Traccia del 21 settembre 2022

1.

(a) Si consideri il seguente sottogruppo di S_{18} :

$$H = \{(1,2,3)^a(13,15,17)^b(14,16,18)^c | a,b,c \in \mathbb{Z}\}.$$

Si ha $|H| = 3^3 = 27$. Inoltre

$$\sigma^{20} = (1,3,2)(13,15,17)(14,16,18) = (1,2,3)^2(13,15,17)(14,16,18) \in H.$$

Ciò prova che $H \cap \langle\sigma\rangle \neq \{id\}$.

(b) Si consideri che $|K| = 4 \cdot 6 = 24$, mentre $|\langle\sigma\rangle| = o(\sigma) = \mathrm{mcm}(6,5,4,3) = 60$. Pertanto, per Lagrange, $|K \cap \langle\sigma\rangle|$ è un divisore di $\mathrm{MCD}(24,60) = 12$. Si osservi inoltre che $K \cap \langle\sigma\rangle$ è ciclico, in quanto sottogruppo di un gruppo ciclico. Sia α un suo generatore. Allora, poiché ogni elemento di K lascia fissi 1 e 8, lo stesso dovrà avvenire per α. Sarà dunque $\alpha = \sigma^s$, con $s = 15k$ (per qualche $k \in \mathbb{Z}$). Quindi $K \cap \langle\sigma\rangle = K \cap \langle\sigma^{15}\rangle$, ove

$$\sigma^{15} = (4,7,6,5)(13,16)(14,17)(15,18).$$

D'altra parte $\sigma^{15} = (4,5,6,7)^3(13,14,15,16,17,18)^3 \in K$.
In conclusione, $K \cap \langle\sigma\rangle = \langle\sigma^{15}\rangle$, gruppo di ordine 4.

2.

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

per ogni $a, a', b, b' \in \mathbb{Z}$,
$n|a-a'$ e $n|b-b'$ (*) $\Longrightarrow n^2|nab - na'b' = n(ab - ab' + ab' - a'b') = n(a(b-b') + b'(a-a'))$.

Ma quest'ultima relazione di divisibilità equivale alla condizione $n|(a(b-b') + b'(a-a')$, che è sempre verificata se vale la premessa (*). Ciò prova che φ è sempre ben definita.

(b) Siano $a, b \in \mathbb{Z}$. Allora

$$\varphi([a]_n, [b]_n) = [n]_{n^2} \text{ se e solo se } nab \equiv n \pmod{n^2},$$

ossia se e solo se $n|ab-1$, ossia se e solo se $[a]_n[b]_n = [1]_n$, ossia se e solo se $[a]_n$ è invertibile nell'anello $\mathbb{Z}_n$ e $[b]_n$ è il suo inverso. Ne consegue che le coppie $([a]_n, [b]_n)$ appartenenti a $\varphi^{-1}([n]_{n^2})$ sono tante quanti gli elementi di $\mathcal{U}(\mathbb{Z}_n)$, ossia il loro numero è $\phi(n)$, essendo ϕ la funzione toziente di Eulero.

3.

(a) Si ha

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

Quindi $\alpha \in \mathbb{Z}_p$ è radice comune di f e g solo se $\alpha \neq \overline{0}$ e

$$\alpha^2 + \alpha + \overline{1} = \alpha^p + \alpha + \overline{1} = \overline{0}, \quad \text{ossia} \quad \alpha^2 = \alpha^p = -\alpha - \overline{1}.$$

In virtù del Piccolo Teorema di Fermat, si ha $\alpha^p = \alpha$. Quindi la penultima uguaglianza stablisce che $\alpha^2 = \alpha$, cioè $\alpha(\alpha - \overline{1}) = \overline{0}$, da cui $\alpha = \overline{1}$. Ma questa è radice di $f(x)$ e $g(x)$ se e solo se $p = 3$. In tutti gli altri casi non vi sono radici comuni.

(b) Se $\alpha \in \mathbb{Z}_p$ è radice di g, allora $\alpha \neq \overline{0}$ e inoltre, per il Piccolo Teorema di Fermat,

$$\overline{0} = \alpha^p + \alpha + \overline{1} = 2\alpha + \overline{1}.$$

Sia $\alpha \in \mathbb{Z}_p^*$. Poiché $h(\alpha) = \alpha^{p+2}\left(\alpha^{p^2-p-2} + x^{p-2} + \overline{1}\right)$, α è anche radice di h se e solo se

$$\overline{0} = \alpha^{p^2-p-2} + \alpha^{p-2} + \overline{1},$$

equivalentemente, per lo stesso teorema, se e solo se

$$\overline{0} = \alpha^{-2} + \alpha^{-1} + \overline{1}, \text{ se e solo se } \overline{0} = \alpha^2(\alpha^{-2} + \alpha^{-1} + \overline{1}), \text{ ossia } \overline{0} = \overline{1} + \alpha + \alpha^2.$$

Quindi, se α è radice comune di g e h, allora $2\alpha + \overline{1} = \overline{1} + \alpha + \alpha^2$, ossia $\alpha = \alpha^2$ e dunque, essendo $\alpha \neq \overline{0}$, si ha $\alpha = \overline{1}$. Ma questa è una radice di g e h se e solo se $p = 3$.

(c) I calcoli precedenti mostrano che f e h hanno le stesse radici, ossia $\overline{0}$ insieme a tutti e soli gli $\alpha \in \mathbb{Z}_p$ tali che

$$\overline{1} + \alpha + \alpha^2 = \overline{0}.$$

Quindi le radici sono esattamente due se e solo se esiste un solo α siffatto, ossia se e solo se il polinomio $x^2 + x + \overline{1} \in \mathbb{Z}_p[x]$ ha una radice doppia α, ossia esiste $\alpha \in \mathbb{Z}_p$ tale che si abbia $x^2 + x + \overline{1} = (x - \alpha)^2$, ossia tale che

$$\alpha^2 = \overline{1} \quad \text{e} \quad 2\alpha = -\overline{1}.$$

Queste due uguaglianze sono verificate solo da $\alpha = \overline{1}$ per $p = 3$. Quindi f e h hanno esattamente due radici comuni se e solo se $p = 3$.