Traccia del 6 giugno 2023

1.

(a) L'intersezione cercata è un gruppo ciclico. Detto α un suo generatore, esisteranno due interi s e t tali che $\alpha = \sigma^s = \tau^t$. Si noti che $o(\sigma) = \mathrm{MCD}(6,5,4) = 60$, mentre $o(\tau) = \mathrm{MCD}(6,5,2) = 30$. Poiché $o(\sigma^s)$ deve dividere 30, si avrà che $s = 2h$, per qualche intero h. Ora, l'orbita di 14 sotto l'azione di σ^{2h} è $\{14,\ 16,\ 18\}$ se 3 non divide h, altrimenti è $\{14\}$. Ne consegue che $t = 2k$ per qualche intero k. Ma τ^{2k} lascia fisso 1, mentre l'orbita di 1 sotto l'azione di σ^2 è $\{1,3\}$. Ne consegue che $h = 2u$ per qualche intero u, così che $s = 4u$. In conclusione, l'intersezione cercata è contenuta nel sottogruppo ciclico generato da

$$\sigma^4 = (9,13,12,11,10)(14,18,16)(15,19,17).$$

D'altra parte,

$$\tau^2 = (9,11,13,10,12)(14,18,16)(15,19,17).$$

e quindi $\tau^{2v} = \sigma^4$ per un intero v tale che $v \equiv 2 \pmod 5$ e $v \equiv 1 \pmod 3$. Per il Teorema Cinese del Resto, un intero siffatto esiste (ad esempio, $v = 7$). Ciò prova che

$$\langle \alpha \rangle \subset \langle \sigma^4 \rangle = \langle \tau^{14} \rangle \subset \langle \sigma \rangle \cap \langle \tau \rangle.$$

L'intersezione cercata è dunque $\langle \alpha \rangle = \langle \sigma^4 \rangle = \langle \tau^{14} \rangle = \langle \tau^2 \rangle$.

(b) Si osservi che:

- il ciclo $\gamma_1 = (1,5,2,6,3,7,4,8)$ commuta con σ e τ, in quanto

$$\gamma_1^2 = (1,2,3,4)(5,6,7,8) \quad \text{e} \quad \gamma_1^4 = (1,3)(2,4)(5,7)(6,8);$$

- il ciclo $\gamma_2 = (9,10,11,12,13)$ è associato ad entrambi σ e τ;
- la permutazione $\gamma_3 = (14,16,18)(15,17,19)$ commuta con σ e τ, in quanto è una potenza di un ciclo associato a σ e di un ciclo associato a τ :

$$\gamma_3 = (14,15,16,17,18,19)^2 = (14,19,18,17,16,15)^4.$$

Ne consegue che il seguente sottogruppo di S_{19} è contenuto in $C(\sigma) \cap C(\tau)$:

$$H = \{\gamma_1^a \gamma_2^b \gamma_3^c | a,b,c \in \mathbb{Z}\}.$$

Si ha, inoltre, $|H| = o(\gamma_1)o(\gamma_2)o(\gamma_3) = 8 \cdot 5 \cdot 3 = 120$, come richiesto.

2.

(a) Il numero $N = n^3 - 5n^2 - 8n + 12 = (n-1)(n+2)(n-6)$ è divisibile per $125 = 25^3$ se e solo se il primo 5 compare complessivamente almeno 3 volte nelle decomposizioni dei tre fattori indicati. Ora:

- se 5 divide $n+2$, non divide nessuno degli altri due fattori; quindi, in questo caso si avrà la proprietà voluta se e solo se $n+2$ è divisibile per 125.
- 5 divide $n-1$ se e solo se divide $n-6$, ed allora non divide $n+2$; quindi, in questo caso si avrà la proprietà voluta se e solo se uno tra $n-1$ e $n-6$ è divisibile per 25.

