^{k+48t} - b^{k+48t} = 0$

sse $5(k+48t) - 5(k+48t) = 0$

sse $5k + 240t - 5k - 240t = 0$

sse $\overline{60} \mid \overline{5k+240t}$ sì

Ben definita

Omomorfismo?

$f(g^h \cdot g^k) = f(g^h) + f(g^k)$

$f(g^{h+k}) = \overline{5h} + \overline{5k}$

$\overline{5 \cdot (h+k)} = \overline{5(h+k)}$ ✓ omomorfismo

Iniettivo?

$\mathrm{Ker}(f) = \{\overline{0}\} \longleftrightarrow$ è iniettivo

$= \{g^k \mid f(g^k) = \overline{0} \text{ in } \mathbb{Z}_{60}\}$

$= \{k \in \mathbb{N} \mid k < 48 \wedge 5 \cdot k = \overline{0}\ \mathbb{Z}_{60}\}$

$= \{g^0, g^{12} \dots\} \neq \{g^0\}$ Non è iniettiva

$$\begin{array}{lcccccccccccc} & \overline{5}, & \overline{10}, & \overline{15}, & \overline{20}, & \overline{25}, & \overline{30}, & \overline{35}, & \overline{40}, & \overline{45}, & \overline{50}, & \overline{55}, & \overline{60} \dots \\ \text{con } k = & 1^{*} & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 \end{array}$$

Suriettiva? $\quad \mathrm{Im}(f) = \mathbb{Z}_{60} \longleftrightarrow$ suriettiva

$\mathrm{Im}(f) = \{\overline{5x} \text{ in } \mathbb{Z}_{60}\}$ * $\neq \mathbb{Z}_{60} \to$ non è suriettiva

Problema 1: Sia $C = \langle g \rangle$ un gruppo ciclico con 48 elementi.

1. (Punti 4) Dimostrare che la funzione $f : C \to \mathbb{Z}_{60}$, $f(g^k) = \overline{5k}$, è un omomorfismo ben definito e decidere se è iniettivo e/o suriettivo.
2. (Punti 3) Sia $H < \mathbb{Z}_{60}$ l'immagine di f. Dire quanti generatori ha H.
3. (Punti 4) Calcolare il rappresentante tra 0 e 59 di $(f(g^7))^{18}$.

1.2) $H = \{\overline{5}, \overline{10}, \overline{15}, \overline{20}, \overline{25}, \overline{30}, \overline{35}, \overline{40}, \overline{45}, \overline{50}, \overline{55}\}$ sono $\langle 1 \rangle, \langle 7 \rangle, \langle 11 \rangle$

$\langle 8 \rangle$ = 4 elementi

MCD(1, 60) = 1 ✓ $\quad 60 = 60 \cdot 1 + 0$

MCD(2, 60) = 2 ✗

MCD(3, 60) = 3 ✗

MCD(4, 60) = 4 ✗ $\quad 60 = 15 \cdot 4 + 0$

MCD(5, 60) = 5 ✗

MCD(6, 60) = 6 ✗ $\quad 60 = 10 \cdot 6 + 0$

MCD(7, 60) = 1 ✓ $\quad 60 = 8 \cdot 7 + 4 \quad 7 = 1 \cdot 4 + 3 \quad 4 = 1 \cdot 3 + 1 \quad 3 = 3 \cdot 1 + 0$

MCD(8, 60) = 1 ✓ $\quad 60 = 7 \cdot 8 + 4 \quad 8 = 4 \cdot 2 + 0$

MCD(9, 60) = 3 ✗ $\quad 60 = 6 \cdot 9 + 6 \quad 9 = 1 \cdot 6 + 3 \quad 6 = 2 \cdot 3 + 0$

MCD(10, 60) ≠ 1 ✗

MCD(11, 60) = 1 ✓ $\quad 60 = 5 \cdot 11 + 5 \quad 11 = 2 \cdot 5 + 1 \quad 5 = 5 \cdot 1 + 0$

$\begin{array}{c|c} 60 & 4 \\ 4 & 15 \\ 20 & \end{array} \qquad \begin{array}{c|c} 60 & 8 \\ 56 & 7 \end{array}$

