Traccia del 5 giugno 2025

1.

(a) Sia $\alpha = \sigma^s = \tau^t$ un generatore del sottogruppo cercato, che è certamente ciclico. Dal confronto tra le orbite di 1 sotto l'azione delle potenze di σ e di τ si deduce che $3|s$ e che $4|t$. Inoltre, i sottogruppi ciclici generati dal 7-ciclo γ_1 di σ e dal 7-ciclo γ_2 di τ sono disgiunti, in quanto γ_1 e γ_2, che sono distinti, sono, rispettivamente nel primo e nel secondo sottogruppo, gli unici elementi ad inviare 13 in 14. Ne consegue che l'unica potenza comune di γ_1 e di γ_2 è la permutazione identica. Ciò comporta due ulteriori condizioni di divisibilità: $7|s$ e $7|t$. In conclusione, si deve avere che $21|s$ e che $28|t$. Il sottogruppo cercato è dunque $\langle \sigma^{21} \rangle \cap \langle \tau^{28} \rangle$, dove

$\sigma^{21} = (20, 23, 26)(21, 24, 27)(22, 25, 28),$
$\tau^{28} = (20, 26, 23)(21, 27, 24)(22, 28, 25).$

Poiché queste due permutazioni sono una l'inversa dell'altra, generano lo stesso sottogruppo di ordine 3, che è dunque l'intersezione cercata.

(b) Al sottogruppo $C(\sigma) \cap C(\tau)$ appartiene il 12-ciclo $\beta = (1, 5, 9, 2, 6, 10, 3, 7, 11, 4, 8, 12)$, in quanto

$\beta^4 = (1, 6, 11)(5, 10, 4)(9, 3, 8)(2, 7, 12)$, che è prodotto di cicli di σ, e
$\beta^3 = (1, 2, 3, 4)(5, 6, 7, 8)(9, 10, 11, 12)$, che è prodotto di cicli di τ.

Ne consegue che un sottogruppo del tipo cercato è $H = \langle \beta \rangle$.

2.

(a) Un omomorfismo di anelli $\varphi : \mathbb{Z}_6 \times \mathbb{Z}_{12} \to \mathbb{Z}_8 \times \mathbb{Z}_9$ invia l'elemento uno dell'anello di partenza nell'elemento uno dell'anello immagine, che in particolare, è un elemento idempotente rispetto al prodotto. Siano dunque $a, b \in \mathbb{Z}$ tali che $\varphi([1]_6, [1]_{12}) = ([a]_8, [b]_9)$. Ora, $o([1]_6, [1]_{12}) = 12$. Poiché φ è, in particolare, un omomorfismo di gruppi additivi, e, in quanto tale, conserva i multipli e l'elemento zero, ne consegue che $12([a]_8, [b]_9) = ([0]_8, [0]_9)$, ossia $o([a]_8, [b]_9))$ divide 12. Dato che, per il Teorema di Lagrange, $o([a]_8)|8$ e $o([b]_9)|9$, ciò implica che $o([a]_8)|4$ e $o([b]_9)|3$, e dunque $a = 2h$, $b = 3k$, per opportuni interi h e k. A questo punto ricordiamo che l'elemento sino a qui considerato, ovvero $([2h]_8, [3k]_9)$, è idempotente. Ciò significa che $8|2h(2h-1)$ e $9|3k(3k-1)$. Questa coppia di condizioni equivale alla seguente: $4|h$ e $3|k$. Ma allora $([a]_8, [b]_9) = ([0]_8, [0]_9)$, da cui si deduce subito che l'anello immagine è banale, ossia φ è l'omomorfismo nullo. Esiste dunque un solo omomorfismo di anelli da $\mathbb{Z}_6 \times \mathbb{Z}_{12}$ a $\mathbb{Z}_8 \times \mathbb{Z}_9$.

