Note alla traccia del 13 novembre 2020

1. Si osservi che il centralizzante di un elemento di un gruppo è sempre un sottogruppo, e quindi è chiuso rispetto all'operazione del gruppo, vi appartiene l'elemento neutro, ed è chiuso rispetto alla formazione degli elementi simmetrici. Conseguentemente, in un gruppo moltiplicativo, è chiuso rispetto all'elevamento a potenza. Pertanto:

- se un elemento g di un gruppo moltiplicativo commuta con altri due elementi h e k, ossia h e k appartengono al centralizzante di g, allora a tale centralizzante appartiene anche il loro prodotto: in altri termini, se un elemento commuta con altri elementi, commuta anche con ogni loro prodotto;
- se un elemento g di gruppo moltiplicativo commuta con un altro elemento h, ossia h appartiene al centralizzante di g, a tale centralizzante appartiene ogni potenza di h: in definitiva, se un elemento commuta con un altro elemento, commuta con ogni potenza di quest'ultimo.

2.

(a) L'omomorfismo indicato è ben definito, in quanto, per ogni $a, a' \in \mathbb{Z}$ tali che $[a]_n = [a']_n$, si ha che n divide $a - a'$, e quindi mn divide $m(a - a') = ma - ma'$, ossia $[ma]_{mn} = [ma']_{mn}$.

Ora: $[m]_{nm} = m[1]_{nm}$, ove m è un divisore di $o([1]_{nm}) = nm$. Dunque $o([m]_{nm}) = \dfrac{nm}{m} = n$.

(c) Si ricordi che l'immagine di un omomorfismo di gruppo è sempre un sottogruppo del gruppo di arrivo. Nel nostro caso, $\mathrm{Im}\psi$ è dunque un sottogruppo di $\mathbb{Z}_{nm}$. Ora, ogni sottogruppo a cui appartenga $[1]_{mn}$ contiene il sottogruppo ciclico da esso generato, che è tutto $\mathbb{Z}_{nm}$. Quindi, se fosse $[1]_{nm} \in \mathrm{Im}\psi$, si avrebbe $\mathrm{Im}\psi = \mathbb{Z}_{nm}$. In tal caso, poiché gli insiemi di partenza e di arrivo hanno la stessa cardinalità finita, pari a nm, ψ sarebbe bigettivo, e quindi un isomorfismo.

Sia ora $(\alpha, \beta) \in \mathbb{Z}_n \times \mathbb{Z}_m$. Questo è un elemento periodico (in quanto appartenente ad un gruppo finito), e il suo periodo è $\mathrm{mcm}(o(\alpha), o(\beta))$. Ora, per il Teorema di Lagrange, $o(\alpha)$ divide n, mentre $o(\beta)$ divide m. Quindi $\mathrm{mcm}(n, m)$, che è multiplo di n e m, per la transitività della relazione di divisibilità, è multiplo comune di $o(\alpha)$ e di $o(\beta)$. Ne consegue che $\mathrm{mcm}(o(\alpha), o(\beta))$ divide $\mathrm{mcm}(n, m)$.

Ora, essendo n, m non coprimi, si ha $\mathrm{MCD}(n, m) > 1$, quindi $\mathrm{mcm}(n, m) = \dfrac{nm}{\mathrm{MCD}(n, m)} < nm$.

3.

(a) Il criterio di Eisenstein risulta soddisfatto, poiché

- il polinomio $f(X)$ è monico,
- $\mathrm{Re}(\alpha)$ è un numero intero, quindi il suo doppio un numero pari,
- in virtù della moltiplicatività della norma dei numeri complessi, il termine noto è $||\alpha|| = \prod_{k=0}^{n} ||\alpha_k||$, ossia il prodotto $\prod_{k=0}^{n} \left(2^{2k} + 1\right)$, in cui il fattore corrispondente a $k = 0$ è 2, mentre i restanti fattori sono tutti dispari; quindi 2^2 non divide il termine noto.