7, 14, 21, 28, 35, 42, 49, 56

8, 16, 24, 32, 40, 48, 56, 64

9, 18, 27, 36, 45, 54, 63, 72, 81

1.3) $f(g)^7 = \overline{35}$ in $\mathbb{Z}_{60}$ $\qquad 35^{18}$ mod $\mathbb{Z}_{60}$ $\quad 18 = 1 \cdot 16 + 2$

$\varphi(60) = \varphi(2^2 \cdot 5 \cdot 3) = 2 \cdot \cancel{4} \cdot 2 = 16$

35^{18} mod 60

$7^{18} \cdot 5^{18}$ mod 60

$\begin{array}{c} 16 \\ 8 \end{array}$

MCD(60, 35) = 5 $\quad \overline{35}$ non è invertibile

$60 = 1 \cdot 35 + 25$ $\qquad$ MCD(60, 7) = 1

$35 = 1 \cdot 25 + 10$ $\qquad$ MCD(60, 5) = 5

$25 = 2 \cdot 10 + 5$ $\qquad$ 7, 14, 21, 28, 35, 42, 49, 56

$10 = 2 \cdot 5 + 0$ $\qquad$ $60 = 8 \cdot 7 + 4$

$7 = 1 \cdot 4 + 3$ $\qquad$ 0 $\quad 5^0$ mod 60 = 1

$7^{18} = 7^{\cancel{16}} \cdot 7^2$ mod 60 $\qquad 4 = 1 \cdot 3 + 1$ $\qquad$ 1 $\quad 5$ mod 60

49 mod 60 $\qquad 3 = 3 \cdot 1 + 0$ $\qquad$ 2 $\quad 25$ mod 60

3 $\quad 125$ mod 60 = 5 mod 60

$\begin{array}{c|c} 125 & 60 \\ 120 & 2 \\ 5 & \end{array}$

$5^{18} = 5^{3^5} \cdot \cancel{8}^{\cancel{3}}$

$= 5^5 = \cancel{8}^{\cancel{3}} \cdot 5^2$ mod 60

25 mod 60 $\qquad$ ok

1225 mod 60

25 mod 60

$\begin{array}{c} 49 \cdot \\ 25 \end{array}$

$\begin{array}{c|c} 1225 & 60 \\ 120 & 2 \\ 25 & \end{array}$

$|S_1|=10 \quad |S_2|=10 \quad |S_3|=10 \quad |S_4|=10$

$|G|=3$

Problema 2: Adriana, Berto e Camilla giocano con un mazzo di 40 carte, 10 di ciascun seme.

1. (Punti 4) Scelte 12 carte coperte dal mazzo, quanti modi ci sono per distribuirle fra i tre giocatori?
2. (Punti 3) Adriana ha ricevuto 2 carte e sono entrambe di cuori. Quante sono le possibili mani di Adriana?
3. (Punti 4) Berto ha ricevuto 3 carte e Camilla 7. Quante possono essere complessivamente le loro mani se entrambi hanno ricevuto lo stesso numero di carte di cuori?

1.1) $\cancel{\binom{12}{3}\cdot\binom{9}{3}\cdot\binom{6}{3}}$ $\quad \binom{12+3-1}{3-1}=\binom{14}{2}$

1.2) I cuori hanno 10 carte $\binom{10}{2}$ ok

1.3) Se entrambi hanno lo stesso numero di cuori allora entrambi possono avere: 0, 1, 2 o 3 carte di cuori

Per Berto $\quad \underbrace{\binom{30}{3}}_{0\text{ cuori}}+\underbrace{\binom{30}{2}\cdot 10}_{1\text{ cuore}}+\underbrace{30\cdot\binom{10}{2}}_{2\text{ cuori}}+\underbrace{\binom{10}{3}}_{3\text{ cuori}}$

Per Camilla $\quad \binom{27}{7}+\binom{28}{6}\cdot 9+\binom{29}{5}\cdot\binom{8}{2}+\binom{30}{4}\cdot\binom{7}{3}$

Tolte le carte di Berto

ok

Problema 1: Si consideri il gruppo $\mathbb{Z}_{14}\times\mathbb{Z}_{21}$ con la consueta operazione di somma componente per componente e sia data la funzione

$$f:\mathbb{Z}\to\mathbb{Z}_{14}\times\mathbb{Z}_{21}$$

definita da $f(n)=([2n]_{14},[3n]_{21})$, per ogni $n\in\mathbb{Z}$.

