

# MCD • SUCCESSIONE "18"

Esercizio 1. Serena ha comprato anche quest'anno 6 regali diversi per i suoi 6 nipotini.

- Per incartarli ha comprato 6 fogli di carta di colori diversi. In quanti modi può abbinare la carta ai regali?
- Lo scorso anno aveva comprato per i nipotini 3 modellini di auto (uguali) e 3 giochi da tavolo (tutti diversi). In quanti modi diversi poteva distribuire i regali ai nipoti?
- Due anni fa ognuno dei 6 regali aveva almeno uno delle seguenti caratteristiche: era stato incartato, aveva un fiocco oppure era grande. Più esattamente: 3 erano incartati, 3 erano grandi e 3 avevano sopra un fiocco. 2 erano incartati e grandi, 1 era incartato e con fiocco, e 1 era grande con fiocco. Quanti regalini hanno ricevuto un pacco grande, incartato e con fiocco?

1.b)

$\begin{matrix} 3 \\ \text{3 nipoti} \\ \text{hanno lo} \\ \text{stesso regalo} \end{matrix}$ 

 $\begin{pmatrix} 3 \\ 3 \end{pmatrix}$ 
 $= \cancel{\frac{3!}{3!}} \cdot \underline{(3 \cdot 2 \cdot 1)}$ 
  
giusto per i rimanenti

$\cancel{\frac{3!}{3!}} \cdot \underline{(3 \cdot 2 \cdot 1)}$

1.c)  $R = \text{regali}$ ,  $x = \{ r \in R \mid r \text{ è incartato} \}, |x| = 3$

$$\begin{cases} |x \cap y| = 2 \\ |x \cap z| = 1 \\ |y \cap z| = 1 \end{cases}$$

$$y = \{ r \in R \mid r \text{ è grande} \}, |y| = 3$$

$$z = \{ r \in R \mid r \text{ ha un fiocco} \}, |z| = 3$$

$$|x \cup y \cup z| = 6$$

$$|x \cup y \cup z| = |x| + |y| + |z| - |x \cap y| - |x \cap z| - |y \cap z| + |x \cap y \cap z|$$

$$\begin{aligned} 6 &= 3 + 3 + 3 - 2 - 1 - 1 + \cancel{x} \cancel{x} \\ -x + 6 &= 9 - 4 \\ -x &= 5 - 6 \\ x &= +1 \quad \text{solo 1 regalo} \end{aligned}$$

Scelte

$$\begin{matrix} 6 \circ 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1 \\ \cancel{a} \cancel{l} \quad \cancel{1} \cancel{4} \cancel{3} \cancel{2} \cancel{1} \\ \cancel{1}^0 \quad 2^0 \quad 3^0 \quad 4^0 \end{matrix}$$

(ou)

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

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

- a) Determinare la decomposizione in cicli disgiunti di  $\sigma$  e  $\tau$ .  
 b) Calcolare il periodo di  $\sigma$ ,  $\tau$  e  $\sigma\tau$ .

c) Dire perché la funzione  $f : \mathbb{Z}_{10} \rightarrow S_7$ ,  $f(\bar{k}) = \sigma^k$  è ben definita, perché è un omomorfismo non suriettivo e determinarne il nucleo.

2.a

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

$\textcircled{O} u$

2.b

$$\begin{aligned}\text{Periodo } (\sigma) &= 5 \\ \text{Periodo } (\tau) &= (3, 3)\end{aligned}$$

2.c Ben definita

$$\begin{aligned}\text{Periodo } = 5 \\ \text{Periodo } = 3\end{aligned}$$

$$\text{Periodo } (\sigma\tau) = 3$$

$\textcircled{O} u$

$\mathbb{Z}_{10}$  sono i numeri nella forma  $z = n + 10$   
 l'inverso è  $\bar{z}$  tale che  $\text{MCD}(z, 10) = 1$   
 Ovvero  $\bar{z} = z \cdot x + y \cdot 10$  quindi

$$\bar{y} \cdot 10 = \bar{0} \text{ in } \mathbb{Z}_{10}$$

$$\begin{aligned}f(x \cdot z + y \cdot 10) &= f(x) \\ f(xz) &= \sigma^{xz} \Rightarrow (\sigma^z)^x \Rightarrow \sigma^z \quad \text{Verificato} \\ \text{Omomorfismo} \quad f(\bar{z}) \cdot f(\bar{y}) &= f(\bar{z} \cdot \bar{y}) \\ \sigma^z \cdot \sigma^y &= f(\bar{z} \cdot \bar{y}) \\ \sigma^{z+y} &= \sigma^z \cdot \sigma^y\end{aligned}$$

$$\underline{\text{Nucleo}} \quad \text{Kernel}(f) = \{g \in \mathbb{Z}_{10} \mid f(g) = \text{id}_{S_7}\}$$

