# MD1 • SIMULA "ESAMI 21-22"

**Problema 1:**
Consideriamo una classe di una scuola elementare di Torino, in cui ci sono 25 bambini.

1. (Punti 3) La scuola propone come attività pomeridiane facoltative un laboratorio di teatro al lunedí e un corso di minibasket al mercoledí. Nella classe 13 bambini partecipano al laboratorio di teatro, 15 al corso di minibasket, e 3 bambini non aderiscono a nessuna delle due iniziative. Quanti sono i bambini che partecipano sia al laboratorio di teatro, sia al corso di basket?
2. (Punti 4) Nella classe ci sono 10 bambini e 15 bambine. Il maestro per premiarli a fine quadrimestre per i loro buoni voti, decide di regalare a ognuno una penna. Per i maschi, compra 5 penne rosse e 5 nere, per le femmine compra 8 penne verdi e 7 blu. In quanti modi il maestro può distribuire le penne ai suoi scolari?
3. (Punti 4) I bambini della classe, all'uscita da scuola, si mettono in fila per due. Ovviamente un bambino rimane senza compagno di fila, e sta primo nella fila con il maestro. Se non conta quale bimbo sta a destra e quale a sinistra in ogni coppia della fila, in quanti modi diversi i bimbi possono sistemarsi in fila?

$|B| = 25$

$|T| = 13 \qquad |B \setminus T \setminus M| = 3$

$|M| = 15$

$|M \cup T| = |T| + |M| - |M \cap T|$

$-|M \cap T| = |M \cup T| - |T| - |M|$

$|M \cap T| = -|M \cup T| + |T| + |M|$

$= -22 + 13 + 15 \to -22 + 28 = \underline{6}$

$|M \cup T| = 25 - 3 = 22$

$x = y + z - c \qquad c + x = y + z$

$x - y - z = -c \qquad c = -x + y + z$

$-x + y + z = c$

OK

2) $|Ma| = 10 \quad |Fe| = 15$

5 rosse e 5 nere 8 verdi 7 blu

Per i Maschi: $\underset{\text{rosse}}{\binom{10}{5}} \cdot \underset{\text{nere}}{\binom{5}{5}}$ $\cdot$ Per le Femmine: $\underset{\text{verdi}}{\binom{15}{8}} \cdot \underset{\text{blu}}{\binom{7}{7}}$

OK

3) $B_1 \to$

$B_2 \; B_3$   24 +1

$B_4 \; B_5$   12 coppie

$\cancel{\underset{\text{1 colonna}}{\binom{25}{12}} \cdot \underset{\text{2° colonna}}{\binom{13}{12}} \cdot 1}$

No, così si contano con l'ordine, va prima scelto il 1°

$25 \cdot \binom{24}{2} \cdot \binom{22}{2} \cdot \binom{20}{2} \cdots \binom{2}{2} = \frac{25!}{2^{12}}$

**Problema 2:**
Si risolvano i seguenti problemi:

1. (Punti 3) Per quali classi $\bar{a} \in \mathbb{Z}_{12}$ la congruenza $ax \equiv 3 \bmod 12$ ammette almeno una soluzione?
2. (Punti 4) Se $\bar{y}$ è inversa di $\bar{x}$ in $\mathbb{Z}_7$, qual'è l'inversa di $\overline{2x}$?
3. (Punti 4) Sia $n > 0$ un intero. Spiegare perchè MCD(n, n + 3) può essere solo 1 o 3.

1\. Se $MCD(a,12) = 1 \to a$ è invertibile quindi

$ax \equiv 3 \bmod 12 \to a^{-1} \cdot a x \equiv 3 \cdot a^{-1}$

$x \equiv 3 \cdot a^{-1} \bmod 12$

2\. Se $MCD(a,12) \neq 1 \to a$ non è invertibile

- Se $MCD(a,12) \mid 3$ allora è come fare

$\frac{a}{d} x \equiv \frac{3}{d} \bmod \frac{12}{d}$

$\frac{d}{a} \cdot \frac{a}{d} x \equiv \frac{3}{d} \cdot \frac{a}{d} \bmod \frac{12}{d} \to x \equiv \frac{3a}{d^2} \bmod 12$

