Traccia del 6 giugno 2024

1.

(a) La permutazione $\alpha_1 = (1,4,2,5,3,6)$ appartiene a $C(\sigma)$. Infatti α_1 commuta con $(1,2,3)(4,5,6)$, che è il suo quadrato, ed è disgiunta dai restanti cicli di σ. Inoltre a $C(\sigma)$ appartengono anche $\alpha_2 = (10,11,12,13,14)$ e $\alpha_3 = (15,16,17,18,19,20,21)$, in quanto sono entrambi cicli di σ. Poiché le permutazioni $\alpha_1, \alpha_2, \alpha_3$ sono a due a due disgiunte, il seguente insieme è un sottogruppo di $C(\sigma)$:

$$H = \left\{ \alpha_1^{a_1} \alpha_2^{a_2} \alpha_3^{a_3} | a_1, a_2, a_3 \in \mathbb{Z} \right\}.$$

Inoltre $|H| = o(\alpha_1)o(\alpha_2)o(\alpha_3) = 6 \cdot 5 \cdot 7 = 210$, come volevasi.

(b) A $C(\sigma)$ appartiene, oltre ad α_1, anche il 3-ciclo $\beta = (1,2,3)$. Ma $\alpha_1\beta(1) = 5 \neq 4 = \beta\alpha_1(1)$. Ciò prova che $C(\sigma)$ non è abeliano.

2.

(a) Si osservi anzitutto che $N = (n-1)(n+1)(n+2)$ è sempre pari. Inoltre $450 = 2 \cdot 3^2 \cdot 5^2$. Quindi la condizione indicata vale se e solo se 3 e 5 non sono divisori di N. Ora 3 divide N se e solo se divide uno dei tre fattori della precedente decomposizione, e ciò avviene se e solo se $n \equiv 1 \pmod 3$ oppure $n \equiv 2 \pmod 3$. Dunque 3 non divide N se e solo 3 divide n. In modo analogo si vede che 5 non divide N se e solo se $n \equiv 0 \pmod 5$ oppure $n \equiv 2 \pmod 5$. Dunque, alla luce del Teorema Cinese del Resto, l'insieme cercato è

$$\{15k | \, k \in \mathbb{Z}\} \cup \{15k + 12 | \, k \in \mathbb{Z}\}.$$

(b) Condizione necessaria affinché si abbia la relazione indicata è che 3 non divida N. In base a quanto stabilito al punto (a), ciò equivale a richiedere che 3 divida n. In tal caso, per il Teorema di Eulero, $N^2 \equiv 1 \pmod 3$. Ne consegue che $N^{3456} \equiv 1 \pmod 3$. Quindi l'insieme cercato è

$$\{3k | \, k \in \mathbb{Z}\}.$$

(c) Il ragionamento è analogo a quello appena effettuato al punto (b). Quando 5 non divide N, si ha $N^4 \equiv 1 \pmod 5$, e poiché l'esponente 98765 è congruo a 1 modulo 4, se ne deduce che $N^{98765} \equiv N \pmod 5$. In conclusione, si ha la condizione voluta se e solo se $N \equiv 2 \pmod 5$. In tal caso 5 non divide N, e quindi, alla luce di quanto stabilito al punto (a), si avrà $n \equiv 0 \pmod 5$ oppure $n \equiv 2 \pmod 5$. Tuttavia, nel primo caso, $N \equiv 3 \pmod 5$. Nel secondo caso, invece, si ha $N \equiv 2 \pmod 5$. L'insieme cercato è dunque

$$\{5k + 2 | \, k \in \mathbb{Z}\}.$$

3.

(a) Per $p = 2$, le radici di $f(x)$ sono $\overline{0}$ e $\overline{1}$. Esaminiamo ora il caso in cui $p > 2$. Si noti che $\overline{0}$ è sempre radice di $f(x)$. Sia dunque $\alpha \in \mathbb{Z}_p$ non nullo. Si ha, in virtù del Teorema di Eulero e del Piccolo Teorema di Fermat,

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

Ne consegue che α è radice non nulla di $f(x)$ se e solo se $o(\alpha) = 4$ nel gruppo moltiplicativo (ciclico) $\mathbb{Z}_p^*$. Un siffatto elemento α esiste se e solo se $4 | \, p-1$. in tal caso le radici non nulle di $f(x)$ sono due, una l'opposta

dell'altra, e $f(x)$ ha pertanto, complessivamente, tre radici.

(b) Se $p = 2,\ g(x) = x^2 + x$ divide $f(x) = x^4 + x^3,$ e quindi $\mathrm{MCD}(f(x), g(x)) = g(x)$. Sia ora $p > 2$. Si ha $g(x) = \prod_{\alpha \in \mathbb{Z}_p} (x - \alpha)$. Quindi, alla luce del punto (a), e tenendo conto del Teorema di Ruffini, sarà

- $\mathrm{MCD}(f(x), g(x)) = x$, se 4 non divide $p - 1$,
- $\mathrm{MCD}(f(x), g(x)) = x\left(x^2 + \overline{1}\right) = x^3 + x$, se 4 divide $p - 1$.

Riguardo all'ultima affermazione, basta osservare che, se α è una radice non nulla di $f(x)$, l'altra radice non nulla è $-\alpha$, e si ha, in virtù di (*),

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