Ovvero tutti i  $n'$  che hanno inverso  $n = 0$   
 $\frac{n \cdot n'}{10} = \bar{0}$  e  $n$  è multiplo di 10  
 $n = 10n$

Quindi sono tutti i multipli di 10 con resto 0

$$\sigma^0 = \sigma^0 = \text{id}_{S_7}$$

$$\left( \begin{array}{ccccccc} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 5 & 4 & 3 & 7 & 6 & 1 & 2 \\ 1 & 5 & 3 & 4 & 6 & 2 & 7 \end{array} \right) \xrightarrow{\tau} \left( \begin{array}{ccccccc} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 5 & 4 & 3 & 6 & 7 & 1 & 2 \\ 1 & 5 & 3 & 6 & 2 & 7 & 4 \end{array} \right)$$

$$\sigma\tau = (2, 5, 6) \quad \text{Periodo } = 3$$

**Esercizio 3. a)** Calcolare  $\text{MCD}(3575, 654)$  e realizzare l'identità di Bezout.

b) Calcolare il resto della divisione per 27 del numero  $3^{12007} + 5^{36184}$ .

c) Dire se il gruppo  $\mathbb{Z} \times \mathbb{Z}_4$  è ciclico o no.

oa

$$\begin{array}{l}
 \text{3.a) } \text{MCD}(3575, 654) \\
 3575 = 5 \cdot 654 + 305 \\
 654 = 2 \cdot 305 + 44 \\
 305 = 6 \cdot 44 + 41 \\
 44 = 1 \cdot 41 + 3 \\
 41 = 13 \cdot 3 + 2 \\
 3 = 1 \cdot 2 + 1 \\
 2 = 2 \cdot 1 + 0
 \end{array}
 \quad
 \begin{array}{l}
 \text{Bezout} = 1219 \cdot 654 - 223 \cdot 3575 \\
 1 = 104 \cdot 654 - 223 \cdot (3575 - 5 \cdot 654) \Rightarrow 104 \cdot 654 - 223 \cdot 3575 + 1115 \cdot 654 \\
 1 = 104 \cdot (654 - 2 \cdot 305) - 15 \cdot 305 \Rightarrow 104 \cdot 654 - 208 \cdot 305 - 15 \cdot 305 \\
 1 = 14 \cdot 44 - 15 \cdot (305 - 6 \cdot 44) \Rightarrow 14 \cdot 44 - 15 \cdot 305 + 90 \cdot 44 = 104 \cdot 44 - 15 \cdot 3 \\
 1 = 14(44 - 1 \cdot 41) - 41 \Rightarrow 14 \cdot 44 - 14 \cdot 41 - 41 = 14 \cdot 44 - 15 \cdot 41 \\
 1 = 3 - (44 - 13 \cdot 3) \cdot 1 \Rightarrow 3 - 44 + 13 \cdot 3 \Rightarrow 14 \cdot 3 - 41 \\
 1 = 3 - 2 \cdot 1 \qquad \qquad 2 = 44 - 13 \cdot 3 \\
 1 = 3 = 44 - 1 \cdot 41
 \end{array}$$

$$3.b) \quad \ell(2z) = \ell(z^3) = z^2 \cdot 2 = 18$$

$\text{MCD}(3, 27) \Rightarrow 27 = 9 \cdot \underline{3} + 0$  Non si può fare altro, provo lo stesso...

$$3^3 \bmod 27 \quad 3^3 \bmod 27 = 27 \bmod 27 \quad \text{quindi} \quad \begin{array}{c} 3 \\ \times 3 \\ \hline 9 \\ \times 3 \\ \hline 27 \end{array}$$

$$3 \cdot 3 \equiv 0 \pmod{27}$$

$$\begin{aligned} S &= 2 \cdot 2 + 1 \\ 2 &= 2 \cdot 1 + 0 \end{aligned}$$

$$36184 = 21 \cdot 18 + 4$$

$$S^u \equiv S^{u \bmod 27} \quad (\text{mod } 27)$$

$$0 + 5^4 \bmod 27 \Rightarrow 625 \bmod 27 \Rightarrow \cancel{625} \bmod 27$$

3c)  $\mathbb{Z}$  è infinito = {0, 1, 2, 3, ...} mentre  $\mathbb{Z}_n$  non lo è per cui  $\mathbb{Z} \times \mathbb{Z}_n$  non è in grado di generare elementi infiniti, ma solo elementi che si ripetono

**Esercizio 1.** Ad un corso di tango sono iscritti 8 donne e 12 uomini. Si tengono due lezioni la settimana, il lunedì e il giovedì.

a) Se ad una lezione tutti gli studenti sono presenti, quante sono le possibili coppie (uomo-donna) che si possono formare durante la lezione?

b) Per uno spettacolo alla fine del corso i maestri scelgono fra gli studenti 4 uomini e 4 donne per una certa coreografia. Quante sono le scelte possibili di quei 8 studenti?

c) La scorsa settimana ogni studente era presente ad almeno una lezione: al lunedì erano presenti 8 uomini e 6 donne mentre al giovedì erano presenti 9 uomini e 7 donne. Quanti dei 20 studenti erano presenti ad entrambe le lezioni?