- Se $MCD(a,12) \nmid 3 \to$ Non è risolubile

2) Se $y$ è $x^{-1}$ in $\mathbb{Z}_7$ allora

$\bar{1} = \overline{x \cdot y} \to \overline{2 \cdot 1} = \overline{2 \cdot (x \cdot y)}$

$\bar{2} = \overline{2x \cdot 2y}$

3) Espandendo $MCD(n, n+3)$ considero

$n + 3 = 1 \cdot n + 3$

$n = x \cdot 3 + y$

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

$2 = 2 \cdot 1 + 0$

$3 = 3 \cdot 1 + 0$

Sappiamo che $r \leq d$ per cui $y \leq 3$

Se $y = 2$ $MCD(n, n+3) = 1$

Se $y = 1$ $MCD(n, n+3) = 1$

Se invece $3 \nmid n$ ovvero $n = 2 \vee n = 1$

$n = 2 \quad 2 = 0 \cdot \underline{3} + 2 \quad 1 = 0 \cdot 3 + 3$

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

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

$2 = 0 \cdot 3 + 2$

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

$n = 3$: $6 = \underline{3} \cdot 2 + 0$

$MCD(n, n+3)$

$n = x \cdot 3 + y \qquad n = x \cdot 3 + 2 \qquad n = x \cdot 3 + \underline{1}$

$3 = 1 \cdot 2 + \underline{1} \qquad 3 = 3 \cdot 1 + 0$

**Prova a distanza**

**Problema 1:**
Un chimico vuole preparare un profumo miscelando in parti uguali 12 essenze base a sua disposizione.

1. (Punti 4) Quante sono in totale le miscele possibili usando 2, 3 o 4 essenze?
2. (Punti 4) Una volta scelta la miscela questa viene commercializzata in scatolette contenenti 6 boccette ciascuna, ognuna delle quali può essere di 4 colori diversi. Quante sono le confezioni possibili se le 6 boccette sono prese a caso?
3. (Punti 3) Quante invece sono le confezioni possibili se ogni scatola contiene 3 coppie di boccette dello stesso colore?

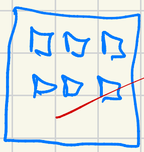
$|E| = 12$

1) Per 2 essenze $\binom{12}{2} = \frac{12!}{2!\cdot 10!} = \frac{12\cdot 11\cdot \cancel{10!}}{2!\cdot \cancel{10!}} = \frac{12\cdot 11}{2}$

Per 3 essenze $\binom{12}{3} = \frac{12!}{3!\cdot 9!} = \frac{12\cdot 11\cdot 10\cdot \cancel{9!}}{3!\cdot \cancel{9!}} = \frac{12\cdot 11\cdot 10}{3\cdot 2}$

Per 4 essenze $\binom{12}{4} = \frac{12!}{4!\cdot 8!} = \frac{12\cdot 11\cdot 10\cdot 9\cdot \cancel{8!}}{4!\cdot \cancel{8!}} = \frac{12\cdot 11\cdot 10\cdot 9}{4!}$

Totale $= 66 + 220 + 495 = 785$

2)  ~~$|C| = 4$~~ ~~$4\cdot 4\cdot 4\cdot 4\cdot 4\cdot 4 = 4^6 = 4096$~~

In questo caso scegliendone 6 su 4 con ripetizione sono combinazioni con ripetizione $\binom{9}{3} = 84$

3) Escludendo le 3 con colore uguale, le altre 3 possono avere $3^3 = 27$ combinazioni differenti. Le altre 3 hanno 4 possibili colori da cui scegliere per cui

$3^3 \cdot 4 = 108$ possibili combinazioni

LOL comprensione del Testo 0. 3 coppie uguali vuol dire che su 6 sono tutte uguali ovvero ci sono 4 possibilità