(b) Per la seconda formulazione del Teorema cinese del resto, il gruppo $\mathbb{Z}_8 \times \mathbb{Z}_9$ è ciclico ed ha come generatore $([1]_8, [1]_9)$. Se $\varphi : \mathbb{Z}_8 \times \mathbb{Z}_9 \to \mathbb{Z}_6 \times \mathbb{Z}_{12}$ è un omomorfismo di gruppi tale che $\varphi([1]_8, [1]_9) = (\alpha, \beta)$, allora questa assegnazione lo determina univocamente, in quanto, stante la conservazione dei multipli, per ogni $n \in \mathbb{Z}$ si avrà che $\varphi([n]_8, [n]_9) = (n\alpha, n\beta)$. Si può osservare che questa uguaglianza fornisce, per ogni scelta di (α, β), una buona definizione dell'applicazione φ. Infatti, dati $n, m \in \mathbb{Z}$ tali che $([n]_8, [n]_9) = ([m]_8, [m]_9)$, si ha che $8 \cdot 9 | n - m$. In particolare, $12|n-m$. Poiché, per il Teorema di Lagrange, 12 è multiplo sia di $o(\alpha)$, sia di $o(\beta)$, e quindi lo è a maggior ragione $n - m$, per la caratterizzazione del periodo avremo quindi

$$n\alpha - m\alpha = (n-m)\alpha = 0 = (n-m)\beta = n\beta - m\beta,$$

ossia $\varphi([n]_8, [n]_9) = (n\alpha, n\beta) = (m\alpha, m\beta) = \varphi([m]_8, [m]_9)$. Ciò prova la buona definizione di φ.

D'altra parte, un'applicazione così definita è sempre un omomorfismo di gruppi, com'è immediato verificare. In conclusione, il numero degli omomorfismi di gruppi da $\mathbb{Z}_8 \times \mathbb{Z}_9$ a $\mathbb{Z}_6 \times \mathbb{Z}_{12}$ è pari al numero degli elementi di $\mathbb{Z}_6 \times \mathbb{Z}_{12}$, ossia $6 \cdot 12 = 72$.

(c) Si ricordi che un gruppo ciclico finito ha, per ogni divisore positivo del suo ordine, esattamente un sottogruppo avente come ordine quel divisore. Ora, per la seconda formulazione del Teorema cinese del resto, $\mathbb{Z}_{p^n} \times \mathbb{Z}_{q^m}$ è un gruppo ciclico di ordine $p^n \cdot q^m$. Dunque il numero dei suoi sottogruppi è pari al numero dei divisori di $p^n \cdot q^m$. Questi divisori sono tutti e soli i prodotti della forma $p^s q^t$, con s, t interi tali che

$0 \leq s \leq n,\ 0 \leq t \leq m$. Il loro numero è dunque $(n+1)\cdot(m+1)$.

3.

(a) Poiché $g(x) = f(x)^{p^3} - f(x)^p + \overline{2}f(x) - x^p - \overline{2}x + \overline{1}$, il quoziente è $f(x)^{p^3-1} - f(x)^{p-1} + \overline{2}$, mentre il resto è $-x^p - \overline{2}x + \overline{1}$.

(b) Si ha $h(x)^{p^2} = g(x) + \left(x^2 - \overline{1}\right)^{p^2}$. Pertanto, posto $d(x) = \mathrm{MCD}(g(x),\ h(x))$, si ha che $d(x)$ divide $\left(x^2 - \overline{1}\right)^{p^2}$. I fattori irriducibili di quest'iltimo polinomio sono $x - \overline{1}$ e $x + \overline{1}$. Nessuno di questi, tuttavia, divide $g(x)$, in quanto nessuno tra $\overline{1}$ e $-\overline{1}$ è radice di $g(x)$ nell'ipotesi che sia $p > 2$. Ne consegue che nessuno fra $x - \overline{1}$ e $x + \overline{1}$ divide $d(x)$, e da ciò si conclude che $d(x) = \overline{1}$.