~~$$8 \cdot 8 \cdot 7 \cdot 7 \cdot 6 \cdot 6 \cdot 5 \cdot 5 \cdot 6 \cdot 6 \cdot 3 \cdot 3 \cdot 2 \cdot 2 \cdot 1 = 8! \cdot 8!$$~~

2.b)  $\binom{9}{8} \cdot \binom{12}{4}$  OU

donne 4

1.c)  $|S_2| = 8+6 = 14$  J

$|S_6| = 9+7 = 16$

$$\begin{aligned}|S_2 \cap S_6|? &= |S_2| + |S_6| - |S_2 \cup S_6| \\&= 14 + 16 - 8 \\&= 30 - 8 \\&= 22\end{aligned}$$

OU

**Esercizio 2.** Consideriamo le seguenti due permutazioni di  $S_9$  date come prodotto di cicli:

$$\alpha = (3 \ 7 \ 6 \ 9 \ 5)(2 \ 8 \ 4), \quad \beta = (1 \ 3 \ 7 \ 9 \ 8 \ 4)^2.$$

a) Determinare il periodo di  $\alpha$  e  $\beta$ .

b) Calcolare la parità di  $\alpha$ , di  $\beta$  e di  $\alpha^3 \circ \beta^{-1}$ .

c) Dire (motivando la risposta) quali dei seguenti gruppi sono isomorfi a  $(\mathbb{Z}_{15}, +)$ :

$$H = (\langle \alpha \rangle, \circ), \quad L = (\mathbb{Z}_3 \times \mathbb{Z}_5, +), \quad M = (\mathbb{Z}_5 \times \mathbb{Z}_5 \times \mathbb{Z}_5, +).$$

2.a)  $\text{Parity}(\alpha) = D+D = P$  OU  
 $\text{Parity}(\beta) = D+D = P$

2.c) Per isomorfismo si intende  
Omomorfismo biettivo.

2.c.1 se  $H$  è isomorfo a  $(\mathbb{Z}_{15}, +)$  allora  $h \cdot h'$  in  $\alpha$  è come dire  $f(h \cdot h') = f(h) + f(h')$

$$\alpha^u \cdot \alpha^v = \alpha^{u+v}$$

$\langle \alpha \rangle =$  ogni elemento di  $\alpha$   
è gerenabile a partire  
dal  $\alpha$

2.c.2  $15 = 3 \cdot 5$ , EZ

Per def. 3 e 5 sono coprimi  $\text{PGCD}(3,5)=1$

$\mathbb{Z}_5$  è isomorfo al prod. cartesiano dei suoi elementi  $\mathbb{Z}_3 \times \mathbb{Z}_5$

$\mathbb{Z}_3 \times \mathbb{Z}_5 \times \mathbb{Z}_5$  Non possono essere un isomorfismo in quanto 3,5,5 non sono componenti di 15.

2.c.3  $15 = 3 \cdot 5$

SA

Esercizio 3. Sia  $f: \mathbb{Z}_{18} \rightarrow \mathbb{Z}_9$  data da  $f([a]_{18}) = [4a]_9$ .

a) Verificare che  $f$  è ben definita ed è un omomorfismo tra i gruppi  $(\mathbb{Z}_{18}, +)$  e  $(\mathbb{Z}_9, +)$ .

b) Determinare l'immagine di  $f$  è stabilire se  $f$  è suriettivo.

c) Determinare tutti i numeri interi  $x$  tali che  $0 \leq x < 18$  e  $[x]_{18} = [7^{344}]_{18}$ .

3.a)

$n \in \mathbb{Z}_{18}$  sono definibili come  
 $n \in \mathbb{Z}_9 \quad \equiv \quad n = y + 18$

$$n = y + 9$$

$$\begin{aligned} f([y+18]) &= [4 \cdot (y+18)]_9 \\ &= [4 \cdot y + 4 \cdot 18]_9 \\ &= [4 \cdot y]_9 \end{aligned} \quad \begin{array}{l} 18 = 0_2 \text{ in } \mathbb{Z}_9 = 0 \\ \text{Verificata} \quad \text{Benz del.} \end{array}$$

$$f([a]_{18}) + f([a]_{18}) = f([a]_{18} + [a]_{18})$$

OK

$$\begin{aligned} [4a]_9 + [\sum 4a]_9 &= f([a+a]_{18}) \\ [4(a+a)]_9 &= [4 \cdot (a+a)]_9 \end{aligned}$$

Verificata

3.b)