1. (punti 4) Dimostrare che f è un omomorfismo di gruppi e determinarne il nucleo.
2. (punti 4) Determinare la cardinalità di $\mathrm{Im}(f)$ e le controimmagini di $([3]_{14},[3]_{21})$.
3. (Punti 3) Calcolare il resto della divisione di $2^{141232}+7^{6536779}$ per 30.

1.1) Ben Definita $\quad$ Dati $a,b\in\mathbb{Z}\to a=b$ se $a-b=0$ sse $([2a]_{14},[3a]_{21})-([2b]_{14},[2b]_{21})$ Ben definita

$f(a+b)=f(a)+f(b)$

$([2\cdot(a+b)]_{14},[2(a+b)]_{21})=([2a]_{14},[3a]_{21})+([2b]_{14},[3b]_{21})$

$([2\cdot(a+b)]_{14},[2(a+b)]_{21})=([2(a+b)]_{14},[2(a+b)]_{21})$

$\mathrm{Kernel}(f)=\{n\in\mathbb{Z}\mid f(n)=([0]_{14},[0]_{21})\}$
$=\{n\in\mathbb{Z}\mid 14|n \wedge 21|n\}$
$\{n\in\mathbb{Z}\mid 7|n\}$ ok

$MCD(14,21)=7$
$21=1\cdot 14+7$
$14=2\cdot 7+0$
$mcm(14,21)=\frac{21\cdot\cancel{14}^{2}}{\cancel{7}}=42$

1.2) $\mathrm{Im}(f)=\{([0]_{14},[0]_{21}),([2]_{14},[3]_{21}),([4]_{14},[6]_{21}),([6]_{14},[9]_{21}),$
$|\mathrm{Im}(f)|=7$ $\quad ([8]_{14},[12]_{21}),([10]_{14},[15]_{21}),([12]_{14},[18]_{21})\}$

$[2n]_{14}=[3]_{14}$ sse $\cancel{2n=14t+3}$
$[3n]_{21}=[3]_{21}$ sse $\cancel{n=21t}$

$\begin{cases}2n\equiv 3 \mod 14\\ 3n\equiv 3\mod 21\end{cases}=\begin{cases}2\equiv 3\mod 14\\ n\equiv 1\mod 7\end{cases}$ Non esiste

$MCD(2,14)=2$ e $2\nmid 3$ non si può fare $\quad n=1+7t \quad 2n=2+14t$

$14=7\cdot 2+0 \quad \vee \quad MCD(3,21)=3 \quad 3|3\to \frac{3n}{3}\equiv\frac{3}{3}^{1}\mod\frac{21}{3}^{7} \quad 2n=2$ in $\mathbb{Z}_{14}$

Problema 1: Si consideri il gruppo $\mathbb{Z}_{14} \times \mathbb{Z}_{21}$ con la consueta operazione di somma componente per componente e sia data la funzione

$$f : \mathbb{Z} \to \mathbb{Z}_{14} \times \mathbb{Z}_{21}$$

definita da $f(n) = ([2n]_{14}, [3n]_{21})$, per ogni $n \in \mathbb{Z}$.

1. (punti 4) Dimostrare che f è un omomorfismo di gruppi e determinarne il nucleo.
2. (punti 4) Determinare la cardinalità di $\mathrm{Im}(f)$ e le controimmagini di $([3]_{14}, [3]_{21})$.
3. (Punti 3) Calcolare il resto della divisione di $2^{141232} + 7^{6536779}$ per 30.

