Automorfismi di un gruppo ciclico finito

Dato un gruppo ciclico $G,$ su cui fissiamo la notazione moltiplicativa, ogni omomorfismo f che lo abbia come gruppo di partenza è univocamente determinato dall'immagine di un suo generatore: detto g tale generatore, esiste, per ogni elemento a del gruppo di arrivo (che supponiamo anch'esso moltiplicativo), al più un omomorfismo per il quale si abbia $f(g) = a$, precisamente si tratta dell'applicazione tale che, per ogni $n \in \mathbb{Z},\ f\left(g^n\right) = a^n$. L'immagine di g^n è determinata dal fatto che l'omomorfismo f deve conservare le potenze (in quanto conserva elemento uno, prodotti e inversi). Si noti che $\mathrm{Im}f = \langle a \rangle = \langle f(g) \rangle$.
Si tenga presente che f è ben definito se e solo se, per ogni $n, m \in \mathbb{Z},\ g^n = g^m \Longrightarrow a^n = a^m$, ossia se e solo se, per ogni $n \in \mathbb{Z}, g^n = 1 \Longrightarrow a^n = 1,$ ossia:

(i) sempre, se g è aperiodico;

(ii) se g è periodico, se e solo se anche a è periodico e $o(a)|o(g)$.

Supponiamo ora che $G = \langle g \rangle$ sia finito, di ordine m. Sia f un endomorfismo di G. In tal caso $f(g)$ può essere un qualunque elemento $a \in G$ (in quanto, se g è periodico, la condizione (ii) è verificata da ogni $a \in G$). L'omomorfismo f sarà bigettivo se e solo se surgettivo, ossia se e solo se $f(g)$ è un generatore di G. Gli elementi siffatti sono $\varphi(m)$, essendo φ la funzione di Eulero. Ciò prova che, in questo caso, il gruppo $\mathrm{Aut}(G)$ ha ordine $\varphi(|G|)$. Ad esempio, se G ha ordine 4 - ed è, in quanto ciclico, appartenente al "secondo modello" - si avrà che $|\mathrm{Aut}(G)| = 2$.