**Problema 2:** Si considerino le seguenti permutazioni di $S_9$:

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

1. (Punti 3) Si scriva la decomposizione di $\sigma$, $\tau$ e $\sigma \circ \tau^{-1}$ in cicli disgiunti
2. (Punti 4) Calcolare periodo e parità di $\sigma^2$, $\sigma^5$, $\tau^2$.
3. (Punti 4) Si considerino i seguenti sottoinsiemi di $S_9$, considerato come gruppo con l'operazione di composizione:

$$H_1 = \{\sigma^t | t \in \mathbb{Z}\}, \quad H_2 = \{\sigma^t | t \in \mathbb{Z}, \sigma^t(1) = 1\}.$$

Stabilire se $H_1$ e $H_2$ sono sottogruppi di $S_9$, motivando adeguatamente la risposta.

$$\begin{array}{l} \\ \tau^{-1} \\ \sigma \end{array} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 1 & 2 & 5 & 6 & 3 & 4 & 7 & 8 & 9 \\ 5 & 8 & 1 & 4 & 3 & 2 & 7 & 9 & 6 \end{pmatrix}$$

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

ok

1) $(1,5)(2,8,9,6,4) = \sigma$ $\quad \tau = (35)(4,6)$ $\quad \tau^{-1} = (35)^{-1}(4,6)^{-1} \Rightarrow (5,3)(6,4)$

2) $\sigma^2 = (1,5)^2(2,8,9,6,4)^2 = (2,9,4,8,6)$ $\quad \sigma^5 = (1,5)^5(2,8,9,6,4)^5 = (1,5)$ $\quad \tau^2 = (35)^2(4,6)^2 = id$

Tipo $(\sigma^2) = 5$ $\quad$ Tipo$(\sigma^5) = 2$
Periodo$(\sigma^2) = 5$ $\quad$ Periodo$(\sigma^5) = 2$ $\quad$ Periodo$(id = 1$
Parità $(\sigma^2) = P$ $\quad$ Parità$(\sigma^5) = D$ $\quad$ Parità $(id) = P$

3) $H_1$

- Esiste elem. neutro? Sì perché $\sigma^0$ esiste in $H_1$ per $t = 0 \in \mathbb{Z}$
- Esiste inverso? Sì perché essendo $t \in \mathbb{Z}$ senza 'restrizioni' $\forall t \in \mathbb{Z}\ \exists i \in \mathbb{Z}$ t.c. $t - i = 0$ ovvero $\forall \sigma^k \in H_1\ \exists \sigma^m \in H_1$ t.c. $\sigma^k \cdot \sigma^m = id$
- le operazioni sono contenute? Dati $\sigma^k, \sigma^m \in H_1$ con $k, m \in \mathbb{Z}$ $\quad \sigma^k \cdot \sigma^m = \sigma^{k+m}$ quindi $\sigma^{k+m} \in H_1$, $k+m \in \mathbb{Z}$

$H_2$

- Esiste neutro? $\sigma^0 \in H_2$ in quanto $t \in \mathbb{Z}$ e $\sigma^0(1) = 1$
- Esiste inverso? Sì. $\forall t_1 \in \mathbb{Z}\ \exists t_2$ t.c. $t_1 - t_2 = 0$ $\quad \forall \sigma^k \in H_2\ \exists \sigma^m \in H_2$ t.c. $\sigma^k \cdot \sigma^m = \sigma^{k-m} = \sigma^0$
- Le operazioni sono contenute? Dati $\sigma^k \circ \sigma^m$ in cui $\sigma^k, \sigma^m \in H_2$ appartengono ad $H_2$ perché $= \sigma^{k+m}$ in cui $k+m \in \mathbb{Z}$ e $\sigma^k \circ \sigma^m(1) = 1 \Leftrightarrow \sigma^{k+m}_{n \in \mathbb{Z}}(1) = 1$

ok

**Problema 1:** Si consideri la permutazione

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

1. (Punti 3) Calcolare il periodo e determinare la parità di $\pi$.
2. (Punti 4) Dire quante sono le permutazioni di $\mathcal{S}_9$ dello stesso tipo di $\pi$.
3. (Punti 4) Verificare che la funzione

$$f\colon \mathbb{Z}_8 \longrightarrow \mathcal{S}_9, \qquad f(\bar{k}) \mapsto \pi^{5k}$$

è ben definita ed è un omomorfismo. Determinarne poi il nucleo.