$\varphi(30) = \varphi(2 \cdot 3 \cdot 5) = 1 \cdot 2 \cdot 4 = 8$

$MCD(2,30) = 2 \to 2$ non è in in $\mathbb{Z}_{30}$ ma

$2^0 = 1 \mod 30$
$2^1 = 2 \mod 30$
$2^2 = 4 \mod 30$
$2^3 = 8 \mod 30$
$2^4 = 16 \mod 30$
$2^5 = 32 \mod 30$ (2)

$30 = 15 \cdot 2 + 0$

$2^{141232} = 2^{5 \cdot 28246} \cdot 2^2 \mod 30$

$4 \mod 30$

$MCD(7,30) = 1$
$30 = 4 \cdot 7 + 2$
$7 = 3 \cdot 2 + 1$
$2 = 2 \cdot 1 + 0$

$6536779 = 817097 \cdot 8 + 3$

$7^{6536779} = 7^{8 \cdot 817097} \cdot 7^3$

$6536779 \mid 8$
817097

64, 13, 8, 56, 56, 077, 72, 59, 56, 3

5 6 7 64
40 48, 56, 8 9
80 88, 96
10 11

$49 \mod 30$
$19 \mod 30$

$19 + 4 \mod 30$
$\underline{23 \mod 30}$

Problema 2: Si considerino in S_9 le permutazioni

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 5 & 1 & 4 & 3 & 7 & 9 & 8 & 2 & 6 \end{pmatrix}, \quad \tau = (34)(69)$$

1. (Punti 4) Si scrivano come prodotto di cicli disgiunti σ, σ^{-1}, $(\sigma \circ \tau)^{-1}$.
2. (Punti 3) Esibire esplicitamente un sottogruppo di S_9 di ordine 10. Spiegare perchè non esiste in S_9 un sottogruppo di ordine 13.
3. (Punti 4) Verificare che la funzione

$$f : \mathbb{Z}_{10} \to S_9, \quad \bar{t} \mapsto \sigma^t$$

è ben definita. Scrivere esplicitamente quali elementi di $\mathbb{Z}_{10}$ appartengono a $\ker(f)$.

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

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

$\sigma\tau$

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

$\sigma \circ \tau = (1,5,7,8,2) \quad (\sigma\circ\tau)^{-1} = (1,2,8,7,5)$

1.2 ~~$(1,2,3,4,5,6,7,8,9)$~~
~~Reale 13 ≥ periodo di S_9~~

- Ciò vuol dire mostrare un ciclo $\pi \in S_9$ tale che l'mcm del Tipo dia 10 es: $(1,2,3,4,5)(6,7)$ Tipo$(\pi) = (5,2)$

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

$5 = 2\cdot 2 + 1$ $\quad \frac{5\cdot 2}{1} = 10$

$2 = 2\cdot 1 + 0$

- Se l'ordine deve essere 13, allora è ciclico e deve essere formato da cicli disgiunti di lunghezza 13, che però non esistono in S_9

2.3) Ben def? $\quad \bar{a}, \bar{b} \in \mathbb{Z}_{10} \wedge [a]_{10} = [b]_{10} \to f([a]_{10}) = f([b]_{10})$

sse $\sigma^a = \sigma^b$

sse $\sigma^{a-b} = id$ sse $a-b=0$

sse $10 \mid a-b$

sse $a = b + 10t$

sse $f(\bar{a}) = \sigma^{b+10t}$ $\quad \sigma^{k+10t} = \sigma^k$

sse $= \sigma^b = f(\bar{b})$

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

$\text{Ker}(f) = \{ \bar{z} \in \mathbb{Z}_{10} \mid f(\bar{z}) = \sigma^0 \}$

siccome il periodo è 10 per σ si traduce in

$= \{ k \in \mathbb{Z} \mid k = 10t \}$

$= \{ \bar{k} \in \mathbb{Z}_{10} \mid \sigma^k = \sigma^0 \}$

$= \{ \bar{0} \} \to$ tutti gli elementi $k = 10t$ in $\mathbb{Z}_{10}$ che convergono in $\bar{0}$

Problema 1: Il gioco degli scacchi si svolge tra due schieramenti (Bianco e Nero) formati da 8 "pezzi" (Re, Regina, 2 Torri, 2 Alfieri, 2 Cavalli) e 8 "pedoni" ciascuno su una scacchiera di 64 caselle colorate alternativamente bianche e nere.

