Traccia del 9 gennaio 2023

1.

(a) L'intersezione cercata è un gruppo ciclico. Detto α un suo generatore, esisteranno due interi s e t tali che $\alpha = \sigma^s = \tau^t$. Siano $h,\ k$ interi. L'orbita di 4 sotto l'azione di τ^k è uguale a $\{4,7\}$ se k è dispari, altrimenti è banale. L'orbita di 4 sotto l'azione di σ^h è uguale a $\{4,7\}$ se e solo se $h \equiv 3 \pmod 6$, ed è banale se e solo se $h \equiv 0 \ (mod\ 6)$. Dunque può coincidere con l'orbita di 4 sotto l'azione di τ^k solo se $3|k$. Pertanto $s = 3u$ per qualche intero u. Ma allora σ^s lascia fisso 1, e dunque lo stesso dovrà valere per τ^t, ossia dovrà essere $t = 3v$ per qualche intero v. Dunque il sottogruppo cercato è uguale a $\langle\sigma^3\rangle \cap \langle\tau^3\rangle$, ove

$$\sigma^3 = (4,7)(5,8)(6,9)(10,13,16,12,15,11,14)(17,20,19,18)$$
$$\tau^3 = (4,7)(5,8)(6,9)(10,16,15,14,13,12,11)(17,19)(18,20)$$

Il confronto tra le orbite di 17 sotto l'azione di σ^{3v} e di τ^{3u} consente di dedurre che $v = 2a$ per qualche intero a. Quindi il sottogruppo cercato è $\langle\sigma^6\rangle \cap \langle\tau^3\rangle$, ove

$$\sigma^6 = (10,16,15,14,13,12,11)(17,19)(18,20).$$

Ne consegue che ogni elemento del sottogruppo lascia fisso 4. Ciò vale, in particolare, per τ^{3u}, così che $u = 2b$ per qualche intero b. Ma τ^{6b} lascia fisso 17, dunque lo stesso deve valere per σ^{6a}. Pertanto a è pari, così che il sottogruppo cercato è $\langle\sigma^{12}\rangle \cap \langle\tau^6\rangle$, ove

$$\sigma^{12} = \tau^6 = (10,15,13,11,16,14,12)$$

Il sottogruppo cercato è dunque quello generato da $\alpha = \sigma^{12} = \tau^6$, avente ordine 7.

(b) Con σ e τ commutano il 6-ciclo $\delta = (4,5,6,7,8,9)$ e il 4-ciclo $\varepsilon = (17,20,19,18)$, dato che $\delta^3 = (4,7)(5,8)(6,9)$ e $\varepsilon^2 = (17,19)(18,20)$. Quindi un sottogruppo del tipo cercato è $H = \{\delta^a\varepsilon^b | a,b \in \mathbb{Z}\}$, avente ordine $o(\delta)o(\varepsilon) = 6 \cdot 4 = 24$.

(c) Per realizzare una costruzione analoga a quella effettuata al punto (b) basterà trovare due permutazioni disgiunte, entrambe di periodo 3, che commutino con σ e τ. Ciò è vero per $\mu = (1,2,3)$ e $\nu = (4,6,8)(5,7,9) = \delta^2$.

2.

(a) Due omomorfismi di gruppi non banali sono quelli definiti da

$$([a]_4,[b]_5) \mapsto [5a]_{10} \quad \text{e} \quad ([a]_4,[b]_5) \mapsto [2b]_{10} \qquad \text{per ogni } a,b \in \mathbb{Z}.$$

Le verifiche della buona definizione e della conservazione della somma sono pressoché immediate.

(b) Si osserva che, essendo 4 e 5 coprimi, in base alla dimostrazione del Teorema cinese del resto (seconda formulazione), ogni elemento di $\mathbb{Z}_4 \times \mathbb{Z}_5$ può essere espresso nella forma $([a]_4,[a]_5)$, con $a \in \mathbb{Z}$. Quindi si definisce l'applicazione $\varphi : \mathbb{Z}_4 \times \mathbb{Z}_5 \mapsto \mathbb{Z}_{10}$ tale che, per ogni $a \in \mathbb{Z}, \varphi([a]_4,[a]_5) = [a]_{10}$. Questa è ben definita, conserva somma e prodotto ed è evidentemente suriettiva.

(c) L'applicazione φ è ben definita se e solo se

$$\text{per ogni } a, a', b, b' \in \mathbb{Z}, \qquad 4|a-a' \text{ e } 5|b-b' \implies 10|m(a-a')+n(b-b'),$$

ossia, se e solo se, per ogni $h, k \in \mathbb{Z}$, $10|4mh+5nk$. (*) Poiché questa relazione deve valere in particolare quando $\{h,k\}=\{0,1\}$, si ricavano le seguenti due condizioni necessarie su m ed n : $10|4m$ e $10|5n$, equivalenti a $5|m$ e $2|n$. Ma queste sono anche condizioni sufficienti a garantire (*). Dunque le coppie cercate sono tutte e sole quelle della forma $(5s, 2t)$, con $s, t \in \mathbb{Z}$. Ora, $\mathrm{Im}\varphi = \{[5sa+2tb]_{10} | a, b \in \mathbb{Z}\}$, e, per il Lemma di Bézout, questo insieme è $\mathbb{Z}_{10}$ se i numeri $5s$ e $2t$ sono coprimi. Ciò avviene, per esempio, per la coppia $(5, 2)$.

3.
Si ha

$$f(x) = (x+\overline{1})\left(x^{p-1}-\overline{1}\right) = (x+\overline{1})\prod_{\alpha\in\mathbb{Z}_p^*}(x-\alpha) = (x+\overline{1})^2(x-\overline{1})\prod_{\alpha\in\mathbb{Z}_p^*\setminus\{\overline{1},-\overline{1}\}}(x-\alpha)$$

$$g(x) = x(x-\overline{1})^2(x+\overline{1})$$

Dal confronto tra le due fattorizzazioni si ricava $\mathrm{MCD}(f(x), g(x)) = (x+\overline{1})(x-\overline{1}) = x^2-\overline{1}$.