Traccia del 3 luglio 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 $o(\sigma) = o(\tau) = \mathrm{MCD}(7,5,4,2) = 4 \cdot 5 \cdot 7 = 140$. L'unico sottogruppo (ciclico) di ordine 5 di $\langle\sigma\rangle$ è quello generato da $\sigma^{56} = (7,8,9,10,11)$, mentre l'unico sottogruppo ciclico di ordine 5 di $\langle\tau\rangle$ è generato da $\tau^{56} = (7,9,8,10,11)$. Questi due sottogruppi sono distinti, in quanto, nel primo, l'unico elemento che invia 7 in 8 è σ^{56}, mentre nel secondo questo ruolo spetta a un altro elemento, ossia $\tau^{112} = (7,8,11,9,10)$. Ne consegue che 5 non può dividere l'ordine di $\langle\alpha\rangle$. Dunque $\langle\alpha\rangle = \langle\sigma^5\rangle \cap \langle\tau^5\rangle$, ove

$$\sigma^5 = (1,2)(3,4)(5,6)(12,13,14,15)(16,21,19,17,22,20,18),$$
$$\tau^5 = (1,3)(2,4)(5,6)(12,14,13,15)(16,18,20,22,17,19,21).$$

Dal confronto tra le orbite di 1 sotto le azioni di σ^5 e τ^5 si deduce che $\langle\alpha\rangle = \langle\sigma^{10}\rangle \cap \langle\tau^{10}\rangle$, ove

$$\sigma^{10} = (12,14)(13,15)(16,19,22,18,21,17,20),$$
$$\tau^{10} = (12,13)(14,15)(16,20,17,21,18,22,19).$$

Dal confronto tra le orbite di 12 sotto le azioni di σ^{10} e τ^{10} si deduce infine che $\langle\alpha\rangle = \langle\sigma^{20}\rangle \cap \langle\tau^{20}\rangle$, ove

$$\sigma^{20} = (16,22,21,20,19,18,17),$$
$$\tau^{20} = (16,17,18,19,20,21,22).$$

Queste due permutazioni sono l'una l'inversa dell'altra, quindi generano lo stesso sottogruppo, che è, pertanto, l'intersezione cercata: $\langle\alpha\rangle = \langle\sigma^{20}\rangle = \langle\tau^{20}\rangle$.

(b) Si osservi che:

- le permutazioni $\alpha_0 = \mathrm{id}$, $\alpha_1 = (1,2)(3,4)$, $\alpha_2 = (1,3)(2,4)$ e $\alpha_3 = (1,4)(2,3)$ formano un sottogruppo commutativo V di S_{22}, in particolare commutano tra di loro e quindi commutano con σ e τ, a fronte della decomposizione in cicli disgiunti di queste ultime;
- il ciclo $\beta = (5,6)$ è associato ad entrambe σ e τ;
- il ciclo $\gamma = (16,17,18,19,20,21,22)$ commuta con σ e τ, in quanto è un ciclo associato a σ e, come abbiamo visto in (a), è anche una potenza di τ .

Ne consegue che il seguente sottogruppo di S_{22} è contenuto in $C(\sigma) \cap C(\tau)$:

$$H = \{\alpha_i \beta^b \gamma^c \mid i \in \{0,1,2,3\}, b, c \in \mathbb{Z}\}.$$

Si ha, inoltre, $|H| = 4o(\beta)o(\gamma) = 4 \cdot 2 \cdot 7 = 56$, come richiesto.

(c) A $C(\sigma) \cap C(\tau)$ appartengono due distinti elementi di periodo 2, ovvero $(1,2)(3,4)$ e $(5,6)$. Ciò esclude che sia un gruppo ciclico.

2.

(a) Si ha che $\mathrm{Im}\varphi = \langle [mn]_{m^2} \rangle \times \langle [mn]_{n^2} \rangle$. Ora:

$$o([mn]_{m^2}) = \frac{mn}{\mathrm{MCD}\left(mn, m^2\right)} = \frac{mn}{m\mathrm{MCD}(n,m)} = \frac{n}{\mathrm{MCD}(n,m)}$$

e, analogamente,

$$o([mn]_{n^2}) = \frac{m}{\mathrm{MCD}(n,m)}.$$

Pertanto $|\mathrm{Im}\varphi| = \dfrac{mn}{\mathrm{MCD}(m,n)^2}$.

(b) L'applicazione è iniettiva se e solo se $|\mathrm{Im}\varphi| = |\mathbb{Z}_m \times \mathbb{Z}_n| = mn$, il che, in base al punto precedente, avviene se e solo se m e n sono coprimi.

3.

(a) Osserviamo anzitutto che

$$f(x) = h(x)^{p^2},$$

ove $h(x) = x^{p+1} + x^p + x^{p-1} - \overline{1}$, mentre

$$g(x) = k(x)^{p^2},$$

essendo $k(x) = x^2 - \overline{1} = (x - \overline{1})(x + \overline{1})$.

Quindi notiamo che $-\overline{1}$ è radice di $h(x)$, mentre tale non è $\overline{1}$. Ne consegue che $\mathrm{MCD}(h(x), k(x)) = x + \overline{1}$, e dunque $\mathrm{MCD}(f(x), g(x)) = (x + \overline{1})^{p^2} = x^{p^2} + \overline{1}$.

(b) Si ha

$$a(x) = u(x)^{p^2},$$

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

$$b(x) = v(x)^{p^2},$$

essendo $v(x) = x^2 + \overline{1}$.

Nel nostro caso, essendo $p = 137 \equiv 1 \pmod 4$, e quindi $\mathbb{Z}_{137}^*$ un gruppo ciclico di ordine divisibile per 4, esistono esattamente due (cioè $\phi(4)$) elementi $\alpha_1, \alpha_2 \in \mathbb{Z}_{137}^*$ aventi periodo 4, ossia tali che $\alpha_i^2 = -\overline{1}$. Pertanto $v(x) = (x - \alpha_1)(x - \alpha_2)$. Ora, α_1, α_2 sono radici di $x^{p-1} - \overline{1}$, e, d'altra parte, in virtù del Piccolo Teorema di Fermat,

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

In altri termini, α_1, α_2 sono anche radici di $x^{p+1} + \overline{1}$. In conclusione, sono radici di $u(x)$, e pertanto $v(x)$ divide $u(x)$. Ne consegue che $v(x)^p$ divide $u(x)^p$, ossia il resto cercato è il polinomio nullo.