1. (Punti 3) Quanti modi ci sono per piazzare in modo casuale i 16 pedoni totali su una scacchiera? (Ogni casella può essere occupata ma non può contenere più di un pedone)
2. (Punti 4) Quanti sono i modi per piazzare in modo casuale gli 8 pezzi bianchi sulla prima riga della scacchiera?
3. (Punti 4) Come nel punto precedente, ma con la richiesta che pezzi dello stesso tipo vengano piazzati su caselle di colore diverso.

1.1) $\cancel{\binom{64}{16}}$ Bisogna considerare i Pedoni di colori diversi $\binom{64}{8}\cdot\binom{56}{8}$

1.2) $\cancel{8!}$ Bisogna pensare come se fosse anag.

$$\frac{8!}{1!\cdot 1!\cdot 2!\cdot 2!\cdot 2!}$$

1.3) $\cancel{\binom{2}{1}\cdot\binom{6}{3}\cdot 3!}$

re/regina

Dovendo prima pensare ai 3 distinti

$$\underbrace{4\cdot 3\cdot 2}\cdot\underbrace{4\cdot 3\cdot 2}\cdot 2$$

4 solo le caselle bianche

4 solo le caselle nere

Gli ultimi 2 saranno riservate alle ultime 2 caselle

Problema 2 Nel gruppo delle permutazioni S_7 si considerino le seguenti permutazioni

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

1. (Punti 3) Scrivere $\sigma,\tau,\sigma\circ\tau,\tau\circ\sigma,\sigma^{-1}$ come prodotto di cicli disgiunti.
2. (Punti 4) Calcolare il periodo di σ e scrivere σ^{999} come prodotto di cicli disgiunti;
3. (Punti 4) Determinare una permutazione $\mu\in S_7$ tale che $\mu\circ\sigma=\tau^2$.

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

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

Ok

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

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

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

$\sigma^{-1}=(2,4)^{-1}(356)^{-1}=(4,2)(3,6,5)$

Tipo$(\sigma)=(2,3)$

Periodo$(\sigma)=$ mcm $2,3=6$

$\sigma^{999}=\cancel{\sigma^{6\cdot 166}}\circ\sigma^{3}$

$\sigma^3=(2,4)^3\cdot(356)^3=(2,4)$ Ok

2.3) $\tau^2=(4,7)^2=id_{S_7}$

Quindi si può usare σ^{-1} in quanto $\sigma\circ\sigma^{-1}=id_{S_7}$

Problema 1:
Si consideri l'insieme $G = [0,1) = \{x \in \mathbb{R} | 0 \le x < 1\} \subset \mathbb{R}$, e la seguente funzione $*$:

$$* : \mathbb{R} \times \mathbb{R} \to \mathbb{R},$$

$$\forall t_1, t_2 \in \mathbb{R}, \quad t_1 * t_2 = \begin{cases} t_1 + t_2, & \text{se } t_1 + t_2 < 1, \\ t_1 + t_2 - 1, & \text{se } t_1 + t_2 \ge 1. \end{cases}$$

1. (Punti 3) Verificare che $*$ ristretta a $G \times G$ è un'operazione su G
2. (Punti 4) Dando per verificato che $*$ come operazione su G è associativa, dimostrare che G con l'operazione $*$ é un gruppo abeliano.
3. (Punti 4) Calcolare il periodo di $\frac{2}{7} \in G$, cioè il più piccolo intero positivo n tale che
$$\underbrace{\frac{2}{7} * \cdots * \frac{2}{7}}_{n \text{ volte}} = 0.$$

1.1) Siccome $t \in G \iff t \in \mathbb{R} \wedge (t \ge 0 \wedge < 1)$ allora

$t_1 + t_2 \in G \iff t_1 \in \mathbb{R} \wedge t_2 \in \mathbb{R} \wedge (t_1 + t_2 \ge 0 \wedge t_1 + t_2 < 1)$

se $t_1 + t_2 < 1$ allora è verificata

se $t_1 + t_2 \ge 1$ per def. $t_1 + t_2 < 2$ quindi

$0 \le t_1 + t_2 < 2$ sse $t_1 + t_2 - 1 < 2 - 1$

verificata sse $t_1 + t_2 - 1 < 1$

1.2) $(g * h) * k = g * (h * k)$?

