Traccia del 17 aprile 2023

1.

(a) Si può notare che $\sigma = \tau^t$ per un intero t che risolva il seguente sistema di congruenze:

$$\begin{aligned} x &\equiv 2 \pmod 3 \\ x &\equiv 2 \pmod 4 \\ x &\equiv 3 \pmod 5 \\ x &\equiv 6 \pmod 7 \end{aligned}$$

Una soluzione esiste in virtù del Teorema Cinese del Resto (ad esempio, procedendo per tentativi, si può trovare la soluzione -22). Ne consegue che $\sigma \in \langle \tau \rangle$, e pertanto l'intersezione cercata è $\langle \sigma \rangle$.

(b) Si ha $o(\tau) = \mathrm{mcm}(7,5,4,3,2) = 420$. D'altra parte

$$|\langle \tau^{52} \rangle| = o\left(\tau^{52}\right) = \frac{420}{\mathrm{MCD}(420,52)} = \frac{420}{4} = 105,$$

e quindi $\langle \tau^{52} \rangle = \langle \tau^4 \rangle$. Poiché, posto $m = \mathrm{mcm}(n,4)$, si ha $\tau^m \in \langle \tau^n \rangle \cap \langle \tau^4 \rangle$, dovrà essere $\tau^m = \mathrm{id}$, ossia $420 | m$, così che $105 | n$. Viceversa, se $105 | n$, allora $\langle \tau^n \rangle \cap \langle \tau^4 \rangle \subset \langle \tau^{105} \rangle \cap \langle \tau^4 \rangle$, e quest'ultimo è il sottogruppo banale, in quanto $|\langle \tau^{105} \rangle| = 4$ e $|\langle \tau^4 \rangle| = 105$ sono coprimi. In conclusione, gli interi cercati sono tutti e soli quelli della forma $n = 105k$ con $k \in \mathbb{Z}$. A questa conclusione si può giungere anche, più rapidamente, ricordando che $\langle \tau^n \rangle \cap \langle \tau^{52} \rangle = \langle \tau^{\mathrm{mcm}(n,52)} \rangle$, così che questo è il sottogruppo banale se e solo se $420 | \mathrm{mcm}(n, 4 \cdot 13)$, ossia se e solo se $420 | \mathrm{mcm}(n,4)$.

2.

(a) L'applicazione φ_n è un omomorfismo di gruppi. Per ogni $a \in \mathbb{Z}$, si ha che $\alpha = [a]_n \in \mathrm{Ker}\varphi_n$ se e solo se $n | 2a$ e $n | 11a$. Ma questa condizione implica che $n | 11a - 10a = a$. Ciò prova che $\mathrm{Ker}\varphi_n = \{[0]_n\}$. Quindi φ_n è un monomorfismo per ogni n.

(b) Evidentemente $\mathrm{Im}\,\omega_n = \langle [2]_n \rangle \times \langle [11]_n \rangle$. Quindi $|\mathrm{Im}\,\omega_n| = o([2]_n) o([11]_n)$. Si osserva che 385 è dispari, inoltre è divisibile per 11. Ne consegue che $o([2]_{385}) = 385$, $o([11]_{385}) = \frac{385}{11} = 35$. Pertanto $|\mathrm{Im}\,\omega_n| = 385 \cdot 35 = 13475$.

3.

(a) Si ha $f(x) = \left(x^3 + x^2 + x + \overline{1}\right)^p$. Quindi $\alpha \in \mathbb{Z}_p$ è radice di $f(x)$ se e solo se $\alpha^3 + \alpha^2 + \alpha + \overline{1} = \overline{0}$. Poiché $\overline{1}$ non è radice, ciò avviene se e solo se

$$\overline{0} = (\alpha - 1)\left(\alpha^3 + \alpha^2 + \alpha + \overline{1}\right) = \alpha^4 - \overline{1}.$$

Questa condizione è verificata da $\alpha = -\overline{1}$, che quindi è sempre radice. Le restanti radici, ove esistenti, sono gli elementi di $\mathbb{Z}_p^*$ aventi periodo 4. Questi esistono, e sono $\varphi(4) = 2$, se e solo se $4 | p - 1$. In tal caso le radici di $f(x)$ sono complessivamente 3. Altrimenti, ossia quando $p \equiv 3 \pmod 4$, la radice è una sola.

(b) Si ha $g(x) = \left(x^2 - \overline{1}\right)^p = (x - \overline{1})^p (x + \overline{1})^p$. Poiché, come osservato sopra, $\overline{1}$ non è radice di $f(x)$, $x - \overline{1}$ non è tra i fattori irriducibili di $f(x)$. Di contro, $x + \overline{1}$ divide $x^3 + x^2 + x + \overline{1}$, dato che quest'ultimo polinomio ha $-\overline{1}$ come radice. Ne consegue che $\mathrm{MCD}(f(x), g(x)) = (x + \overline{1})^p$.

(c) Dato che $\left(x^3+x^2+x+\overline{1}\right)(x-\overline{1})=x^4-\overline{1}$, il polinomio $f(x)$ divide $\left(x^4-\overline{1}\right)^p=x^{4p}-\overline{1}$. Quest'ultimo, a sua volta, divide $h(x)$. Dunque il resto cercato è il polinomio nullo.

Si è utilizzata la proprietà secondo cui, per ogni intero positivo n, il polinomio $x-\overline{1}$ divide il polinomio $x^n-\overline{1}$ (una conseguenza del Teorema di Ruffini), così che, per ogni intero positivo a, il polinomio $x^a-\overline{1}$ divide il polinomio $x^{an}-\overline{1}$.