OK

1) $\pi = (1,8,2,9)(3,7,4,5,6)$ Tipo$(\pi) = (4,5)$ Periodo$(\pi) = $ mcm $4,5 = 20$

Parità$(\pi) = D+P = D$

2) $\dfrac{9 \cdot 8 \cdot 7 \cdot 6}{4} \cdot \dfrac{5 \cdot 4 \cdot 3 \cdot 2 \cdot 1}{5} = 756 \cdot 24 = 18144$ OK

3) Dati $\bar{a}, \bar{b} \in \mathbb{Z}_8$, se $\bar{a} = \bar{b} \rightarrow f(\bar{a}) = f(\bar{b})$

$20 \mid 40t$

Ovvero
$f(\bar{a}) = \pi^{5a} \Rightarrow \pi^{5(b+8t)} \Rightarrow \pi^{5b+40t}$
$= \pi^{5b} = f(\bar{b})$
Ben definita

sse $\pi^{5a} = \pi^{5b}$
sse $\pi^{5a-5b} = id$ OK
sse $a-b=0$
sse $8 \mid a-b$ in $\mathbb{Z}_8$
sse $\exists t$ t.c. $a = b+8t$

$f(\overline{a+b}) = f(\bar{a}) \circ f(\bar{b})$
$f(\overline{a+b}) = \pi^{5a} \circ \pi^{5b}$
$\pi^{5(a+b)} = \pi^{5a+5b}$
$\pi^{5a+5b} = \pi^{5a+5b}$ ✓ omomorfismo

$20 \mid 5 \cdot 0$ ✓
$20 \mid 5 \cdot 2$ ✗
$20 \mid 5 \cdot 3$ ✗
$20 \mid 5 \cdot 4$ ✓
$20 \mid 5 \cdot 5$ ✗
$20 \mid 5 \cdot 6$ ✗
$20 \mid 5 \cdot 7$ ✗

Kernel$(f) = \{\bar{0}, \bar{4}\}$

**Problema 2:**
In questo problema consideriamo classi resto in $\mathbb{Z}_{20}$.

1. (Punti 3) Quanti modi si hanno di scegliere 3 classi invertibili?
2. (Punti 4) Dire se il gruppo moltiplicativo $\mathbb{Z}_{20}^{\times}$ è ciclico o no.
3. (Punti 4) Determinare tutti gli $n \in \mathbb{Z}$ tale che $\bar{3}^n = \bar{9}$.

$\binom{8}{3} = \frac{8!}{3! \cdot 5!} = 56$

1) Elementi invertibili in $\mathbb{Z}_{20} = \{\bar{1}, \bar{3}, \bar{7}, \overline{11}, \bar{9}, \overline{13}, \overline{17}, \overline{19}\}$ ~~ovvero 8!~~

| | | | |
|---|---|---|---|
| MCD(20,1) = 1 ✓ | MCD(20,4) ≠ 1 ✗ | MCD(20,7) = 1 ✓ | MCD(20,10) ≠ 1 ✗ |
| MCD(20,2) ≠ 1 ✗ | MCD(20,5) ≠ 1 ✗ | MCD(20,8) ≠ 1 ✗ | MCD(20,11) = 1 ✓ |
| MCD(20,3) = 1 ✓ | MCD(20,6) ≠ 1 ✗ | MCD(20,9) = 1 ✓ | MCD(20,12) ≠ 1 ✗ |
| MCD(20,13) = 1 ✓ | MCD(20,14) ≠ 1 ✗ | MCD(20,15) ≠ 1 ✗ | MCD(20,16) ≠ 1 ✗ |
| MCD(20,17) = 1 ✓ | MCD(20,18) ≠ 1 ✗ | MCD(20,19) = 1 ✓ | |

2)/3) $\overline{3^0} = \bar{1}$ ✗, $\overline{3^1} = \bar{3}$ ✗, $\overline{3^2} = \bar{9}$ ✓, $\overline{3^3} = \overline{27} = \bar{7}$, $\overline{3^4} = \overline{81} = \bar{1}$

solo $n=3$ prima di raggiungere il periodo è ciclico.