$(g + h) * k = g * (h + k)$

$g + h + k = g + h + k$

In maniera simile nei casi $g + k \ge 1$, $h + k \ge 1$, $g + h \ge 1$

$(g * h) = (h * g)$

se $g + h < 1$ $\quad g + h = h + g$ in $\mathbb{Z}$ $+$ è commutativa

se $g + h \ge 1$ $\quad g + h - 1 = h + g - 1$ applico associatività

$g + h - 1 = g + h - 1$ ✓

$(g * h) = g$ sse se $g + h = g$ sse $h = 0$ $(h + g < 1)$

nel caso di $h + g \ge 1$ non può verificarsi

in quanto se $h + g \ge 1$ ed $h * g = g$ allora $g \ge 1$ ma $g \notin G$

$\forall g \in G$ $\quad g * h = 0$ (se $h + g < 1$)

$h + g = 0$ sse $g = -h$ ma $-h \notin G$

(se $h + g - 1 \ge 1$)

$h + g - 1 = 0$ sse $g = 1 - h$

$\frac{2}{7} * \frac{2}{7} = \frac{4}{7} * \frac{2}{7} = \frac{6}{7} * \frac{2}{7} = \frac{1}{7} * \frac{2}{7} = \frac{3}{7} * \frac{2}{7} = \frac{5}{7} * \frac{2}{7} = 0$

$\frac{8}{7} - 1 = \frac{8 - 7}{7} = \frac{1}{7}$

Problema 2:

1. (Punti 3) Trovare le soluzioni in $\mathbb{Z}$ della congruenza lineare
$$6x \equiv 14 \mod 40.$$
2. (Punti 4) Calcolare MCD(208, 743) e determinare la corrispondente identità di Bezout.
3. (Punti 4) Calcolare il resto della divisione di $3^{5354} + 5^{4358}$ per 14.

2.1] $MCD(6,40)=2$

$40=6\cdot6+4$
$6=1\cdot4+2$
$4=2\cdot2+0$

OK

6 non è inv. in $\mathbb{Z}_{40}$ ma $d \mid b$ ($2 \mid 14$) quindi

$6x \equiv 14 \mod 40$

$3\ \frac{6x}{2} \equiv \frac{14}{2}^{7} \mod \frac{40}{2}^{20}$

$3x \equiv 7 \mod 20$ $\qquad MCD(3,20)=1$

$20=6\cdot3+2$
$3=1\cdot2+1$
$2=2\cdot1+0$

$1=7\cdot3-1\cdot20$
$1=3-1\cdot20+6\cdot3$
$1=3-1\cdot(20-6\cdot3)$
$1=3-1\cdot2$

$\bar{1}=\overline{7\cdot3-1\cdot20}$
$\bar{1}=\bar{7}\cdot\bar{3} \qquad \overline{20}=\bar{0}$ in $\mathbb{Z}_{20}$

$7\cdot3x \equiv 7\cdot7 \mod 20$
$x \equiv 49 \mod 20$
$x \equiv 9 \mod 20$

$=\{\bar{9}, \overline{29}\}$ in $\mathbb{Z}_{40}$

$=\{9, 29, 49 \ldots\}$

$\overset{5}{20}, \overset{6}{24}, \overset{7}{28},$

2) $MCD(208, 743)=1$

$743=3\cdot208+119$
$208=1\cdot119+89$
$119=1\cdot89+30$
$89=2\cdot30+29$
$30=1\cdot29+1$
$29=29\cdot1+0$

OK

$1=\overset{x}{7}\cdot743-\overset{y}{25}\cdot208$
$1=7\cdot119-4\cdot208 \to 7\cdot(743-3\cdot208)-4\cdot208 \to 7\cdot743-21\cdot208-4\cdot208$
$1=3\cdot119-4\cdot89 \to 3\cdot119-4\cdot(208-1\cdot119) \to 3\cdot119-4\cdot208+4\cdot119$
$1=3\cdot30-1\cdot89 \to 3\cdot(119-1\cdot89)-1\cdot89 \to 3\cdot119-3\cdot89-1\cdot89$
$1=30-1\cdot29 \to 30-1\cdot(89-2\cdot30) \to 30-1\cdot89+2\cdot30$
$29=89-2\cdot30 \qquad 30=119-1\cdot89$
$89=208-1\cdot119 \qquad 119=743-3\cdot208$