Siccome  $9 \mid 18$  allora per ogni  $a \in \mathbb{Z}_{18}$   
 $f$  copre  $\mathbb{Z}_9$  come omomorfismo suriettivo  
 visto che è suriettivo per def  $\text{Im}(f) = \mathbb{Z}_9$

3.c)

$$x \equiv 7 \pmod{18}$$

Serve calcolare resto di  
 $7^{344} / 18$

$$\begin{aligned} 7^{344} &\equiv 7 \cdot 6 + 2 \\ 7 &\equiv 7^{344} \pmod{18} \\ &\equiv (7^6)^5 \cdot 7 \end{aligned}$$

$$\begin{aligned} \varphi(18) &= \varphi(3^2) \cdot \varphi(2) \\ &= 3 \cdot 2 \cdot 1 \\ &= 6 \end{aligned}$$

$\text{MCD}(7, 18)$

$$\begin{array}{r} 18 \\ 14 \\ 4 \\ 2 \\ \hline 0 \end{array} \quad \begin{array}{r} 18 \\ 14 \\ 4 \\ 2 \\ \hline 0 \end{array} \quad \begin{array}{r} 18 \\ 14 \\ 4 \\ 2 \\ \hline 0 \end{array}$$

$$\begin{array}{r} 18 = 2 \cdot 7 + 4 \\ 7 = 1 \cdot 4 + 3 \\ 4 = 1 \cdot 3 + 1 \\ 3 = 3 \cdot 1 + 0 \end{array}$$

$$\begin{array}{r} 18 \\ 14 \\ 4 \\ 2 \\ \hline 0 \end{array}$$

$$\begin{array}{r} 6 \\ 18 \\ 8 \\ 4 \\ \hline 2 \\ 16 \\ 14 \\ 2 \\ \hline 0 \end{array} \quad \begin{array}{r} 7 \\ 18 \\ 9 \\ 3 \\ \hline 2 \\ 16 \\ 14 \\ 2 \\ \hline 0 \end{array}$$

$$\begin{array}{r} 36 \\ 30 \\ 6 \\ 2 \\ \hline 0 \end{array} \quad \begin{array}{r} 6 \\ 54 \\ 27 \\ 18 \\ 9 \\ 3 \\ \hline 0 \end{array}$$

$$\begin{array}{r} 18 \\ 12 \\ 6 \\ 2 \\ \hline 0 \end{array} \quad \begin{array}{r} 4 \\ 18 \\ 12 \\ 6 \\ 2 \\ \hline 0 \end{array}$$

Esercizio 1. Anna possiede 11 magliette, 5 paia di pantaloni, 6 paia di scarpe e 2 borsette.

- In quanti modi diversi Anna può scegliere maglietta, pantaloni, scarpe e borsetta per vestirsi?
- Anna ha comprato una scarpiera che ha 14 scomparti. In quanti modi diversi Anna può riporre le sue scarpe mettendo ogni paio di scarpe in un diverso scomparto nella scarpiera?
- Anna parte per un weekend al mare e decide di portare con sé 4 magliette, 2 paia di pantaloni, 2 paia di scarpe e 1 borsetta. Quante sono le possibili scelte di questi capi?

Ovvero deve scegliere le quadri da

2.b

$$14 \cdot 13 \cdot 12 \cdot 11 \cdot 10 \cdot 9$$

2.c

$$\begin{array}{c} \left(\begin{array}{c} 11 \\ 4 \end{array}\right) \quad \left(\begin{array}{c} 5 \\ 2 \end{array}\right) \quad \left(\begin{array}{c} 6 \\ 2 \end{array}\right) \quad \left(\begin{array}{c} 2 \\ 1 \end{array}\right) \\ \text{magliette} \quad \text{pantaloni} \quad \text{scarpe} \end{array}$$

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

$$\alpha = (3\ 5)(1\ 2\ 4)(2\ 7\ 4\ 5), \quad \beta = (1\ 2\ 4\ 7\ 6)(1\ 3\ 5\ 7).$$

- Determinare la decomposizione in cicli disgiunti di  $\alpha$  e di  $\alpha^2$ .
- Calcolare il periodo di  $\alpha$ , il periodo di  $\beta$  e il periodo di  $\beta \circ \alpha$ .
- Dire perché la funzione  $f : \mathbb{Z}_9 \rightarrow S_7$  data da  $f(k) = \alpha^k$  è ben definita, perché è un omomorfismo di gruppi e perché non è né iniettiva né suriettiva.

$$\text{2.b)} \quad \text{Tipo}(\alpha) = (3, 3), \quad P(\alpha) = \text{mcml}(3, 3) = 3$$

$$\alpha^2 = (1\ 7\ 2)(3\ 4\ 5)$$

$$\begin{aligned} \beta &= (1\ 2\ 4\ 7\ 6)(1\ 3\ 5\ 7) \\ &= (1\ 3\ 5\ 6)(4\ 7\ 2) \quad \text{Tipo}(\beta) = (4, 3) \quad P(\beta) = \text{mcml}(4, 3) = 12 \end{aligned}$$