Pertanto $125|N$ se e solo se

- $n \equiv -2 \pmod{125}$

oppure

- $n \equiv 1 \pmod{25}$

oppure

- $n \equiv 6 \pmod{25}$

In conclusione, l'insieme cercato è

$$\{123 + 125k | k \in \mathbb{Z}\} \cup \{1 + 25k | k \in \mathbb{Z}\} \cup \{6 + 25k | k \in \mathbb{Z}\}.$$

(b) Il numero $M = n^3 - 9n^2 + 20n - 12 = (n-1)(n-2)(n-6)$ è divisibile per $90 = 2 \cdot 3^2 \cdot 5$ se e solo se sono verificate le seguenti tre condizioni:

- M è divisibile per 2, e ciò è sempre vero, poiché uno tra $n-1$ e $n-2$ è pari;
- M è divisibile per 9; ora, poiché i numeri $n-1$, $n-2$ e $n-6$ sono a due a due non congrui modulo 3, esattamente uno di essi è divisibile per 3, e dunque la condizione voluta si verifica se e solo se uno dei tre numeri è divisibile per 9;
- M è divisibile per 5, e ciò vale se e solo se uno tra $n-1$ e $n-2$ è divisibile per 5 (il primo caso equivale alla divisibilità per 5 di $n-6$)

Pertanto $90|M$ se e solo se vale una delle seguenti condizioni:

I)

- $n \equiv 1 \pmod{9}$

oppure

- $n \equiv 2 \pmod{9}$

oppure

- $n \equiv 6 \pmod{9}$

insieme ad una delle seguenti:

II)

- $n \equiv 1 \pmod{5}$

oppure

- $n \equiv 2 \pmod{5}$

Combinando in tutti i modi possibili una delle condizioni in I) con una delle condizioni in II) ed applicando il Teorema Cinese del Resto, si conclude che l'insieme cercato è

$$\{n_0 + 45k |\ n_0 \in \{1, 2, 6, 11, 37, 42\},\ k \in \mathbb{Z}\}.$$

(c) Si noti anzitutto che $\alpha^{15} - 3\alpha^{10} + 3\alpha^5 - \overline{1} = \left(\alpha^5 - \overline{1}\right)^3$.

Quindi si osservi che $\varphi(\overline{1}) = \overline{0}$ appartiene all'immagine di φ. Sia ora γ un generatore del gruppo moltiplicativo $\mathbb{Z}_{257}^*$, che è ciclico (si ricordi che 257 è primo). Questo gruppo ha ordine $256 = 2^8$. Supponiamo che n sia un intero dispari. Poiché allora n è coprimo con $o(\gamma)$, ne consegue che anche γ^n è un generatore del gruppo. Dunque, per ogni $\delta \in \mathbb{Z}_{257}^*$, esiste $k \in \mathbb{Z}$ tale che $\delta = \left(\gamma^n\right)^k = \left(\gamma^k\right)^n$. Quanto precede prova che l'applicazione da $\mathbb{Z}_{257}$ a $\mathbb{Z}_{257}$ che invia ogni elemento nella sua potenza n-esima è surgettiva. Ciò si applica, in particolare, a $n = 3$ e a $n = 5$.

Dunque φ è surgettiva in quanto composta di due applicazioni surgettive.

3.
Osserviamo anzitutto che

$$f(x) = x^{p^2}\left(x^{p-1} - \overline{1}\right)^{p^2} + x - \overline{1},$$

ove il polinomio $x^{p-1} - \overline{1}$ è divisibile per ogni fattore lineare del tipo $x - \alpha$ con $\alpha \neq \overline{0}$. In particolare, è divisibile per $x - \overline{1}$ e per $x + \overline{2}$. Ne consegue che $\left(x^{p-1} - \overline{1}\right)^{p^2}$ è divisibile per entrambi i polinomi $(x - \overline{1})^p = g(x)$ e $(x + \overline{2})^{p^2} = x^{p^2} + \overline{2}^{p^2} = h(x)$. Per l'ultima uguaglianza si è applicato il Piccolo Teorema di Fermat. In conclusione, per i quesiti (a) e (b) la risposta è la stessa: il resto è $x - \overline{1}$.