3) $\varphi(14)=\varphi(7\cdot2)=6\cdot1=6$

- 3^{5354} $\quad MCD(3,14)=1$ Si può usare Eulero

$5354=892\cdot6+2 \qquad 3^{5354}=\cancel{3^{6\cdot892}}\cdot3^2$ in $\mathbb{Z}_{14}$

$3^2 \mod 14 \to 9 \mod 14$

- 5^{4358} $\quad MCD(5,14)=1$ Ok eulero

$4358=6\cdot726+2 \qquad 5^{4358}=\cancel{5^{6\cdot726}}\cdot5^2$

$=25 \mod 14 \to 11 \mod 14$

OK

$9+11 \mod 14 \to 20 \mod 14$

$6 \mod 14$

CORSO DI STUDI IN INFORMATICA
MATEMATICA DISCRETA
PROVA SCRITTA 7 SETTEMBRE 2021

Problema 1 Sia G il sottogruppo di S_6 definito da
$$G = \{(12)^i(3456)^j \mid 0 \leq i \leq 1, 0 \leq j \leq 3\}.$$

a) [3 punti] Si scrivano gli elementi di G come prodotti di cicli disgiunti e per ogni elemento di G si determini il periodo
b) [4 punti] Dire se G è un gruppo commutativo e se è ciclico.
c) [4 punti] Sia
$$H = \{\sigma \in G \mid \sigma(1) = 1\}.$$
Elencare gli elementi di H e dire se H è un sottogruppo ciclico di G.

Soluzione

$(3456)^2 = (3,5)(4,6)$

$(3456)^3 = (3,6,5,4)$

$G = \{ id_{S_6},\ (1,2)(3,4,5,6),\ (1,2)(3,5)(4,6),\ (3,5)(4,6),\ (1,2)(3,6,5,4),\ (3,6,5,4) \}$

P(id) = 1 — Tipo = (2,4) — Tipo (2,2,2) — Tipo (2,2) — Tipo (2,4) — Tipo (4)

(1,2) = 2 — periodo (2,4) = 4 — Periodo = 2 — Periodo = 2 — Periodo = 4 — Periodo = 4

(3456) = 4 $\quad 4 = 2 \cdot 2 + 0 \quad \frac{4 \cdot 2}{2} = 4$

Ok

2) $(1,2)^i(3,4,5,6)^j \circ (1,2)^h(3,4,5,6)^k = (1,2)^h(3,4,5,6)^k \circ (1,2)^i(3,4,5,6)^j$

$(1,2)^{i+h}(3,4,5,6)^{j+k} = (1,2)^{h+i}(3,4,5,6)^{k+j}$ verificato

$|G| = 8 \qquad$ Periodo$(i,j) = 8 \qquad \nexists$ nessun elemento sse non è ciclico!

3) $H = \{\sigma \in G \mid \sigma(1) = 1\} \rightarrow$ lascia fermo 1

$= \{(1), (3,4,5,6), (3,5)(4,6), (3,6,5,4)\} \in e_G$ ✓

$= \{(3,4,5,6)^k \mid k \in \mathbb{Z} \wedge k \geq 0 \wedge k \leq 3\}$

quindi H è generato da $\langle 3,4,5,6 \rangle$ ed è ciclico

$|H| = 4$ ed esiste un elemento con periodo 4

Problema 2

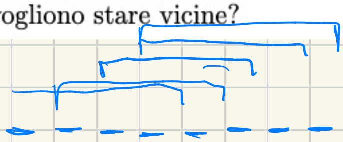
a) (3 punti) In quanti modi diversi 8 persone possono sedersi in fila su una panchina?

b) (4 punti) In quanti modi diversi 8 persone possono sedersi in fila su una panchina se ci sono 4 uomini, 4 donne e gli uomini sono tutti seduti vicini?

c) (4 punti) In quanti modi diversi 8 persone possono sedersi su una panchina se due di esse (A e B) non vogliono stare vicine?

2.1) $8!$

2.2) $4! \cdot 4! \cdot 2$



2.3) $8! - (7 \cdot 2! \cdot 6!)$