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 7 & 5 & 3 & 4 & 6 & 1 \\ 4 & 2 & 6 & 5 & 7 & 1 & 3 \end{pmatrix}_{\beta} \quad \text{Beta}$$

$$\beta \circ \alpha = (1, 4, 5, 7, 3, 6) \quad \text{Tipo}(\beta \circ \alpha) = 6$$

④

$$P(\beta) = 6$$

2.c

$$n \in \mathbb{Z}_a \iff n = y + a$$

$$f(\bar{n} + \bar{k}) = f(\bar{n}) \cdot f(\bar{k}) \quad \text{④}$$

Non è suriettiva in quanto

Non è iniettiva in quanto

$$\ker(f) = \{0, 3, 6\} \neq \{0\}$$

2.a) Anna deve

Scegliere 3 elementi

$$|\mathcal{P}| = 5, |\mathcal{S}| = 6, |\mathcal{B}| = 2$$

$$|\mathcal{H}| = 11$$

④

$$M \times P \times S \times B = 5 \cdot 6 \cdot 2 \cdot 11 = 660$$

④

④

$$2.a) \quad \alpha = (3\ 5)(1\ 2\ 4)(2\ 7\ 4\ 5)$$

④

$$= (1\ 2\ 7)(3\ 5\ 4)$$

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 7 & 5 & 3 & 4 & 6 & 1 \\ 4 & 2 & 6 & 5 & 7 & 1 & 3 \end{pmatrix}_{\alpha} \quad \text{Alpha}$$

per il punto 2.b)  $P(\alpha) = 3$

per cui  $P(\alpha) \mid a$  per

cui per qualsiasi  $n \in \mathbb{Z}_a$

$$f(n) = \sigma^n y = \sigma^y$$

siconcluse che è

ben definita.

Esercizio 3.

- a) Calcolare MCD(5355, 651) e realizzare l'identità di Bezout.  
 b) Determinare le ultime 2 cifre del numero  $17^{20922} + 25^{15775}$ .  
 c) Trovare tutte le soluzioni della congruenza  $12x \equiv 16 \pmod{140}$ .

2a)  $5355 = 8 \cdot 651 + 147 \quad 21 = 9 \cdot (5355 - 8 \cdot 651) - 2 \cdot 651 \Rightarrow 9 \cdot 5355 - 72 \cdot 651 - 2 \cdot 21$   
 $651 = 4 \cdot 147 + 63 \quad 21 = 147 - 2 \cdot (651 - 4 \cdot 147) = 147 - 2 \cdot 651 + 8 \cdot 147$   
 $147 = 2 \cdot 63 + 21 \quad 21 = 147 - 2 \cdot 63$   
 $63 = 3 \cdot 21 + 0$

2b)  $\varphi(100) = \varphi(5^2 \cdot 2^4) = 5 \cdot 4 \cdot 2 = 40$   
 Scompongo le potenze:  $20922 = 523 \cdot 40 + 2$  e  $15775 = 394 \cdot 40 + 15$   
 $523 \cdot 40 + 2 \quad 40^2 \quad \text{MCD}(17, 100) = 1$   
 $17 \Rightarrow 17 \cdot 17 = 289 \pmod{100} = 89 \pmod{100}$

$\text{MCD}(25, 100) \neq 0$  ma  $100 = 4 \cdot 25 + 0 \Rightarrow 25 \mid 100$   
 ovvero  $25^k \equiv 25 \pmod{100}$  quindi  
 $25^{15775} \equiv 25$   
 Quindi  $25 + 89 \pmod{100} = 114 \pmod{100} = 14 \pmod{100}$   
 $12x = 16 \pmod{40}$  a è invertibile  $\text{MCD}(12, 40) = 4$   
 $\text{MCD}(12, 40) \mid 16$        $16 = 11 \cdot 12 + 8$       Non  
 $12 = 3 \cdot 8 + 4$       inutile!  
 $8 = 2 \cdot 4 + 0$

$$3 \frac{12x}{12} + 140y = \frac{16}{12} \cdot 12$$

$$3x + 35y = 4 \Rightarrow 3x \equiv 4 \pmod{35}$$

$$\text{inv. di } a = 12$$

$$x = 4 \cdot 12 \pmod{35}$$

$$= 48 \pmod{35}$$

$$13 \pmod{35}$$

$$x_1 = 13, x_2 = 13 + 35 = 48$$

$$x_3 = 13 + 35 \cdot 2 = 83, x_4 = 13 \cdot 3 \cdot 35 = 118$$

$$\text{MCD}(5355, 651) = 21$$

(16)

$$\text{Bezout} \\ = q \cdot 5355 - 72 \cdot 651$$

$$q = 9, 651 = 4 \cdot 147 + 63$$

$$147 = 2 \cdot 63 + 21$$

$$63 = 3 \cdot 21 + 0$$

$$63 = 651 - 4 \cdot 147 \quad 147 = 5355 - 8 \cdot 651$$

$$147 = 5355 - 8 \cdot (523 \cdot 40 + 2)$$

$$147 = 5355 - 3384 - 16$$

$$147 = 1691$$

$$1691 = 21 \cdot 80 + 1$$

Esercizio 1. a) Calcolare il numero di anagrammi diversi della parola ALMENO e quelli della parola ADEGUATAMENTE.