Prova a distanza

**Problema 1:**
Alle elezioni a Freedonia partecipano 3 liste, A, B e C, ciascuna con 10 candidati e vi sono 2556 cittadini con diritto di voto.

1. (Punti 4) Ogni votante deve scegliere esattamente 2 liste, altrimenti il voto è nullo. In 910 hanno votato per A e B, in 795 per A e C, e B ha ricevuto 1658 voti validi. Quanti sono i voti nulli? Quale lista ha ottenuto più voti?
2. (Punti 3) Viene formato un comitato scegliendo a caso 4, 3 e 2 candidati dalle liste secondo l'ordine del risultato elettorale. Quanti sono i possibili comitati?
3. (Punti 4) Al voto è associato un referendum per la scelta della bandiera. La bandiera deve contenere il rosso, il nero e il blu e può avere tre strisce verticali oppure quattro strisce orizzontali senza colori uguali adiacenti. Quante sono le bandiere possibili?

$|P| = 2556 = |A \cup B \cup C|$

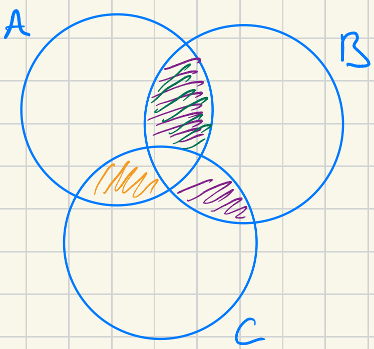
$|A \cap B| = 910$
$|A \cap C| = 795$ $\quad |C \cap B| = ?$

$|B \cap C| + |A \cap B| = 1658 \to$ Lista con B

1) I voti non validi sono

$2556 - 795 - 748 - 910$
$= 910$

Ha ottenuto più voti la lista con A poi B poi C




$A \cap B =$
$A \cap C =$

$B \cap C = 1658 - 910 = 748$
$|A \cap C| + |A \cap B| = 795 + 910 = 1705$
Lista con A
$|A \cap C| + |B \cap C| = 1543$
Lista C

$\binom{10}{4} \cdot \binom{10}{3} \cdot \binom{10}{2}$ ✓

3) $3! + (3 \cdot 2 \cdot 1 \cdot 2)$

**Problema 2:**
Rispondere ai punti seguenti

1. (Punti 3) Calcolare il resto della divisione di $5^{2139}$ per 84.
2. (Punti 4) Dimostrare che per ogni intero $n \geq 1$ si ha $\mathrm{MCD}(n, n^2+1) = 1$.
3. (Punti 4) Dire per quali $b \in \mathbb{Z}$ la congruenza

$$165 \cdot x \equiv 22 \cdot b \bmod 336$$

1) $\varphi(84) = \varphi(2^2) \cdot \varphi(3) \cdot \varphi(7) = 2 \cdot 2 \cdot 6 = 24$
$MCD(84, 5) = 1$
$84 = 16 \cdot 5 + 4$
$5 = 1 \cdot 4 + 1$
$4 = 4 \cdot 1 + 0$

$2139 = 89 \cdot 24 + 3$

1 in $\mathbb{Z}_{84}$

$5^{2139} = 5^{\cancel{89 \cdot 24}} \cdot 5^3 = 125 \bmod 84$
$= 41 \bmod 84$

2) Dimostro per induzione
Caso base $P(1) \Rightarrow MCD(1, \cancel{1^2+1}) = 1$ ? si per def
Caso Induttivo
$n^2+1 = x \cdot n + y$ $\quad$ Per euclide $MCD(n^2+1, n) = 1$
sse $= n \cdot n + 1$ $\quad x = n,\ y = 1$
sse $n = n \cdot 1 + 0$

3)
$MCD(165, 336) = 3 \longleftrightarrow ?$ 165 non è invertibile $\quad$ Per poter essere risolubile,
$336 = 2 \cdot 165 + 6$ $\quad 3 \mid 22 \cdot b$ ovvero
$165 = 27 \cdot 6 + 3$ $\quad = \{n \in \mathbb{Z} \mid n = 22 \cdot z \wedge 3 \mid n\}$
$6 = 2 \cdot 3 + 0$

