Traccia del 29 giugno 2026

1.

(a) Sia $\alpha = \sigma^s = \tau^t$ un generatore del gruppo ciclico $\langle\sigma\rangle \cap \langle\tau\rangle$. Dal confronto tra le orbite di 5 sotto l'azione delle potenze di σ e di τ si deduce che $4|s$ e $2|t$. Quindi $s = 4h$, $t = 2k$, per opportuni interi h, k e il sottogruppo cercato è $\langle\sigma^4\rangle \cap \langle\tau^2\rangle$, dove

$\sigma^4 = (13, 17, 16, 15, 14)(19, 23, 22, 20, 18, 24, 21)$
$\tau^2 = (9, 11)(10, 12)(16, 14, 17, 15, 13)(18, 20, 22, 23, 19, 21, 24).$

Poiché τ^{2k} deve lasciare fisso 9, si deduce ancora che $2|k$. Quindi il sottogruppo cercato è $\langle\sigma^4\rangle \cap \langle\tau^4\rangle$, dove

$\tau^4 = (16, 17, 13, 14, 15)(18, 22, 19, 24, 20, 23, 21).$

Si può notare che

$(16, 17, 13, 14, 15)^4 = (13, 17, 16, 15, 14),$
$(18, 22, 19, 24, 20, 23, 21)^3 = (19, 23, 22, 20, 18, 24, 21).$

Si avrà allora che $\tau^{4\ell} = \sigma^4$ per ogni intero ℓ tale che

$\ell \equiv 4 \pmod 5$
$\ell \equiv 3 \pmod 7.$

Ciò è vero per $\ell = 24$. Dunque $\tau^{96} = \sigma^4$. Ne consegue che $\sigma^4 \in \langle\tau^4\rangle$. Il sottogruppo cercato è $\langle\sigma^4\rangle = \langle\tau^4\rangle$, di ordine 35.

(b) Con σ e con τ commutano le permutazioni $\alpha = (1, 3)(2, 4)$ e $\beta = (5, 6)(7, 8)$, che sono dunque due distinti elementi di periodo 2 in $C(\sigma) \cap C(\tau)$. Ciò esclude che $C(\sigma) \cap C(\tau)$ sia ciclico.

2.

(a) Se esiste un epimorfismo di anelli $\varphi : \mathbb{Z}_{44} \times \mathbb{Z}_{51} \to \mathbb{Z}_6 \times \mathbb{Z}_{11}$, allora $\varphi([1]_{44}, [1]_{51}) = ([1]_6, [1]_{11})$. Poiché φ deve conservare i multipli, si avrà allora, per ogni $a \in \mathbb{Z}$, $\varphi([a]_{44}, [a]_{51}) = ([a]_6, [a]_{11})$. Questa applicazione è ben definita, in quanto, per ogni $a, a' \in \mathbb{Z}$ tali che $44|a - a'$ e $51|a - a'$, si ha naturalmente che 2, 3 e 11 dividono $a - a'$. Inoltre è immediato verificare che φ conserva somma e prodotto. Per la suriettività basta osservare che $\mathrm{Im}\varphi = \langle([1]_6, [1]_{11})\rangle = \mathbb{Z}_6 \times \mathbb{Z}_{11}$.

(b) Se esiste un monomorfismo di gruppi $\psi : \mathbb{Z}_{19} \times \mathbb{Z}_{20} \to \mathbb{Z}_{40} \times \mathbb{Z}_{95}$, questo invierà il generatore $([1]_{19}, [1]_{20})$ in un elemento del gruppo di arrivo avente periodo $19 \cdot 20 = 380$. Un elemento siffatto è $([10]_{40}, [1]_{95})$. Il monomorfismo cercato è dunque definito ponendo, per ogni $a \in \mathbb{Z}$, $\psi([a]_{19}, [a]_{20}) = ([10a]_{40}, [a]_{95})$.

3.

(a) Si ha $f(x) = \left(x^{p-1} + x^2\right)^{p^2} + \left(x^{p-1} + x^2\right)^{p} + \left(x^{p-1} + x^2\right)^{2} + \overline{1}$. Quindi $\overline{1}$ è il resto cercato, mentre il quoziente è il polinomio $\left(x^{p-1} + x^2\right)^{p^2-1} + \left(x^{p-1} + x^2\right)^{p-1} + x^{p-1} + x^2$.

(b) Osserviamo preliminarmente che, per ogni $\alpha \in \mathbb{Z}_p$, si ha $(\alpha - \overline{1})h(\alpha) = \alpha^3 - \overline{1}$. Quindi se α è radice di $h(x)$, allora $\alpha^3 = \overline{1}$ (*). Ora, poiché $\alpha \neq \overline{0}$, applicando i Teoremi di Eulero e di Fermat si ha:

$$f(\alpha) = \overline{1} + \alpha^2 + \overline{1} + \overline{2}\alpha^2 + \alpha^2 + \overline{1} + \alpha^4 + \overline{1} = \alpha^4 + \overline{4}\alpha^2 + \overline{4}.$$

Se α è anche radice di $f(x)$, avremo allora $\overline{0} = f(\alpha) - \overline{4}h(\alpha) = \alpha^4 - \overline{4}\alpha = \alpha\left(\alpha^3 - \overline{4}\right)$, da cui $\alpha^3 = \overline{4}$. Tenendo conto di (*), se ne deduce che $\overline{1} = \overline{4}$, e quindi $p = 3$. In questo caso $\alpha = \overline{1}$ è la sola radice di $h(x)$, e il precedente calcolo mostra che è anche radice di $f(x)$. Negli altri casi non vi sono radici comuni.

(c) Sia $p = 1009$. Ricordiamo che $(\alpha - \overline{1})h(\alpha) = \alpha^3 - \overline{1}$. Poiché $p \equiv 1 \pmod 3$, le radici di $h(x)$ sono dunque i due elementi di $\mathbb{Z}_{1009}^*$ aventi periodo 3, siano essi α_1 e α_2. Pertanto $h(x) = (x - \alpha_1)(x - \alpha_2)$. Ma nessuno dei due fattori lineari di $h(x)$ divide $g(x)$. Altrimenti si avrebbe, per $i = 1$ oppure $i = 2$, $\overline{0} = g(\alpha_i) = \overline{1} + \alpha_i^2$, da cui $\alpha_i^2 = -\overline{1}$. Ma, d'altra parte, $\alpha_i^2 = \alpha_i^{-1}$. Se ne dedurrebbe, quindi, che $\alpha_i = -\overline{1}$, impossibile. Pertanto $g(x)$ e $h(x)$ non hanno alcun fattore irriducibile in comune, ossia $MCD(g(x), h(x)) = \overline{1}$.