b) Ad una gara partecipano 10 squadre ed in palio ci sono 4 premi uguali. Quante possono essere le possibili quaterne di squadre vincitrici?

c) La squadra A ha totalizzato 12 punti. Carlo, Viola e Giovanna, che costituiscono la squadra A, hanno ottenuto rispettivamente  $c$ ,  $v$  e  $g$  punti nelle varie prove. Quante sono le possibili terne  $(c, v, g)$ ?

$$\Sigma = \{a, l, m, e, n, o\} = 6!$$

1.a)  $\Sigma = \{a, l, d, e, g, v, t, m, n\}$   $|P| = 13$

$$= \frac{13!}{3! \cdot 1! \cdot 3! \cdot 1! \cdot 2! \cdot 1! \cdot 1!} = \frac{13!}{3! \cdot 3! \cdot 2!} =$$

1.b)  $|S| = 10$   $|P| = 4$  scegliere 4 su 10 S

$$\binom{10}{4} \quad \text{ou}$$

$$S_1 S_2 S_3 S_4 = S_u S_v S_w S_x$$

$$S_1 S_2 \dots = X$$

$$\in C \times V \times G$$

$$|C \times V \times G|$$

Combinationi con rip.

di 12 punti su 3

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

Esercizio 2. a) Calcolare il periodo della permutazione

$$\pi = (3 \ 4 \ 1 \ 6)(1 \ 6 \ 5 \ 2) \in S_6$$

b) Qual è il periodo massimo di una permutazione in  $S_{10}$ ?

c) Sia  $\sigma = (1 \ 4)(2 \ 5 \ 3) \in S_5$ . Dimostrare che  $f([k]) = \sigma^{2k}$  definisce un omomorfismo  $f : \mathbb{Z}_{18} \rightarrow S_5$  e se ne calcolino nucleo e immagine.

2.a  $(1 \ 3 \ 4)(2 \ 6 \ 5) = \pi$   $\text{Tipo}(\pi) = (3, 3)$   $P(\pi) = 3$

2.b ~~10 periodi. Sono i  $\text{Tipo}(\alpha)$  per cui  $10 = (x, x', x'')$~~  con  $\text{Tipo}(5, 3, 2) = 30$

2.c  $n \in \mathbb{Z}_{18}$  sse  $n = k + 18t$   $\text{Tipo}(\sigma) = (2, 3)$   $P(\sigma) = 6$

$P(\sigma) | 18$  per cui per ogni  $n \in \mathbb{Z}_{18}$

$$f(n) = \sigma^{2n} \quad \text{ovvero } f \text{ è ben definita}$$

$$f([k] + [n]) = f([n]) \circ f([k]) \\ = \sigma^{2n} \cdot \sigma^{2k} \quad \text{SI}$$

$f$  non è suriettiva

$$\text{Kernel}(f) = \{n \in \mathbb{Z}_{18} \mid \bar{z}^n = 0\} \\ = \{\bar{0}, \bar{2}, \bar{4}\}$$

$$\text{Kernel} = \{\bar{0}, \bar{3}, \bar{6}, \bar{9}, \bar{12}, \bar{15}\}$$

$$\text{Im}(f) = \{\bar{0}, \bar{2}, \bar{4}\}$$

Esercizio 3.

- Scrivere il numero 15497 in base 8.
- Calcolare il resto della divisione di  $11^{95774}$  per 28.
- Dei seguenti gruppi additivi uno solo è ciclico. Dire quale ed esibirne 2 generatori esplicativi:

$$\mathbb{Z}_{10} \times \mathbb{Z}_{22}, \quad \mathbb{Z}_{15} \times \mathbb{Z}_{26}, \quad \mathbb{Z}_{18} \times \mathbb{Z}_{21}.$$

3.a)  $15497 = 1937 \cdot 8 + 1$   $15497 = [3621]_8$

$$1937 = 242 \cdot 8 + 1$$

$$242 = 30 \cdot 8 + 2$$

$$30 = 3 \cdot 8 + 6$$

$$3 = 0 \cdot 8 + 3$$

3.b)  $\varphi(28) = \varphi(2^2 \cdot 7) = 2 \cdot 6 = 12$

$$\text{MCD}(21, 28) = 1 \text{ ou}$$

$$28 = 21 \cdot 1 + 7$$

$$21 = 3 \cdot 7 + 0$$

$$7 = 1 \cdot 5 + 2$$

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

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

(6)

$$11^{95774} \equiv 12 \pmod{28}$$

$$11^{95774} \equiv 11 \cdot 11^2 \pmod{28}$$

$$12 \equiv 12 \pmod{28}$$

$$12 \equiv 12 \pmod{28}$$

$$\begin{array}{r} 11 \\ \overline{121} \\ 112 \\ \hline 9 \end{array}$$

(6)