**Problema 1:**
Si considerino le seguenti permutazioni in $\mathcal{S}_8$:

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

1. (Punti 3) Calcolare $\pi \circ \sigma$ e $\sigma \circ \pi$.
2. (Punti 4) Si consideri il sottogruppo ciclico $H = \langle \pi \rangle$ di $\mathcal{S}_8$. Stabilire se $\sigma$ appartiene a $H$.
3. (Punti 4) Si esibisca esplicitamente un sottogruppo di $\mathcal{S}_8$ di ordine 12 oppure si spieghi perché un tale sottogruppo di $\mathcal{S}_8$ non esiste.

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

$\sigma \circ \pi = (3,4,8,6)$

$$\begin{pmatrix} 1&2&3&4&5&6&7&8 \\ 1&7&8&6&2&4&5&3 \\ 1&2&4&8&5&3&7&6 \end{pmatrix} \begin{array}{l} \sigma \\ \pi \end{array} \quad \pi \circ \sigma = (3,4,8,6)$$

2) $\pi = (2,5,7)(3,6,8,4)$ $\quad$ Tipo$(\pi) = (3,4) = 12 =$ Periodo$(\pi)$

$\langle \pi \rangle = \{ id_{\mathcal{S}_8}, \pi, \pi^2, \pi^3, \pi^4, \pi^5, \pi^6, \pi^7, \pi^8, \pi^9, \pi^{10}, \pi^{11} \}$

$\sigma = (2,7,5)(3,8)(4,6)$ $\quad$ $\pi^2 = (2,7,5)(3,8)(6,4)$ sì

3) ~~Per il punto precedente, ogni generatore può avere al massimo periodo 12 perché coincidono il periodo con $\pi \in \mathcal{S}_8$~~ H è sottogruppo ciclico con ordine 12

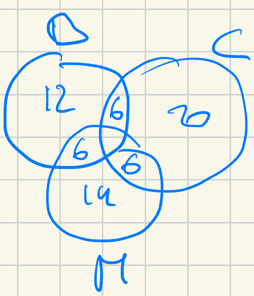
**Problema 2:** Una scuola di ballo deve organizzare il saggio di fine anno, che coinvolgerà in totale 32 partecipanti.

1. (Punti 3) Lo spettacolo prevede 2 protagonisti principali. In quanti modi si possono scegliere i 2 protagonisti tra i 32 partecipanti?
2. (Punti 4) I costumi dei partecipanti al saggio (protagonisti esclusi!) prevedono che 12 ballerini/e indossino una calzamaglia bianca, 20 un cappello e 14 una maglietta blu. Ci sono 6 ballerini che indossano sia la calzamaglia bianca sia il cappello, 6 che indossano sia il cappello sia la maglietta blu e 6 che indossano sia la calzamaglia bianca sia la maglietta blu. Quanti ballerini/e indosseranno cappello e maglietta blu, ma non una calzamaglia bianca?
3. (Punti 4) Una volta scelti i 2 protagonisti principali, gli altri partecipanti al saggio devono formare due file da 15 persone ciascuna. In quanti modi diversi possono essere formate le due file?

$|P| = 32$ $\quad$ Ok

$$\binom{32}{2} = \frac{32!}{2! \cdot 30!} = \frac{32 \cdot 31 \cdot \cancel{30!}}{2! \cdot \cancel{30!}} = 496$$

2) $|P| = 30$ $\quad$ $|B| = 12$ $\quad$ $|C| = 20$ $\quad$ $|M| = 14$ $\quad$ Ok




$|B \cap C| = 6$ $\quad$ $|C \cap M| = 6$ $\quad$ $|B \cap M| = 6$

$|B \cap C \cap M| = 30 - 12 - 20 - 14 + 18 = 2$

$|(C \cap M) \setminus B| = 6 - 2 = 4$

Ok

3) $(30 \cdot 29 \cdot 28 \cdot 27 \cdot 26 \cdot 25 \cdot 24 \cdot 23 \cdot 22 \cdot 21 \cdot 20 \cdot 19 \cdot 18 \cdot 17 \cdot 16) \cdot 15! = 30!$

**Problema 1:**
In questo problema consideriamo il gruppo $\mathcal{S}_7$ delle permutazioni su 7 elementi.

1. (Punti 3) Calcolare periodo e parità della permutazione

$$\pi = (5\ 6\ 3\ 1\ 2)(7\ 4)(1\ 7\ 3)(2\ 5\ 4) \in \mathcal{S}_7.$$

2. (Punti 4) Sia $f : \mathbb{Z}_5 \to \mathcal{S}_7$ un omomorfismo iniettivo. Dire quali delle seguenti permutazioni sicuramente **non** sono nell'immagine di $f$:

$\sigma_1 = (1\ 6)(2\ 7\ 3)$, $\sigma_2 = (2\ 5\ 4\ 6)$
$\sigma_3 = (2\ 4\ 1\ 7\ 6)$, $\sigma_4 = (2\ 5)(1\ 6)(3\ 4)$.

3. (Punti 4) Esiste in $\mathcal{S}_7$ un sottogruppo con 10 elementi?

ok

$\pi = (1,4,5,7)(2,6,3)$ Tipo$(\pi) = (4,3)$ Parità $= D+P = D$
Periodo $= 12$

2)

3) Si per $\sigma \in S_7$ con Tipo $= (2,5)$ es: $(1,2)(3,4,5,6,7)$
Periodo$(2,5) = 10$
quindi $\langle\sigma\rangle = \{id, \sigma, \sigma^2, \sigma^3, \sigma^4, \sigma^5, \sigma^6, \sigma^7, \sigma^8, \sigma^9\}$ ok

**Problema 2:**

1. (punti 4) Dire se esiste l'inverso moltiplicativo di 35 modulo 143 ed in caso affermativo calcolarlo.
2. (punti 4) Calcolare il resto della divisione di $7^{1362} - 11^{449}$ per 60.
3. (Punti 3) Determinare tutte le soluzioni della congruenza

$$15X + 9 \equiv 0 \bmod 36.$$

1) $MCD(35, 143) = 1$ è invertibile

$143 = 4 \cdot 35 + 3$
$35 = 11 \cdot 3 + 2$
$3 = 1 \cdot 2 + 1$
$2 = 2 \cdot 1 + 0$

$1 = 12 \cdot 143 - 49 \cdot 35$
$1 = 12 \cdot 3 - 1 \cdot 35 \to 12 \cdot (143 - 4 \cdot 35) - 1 \cdot 35 \to 12 \cdot 143 - 48 \cdot 35 - 1 \cdot 35$
$1 = 3 - 1 \cdot 2 \to 1 = 3 - 1 \cdot (35 - 11 \cdot 3) \Rightarrow 1 = 3 - 1 \cdot 35 + 11 \cdot 3$
$2 = 35 - 11 \cdot 3$
$3 = 143 - 4 \cdot 35$

$12 \cdot 4 = 48$

$1 = \cancel{12 \cdot 143} - 49 \cdot 35$
$1 = -49 \cdot 35$ l'inverso è $-49$ in $\mathbb{Z}_{143}$ $= 94 \bmod 143$

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

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

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

$1362 : 16 = 85$, resto $2$ ($1362 - 128 = 82$, $82 - 80 = 2$)
$1362 = 85 \cdot 16 + 2$
$7^{1362} = \cancel{7^{16 \cdot 85}} \cdot 7^2$
$49 \bmod 60$

$449 : 16 = 28$, resto $1$ ($449 - 32 = 129$, $129 - 128 = 1$)
$11^{449} = \cancel{11^{16 \cdot 28}} \cdot 11 = 11 \bmod 60$