3.c)

**Esercizio 1.** Un certo corso di studi universitario comporta il superamento di 15 esami. Di questi 15 esami, sette sono obbligatori. Degli altri otto, 4 o 5 vanno scelti in un gruppo A di 9 esami, mentre i rimanenti 3 o 4 vanno scelti in un gruppo B di 6 esami ( $B$  disgiunto da  $A$ , ossia  $A \cap B = \emptyset$ ).

- Quanti sono i piani di studio possibili per quel corso di studi?
- Alberto ha scelto 4 esami dal gruppo  $A$  e 4 dal gruppo  $B$ . In quanti modi può sostenere questi otto esami se quelli del gruppo  $A$  vanno sostenuti prima di quelli del gruppo  $B$ ?
- Elena aveva scelto un piano di studi con 5 esami del gruppo  $A$  e 3 del gruppo  $B$  e aveva già sostenuto 2 esami del gruppo  $A$ . Ora però vuole cambiare piano sostituendo 2 qualsiasi degli esami rimanenti del gruppo  $A$  con 1 (non già scelto) del gruppo  $A$  e uno (non già scelto) del gruppo  $B$ . Quanti modi ha di farlo?

$$\begin{array}{ll} |E|=15 & |A|=9 \\ |O|=7 & |B|=6 \\ Lf=15-7=8 & \end{array}$$

$$A \cap B = \emptyset$$

Scelta degli obbl.

(Q)

$$2.a) \binom{9}{4} \cdot \binom{6}{4} + \binom{9}{5} \cdot \binom{6}{3}$$

$\nearrow$   $\nearrow$   $\nearrow$   $\nearrow$   
 A con 4  
facoltativi A con 4  
facoltativi A con 3  
facoltativi B con 3  
facoltativi

2.b)

$$4! \cdot 4!$$

$$A \text{ rimanenti} = 9-2=7$$

(Q)

$$\binom{3}{2} = 3 \text{ modi}$$

$$|A_p|=52=3$$

Modi di scambiare elementi da A:  $9-5=4$

$$B: 6-3=3$$

$$R=3 \cdot 4 \cdot 3$$

**Esercizio 2.**

Si consideri il gruppo  $S_{10}$  delle permutazioni degli elementi dell'insieme  $\{1, 2, \dots, 10\}$  con l'operazione di composizione e la permutazione

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 6 & 5 & 9 & 4 & 10 & 1 & 7 & 3 & 8 & 2 \end{pmatrix}.$$

a) Determinare la decomposizione in cicli disgiunti di  $\sigma$  e stabilire se  $\sigma$  è una permutazione pari oppure dispari.

b) Calcolare  $\sigma^2$  e  $\sigma^{-1}$ .

c) Determinare tutti gli elementi del sottogruppo  $\langle \sigma \rangle = \{\sigma^k \mid k \in \mathbb{Z}\} \subset S_{10}$ .

d) Verificare che la funzione  $f : \langle \sigma \rangle \rightarrow (\mathbb{Z}_3, +)$  data da  $f(\sigma^k) = [k]_3$  è un omomorfismo di gruppi e determinare il nucleo di  $f$ .

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 6 & 5 & 9 & 4 & 10 & 1 & 7 & 3 & 8 & 2 \end{pmatrix} \xrightarrow{\sigma} \begin{pmatrix} 2 & 1 & 10 & 9 & 8 & 6 & 7 & 5 & 3 & 4 \end{pmatrix} \xrightarrow{\sigma^2} \begin{pmatrix} 3 & 2 & 8 & 10 & 7 & 1 & 9 & 5 & 6 & 4 \end{pmatrix} \xrightarrow{\sigma^3} \begin{pmatrix} 4 & 3 & 5 & 6 & 7 & 8 & 9 & 10 & 2 & 1 \end{pmatrix} \xrightarrow{\sigma^4} \begin{pmatrix} 5 & 4 & 6 & 7 & 8 & 9 & 10 & 1 & 3 & 2 \end{pmatrix} \xrightarrow{\sigma^5} \begin{pmatrix} 6 & 5 & 7 & 8 & 9 & 10 & 1 & 2 & 4 & 3 \end{pmatrix} \xrightarrow{\sigma^6} \begin{pmatrix} 7 & 6 & 8 & 9 & 10 & 1 & 2 & 3 & 5 & 4 \end{pmatrix} \xrightarrow{\sigma^7} \begin{pmatrix} 8 & 7 & 9 & 10 & 1 & 2 & 3 & 4 & 6 & 5 \end{pmatrix} \xrightarrow{\sigma^8} \begin{pmatrix} 9 & 8 & 10 & 1 & 2 & 3 & 4 & 5 & 7 & 6 \end{pmatrix} \xrightarrow{\sigma^9} \begin{pmatrix} 10 & 9 & 1 & 2 & 3 & 4 & 5 & 6 & 8 & 7 \end{pmatrix} \xrightarrow{\sigma^{10}} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \end{pmatrix}$$

$$\sigma = (1, 6)(2, 5, 10)(3, 9, 8)$$

$$\text{Tipo}(\sigma) = (2, 3, 3)$$

$$\text{Parity}(\sigma) = D+P+P = D+P = D$$

(Q)

$$\begin{array}{l} \sigma^2 = (2, 10, 5)(3, 8, 9) \\ \sigma^{-1} = (4, 6)(1, 2, 10, 5)(3, 8, 9) \end{array}$$

(Q)

$$P(\sigma) = \text{mcu}(\sigma) = 6$$

316

$$2.c) \langle \sigma \rangle = \{ \text{id}, \sigma, \sigma^2, \sigma^3, \sigma^4, \sigma^5 \}$$

$$\text{Ben def} \quad \langle \sigma \rangle = \sigma^k \quad \forall k \leq 2$$

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

$$f(\sigma^{k+k'}) = [k]_3 + [k']_3$$

$$[k+k']_3 = \frac{k+k'}{3}$$

$$f(\sigma^k) \rightarrow [k]_3 \quad \text{Per def. } P(\sigma)=6 \text{ quindi}$$

è computabile in  $\mathbb{Z}_3$

$$\text{Kernel}(f) = \{0, 3\}$$

(Q)

Esercizio 3.

Sia  $U = \mathbb{Z}_{10}^*$  il gruppo delle classi resto invertibili di  $\mathbb{Z}_{10}$ .

- Trovare due elementi non nulli in  $\mathbb{Z}_{10}$  il cui prodotto è nullo.
- Provare che  $a = [3^{303}]_{10}$  appartiene a  $U$  e che  $U$  coincide col gruppo ciclico  $\langle a \rangle$ .
- Risolvere la congruenza  $6x \equiv 8 \pmod{20}$ .

On

3.a)  $n \in \mathbb{Z}_{10}$  sse  $n = x + 10t$  quindi  $R = \{ \overline{2}, \overline{5} \}$

$$\overline{0} = x + 10t \cdot y + 10t$$

$$0+10t = \frac{x+10t \cdot y + 10t}{10t} \rightarrow 10t = x \cdot y \quad \text{Ora le due moltiplicati tra loro sono multipli}$$

3.b) Definendo  $U$  come l'insieme delle classi di resto modulo 10:

$$- [3^{303}]_{10} \quad (\text{ultima cifra}) \quad \ell(10) = \ell(2 \cdot 5) = 1 \cdot 4 = 4$$

$$\text{MCD}(3, 10) = 1$$

$$10 = 3 \cdot 3 + \underline{1} \\ 3 = 3 \cdot 1 + 0$$

$$303 = 76 \cdot 4 + 1$$

$$3^{303} = \cancel{3}^{36} \cdot 3 \rightarrow 3 \pmod{10} = 3 \quad \text{appartiene a } U$$

$$\langle a \rangle = \{ \overline{0}, \overline{3}, \overline{6}, \overline{9}, \dots \}$$

3.c)  $\text{MCD}(20, 6) = 2 \rightarrow 6$  non è invertibile in mod 20

2 è divisore di 8 per cui si può scrivere:  $20 = 3 \cdot 6 + 2$

$$6x \equiv 8 \pmod{20} \rightarrow \frac{6x}{2} + \frac{y \cdot 20}{2} = \frac{8}{2} \\ 3x + 10y = 4 \rightarrow 3x \equiv 4 \pmod{10}$$

$$\text{MCD}(3, 10) = 1 \quad \text{Bézout: } 1 = 10 - 3 \cdot 3 \quad 10 = 3 \cdot 3 + \underline{1} \\ 3 = 3 \cdot 1 + 0$$

$$\overline{1} = \overline{10 - 3 \cdot 3} \quad \text{in } \mathbb{Z}_{10} \quad \overline{10} = \overline{0} \rightarrow \overline{1} = \overline{-3 \cdot 3}$$

$$3x \equiv 4 \pmod{10} \rightarrow \overline{3} \cdot \overline{-3x} \equiv \overline{4} \cdot \overline{-3} \pmod{10}$$

$$x \equiv -12 \pmod{10}$$

$$x \equiv 8 \pmod{10}$$

$$\therefore -12, -2, 8, 18, 28$$

$$R_{10} = \{ \overline{8}, \overline{18} \}$$

On