$49 - 11 \bmod 60$
$38 \bmod 60$

**Problema 2:**

1. (punti 4) Dire se esiste l'inverso moltiplicativo di 35 modulo 143 ed in caso affermativo calcolarlo.
2. (punti 4) Calcolare il resto della divisione di $7^{1362} - 11^{449}$ per 60.
3. (Punti 3) Determinare tutte le soluzioni della congruenza

$$15X + 9 \equiv 0 \bmod 36.$$

$15x + 9 \equiv 0 \bmod 36$

$15x \equiv 27 \bmod 36$

$MCD(15,36) = 3$

$36 = 2 \cdot 15 + 6$

$15 = 2 \cdot 6 + 3$

$6 = 2 \cdot 3 + 0$

15 non è invertibile ma $3 | 27$

$$\frac{15x}{3} \equiv \frac{27}{3} \bmod \frac{36}{3}$$

$5x \equiv 9 \bmod 12$

$MCD(5,12) = 1$

$12 = 2 \cdot 5 + 2$

$5 = 2 \cdot 2 + 1$

$1 = 5 - 2 \cdot 2$

$1 = 5 - 2 \cdot (12 - 2 \cdot 5) \rightarrow x \equiv 45 \bmod 12$

$1 = 5 - 2 \cdot 12 + 4 \cdot 5 \quad x \equiv 9 \bmod 12$

$1 = 5 \cdot 5 - 2 \cdot 12$

$= \{9, 21, 33\}$

**Problema 1:**
Ricordato che un numero in base 8 si scrive utilizzando le cifre $\{0, 1, 2, 3, 4, 5, 6, 7\}$ rispondere alle domande seguenti.

1. (Punti 3) Quanti sono in base 8 i numeri di tre cifre (quindi da 100 a 777 inclusi) che non includono la cifra 4?
2. (Punti 4) Quanti sono in base 8 i numeri di tre cifre (quindi da 100 a 777 inclusi) che includono la cifra 6 esattamente una volta?
3. (Punti 4) Quanti sono in base 8 i numeri di tre cifre (quindi da 100 a 777 inclusi) formati da tre cifre consecutive anche non ordinatamente? (ad esempio: 201, 453, eccetera)

1) $6 \cdot 7 \cdot 7 = 294$

2) $\left.\begin{array}{l} 6\,\_\,\_ \to 7 \cdot 7 \\ \_\,6\,\_ \to 6 \cdot 7 \\ \_\,\_\,6 \to 6 \cdot 7 \end{array}\right\} + = 133$

3) Quelle accettate sono (escludendo ordine

$1,2,3$ , $2,3,4$, $3,4,5$, $4,5,6$, $5,6,7$ , $012$ → esclude $012$ $021$

$3! + 3! + 3! + 3! + 3! + 3!$

$= 6 \cdot 3! = 36 - 2 = 34$

$4 = 1 \cdot 3 + 1$

**Problema 2:** Si consideri la permutazione in $\mathcal{S}_8$ data da

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

1. (punti 4) Calcolare periodo e parità di $\sigma$.
2. (punti 3) Trovare una permutazione $\tau \in \mathcal{S}_8$ tale che
$$\sigma \circ \tau = (2\ 5\ 8).$$
3. (Punti 4) Denotato $G = \langle \sigma \rangle$ il sottogruppo di $\mathcal{S}_8$ generato da $\sigma$ si verifichi che la funzione
$$f : G \longrightarrow \mathbb{Z}_8, \qquad f(\sigma^k) = \overline{2k}$$
è un omomorfismo e dire se è iniettivo o suriettivo.

1) $\sigma = (1,4,7)(3,8,6,5)$   tipo $(3,4)$   Periodo mcm$(3,4) = 12$

Parità $= P + D$
$= D$

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

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

3) Ben definita?

Dati $\sigma^a, \sigma^b \in S_8$ allora

se $\sigma^a = \sigma^b \to f(\sigma^a) = f(\sigma^b)$

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

sse $12 \mid a-b$

$24 \mid 2(a-b)$

$24 \mid 2a-2b$ verificato

sse $2a = 2b$

Omomorfismo

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

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

$2(a+b) = 2a + 2b$

$2a + 2b = 2a + 2b$

Immagine

$= \{\overline{0}, \overline{2}, \overline{4}, \overline{6}\}$

$\neq \mathbb{Z}_8$ non è iniettiva

Iniettivo

Kernel$(f)$

$= \{\sigma^k \mid \overline{2k} \equiv \overline{0} \bmod 8\}$

$= \{id, \sigma^4, \sigma^8\}$

Non è iniettiva