Problema 32. Sigui G un grup cíclic finit. Calculeu $Aut(G)$, el grup dels automorfismes de G.

Solució. Sigui G un grup cíclic, és a dir $G = \langle g \rangle$ on $|G| = o(g) = n$. Hem de trobar el grup $Aut(G)$, és a dir, els isomorfismes de $G \to G$. Que sigui isomorfisme equival a dir que sigui morfisme i bijectiu. Veurem doncs la injectivitat i l'exhaustivitat.

Per a veure quins són els possibles morfismes d'un grup cíclic, n'hi ha prou en veure quina és la imatge d'un generador del grup; ja que si tenim un element $a \in G$ qualsevol i $G =< g >$ aleshores $a = g^r$, amb $r \in \mathbb{Z}$. Per tant, sigui f un morfisme qualsevol $f(a) = f(g^r) = (f(g))^r$, com havíem dit, equival a buscar una imatge del generador.

Donat $k \in \mathbb{Z}$ podem definir $\forall a \in G$

$$f_k : G \to G$$
$$a \longmapsto a^k$$

Comprovem que és morfisme de grups i que està ben definit:

Sigui $g^i, g^j \in G \to f_k(g^i g^j) = g^{(i+j)^k} = g^{ik+ij} = g^{ik} g^{jk} = f_k(g^i) f_k(g^j)$

Sigui $G =< g >$ i g d'ordre n. Donat $\sigma \in Aut(G)$, $\sigma(g) \in G$, de manera que $\exists k \in \mathbb{Z}$ $\sigma(g) = g^k$. Notem que k està ben definit mòdul n (perquè g és d'ordre n). A més a més, si σ és automorfisme, $\sigma(g)$ ha de ser un generador de G; o sigui, tenim que $1 \leq k \leq n$ i que $mcd(k, n) = 1$. O sigui, $k := \chi(\sigma) \in (\mathbb{Z}/n\mathbb{Z})^*$. Això defineix una aplicació

$$\chi : Aut(G) \to (\mathbb{Z}/n\mathbb{Z})^*$$
$$\sigma \mapsto \chi(\sigma)$$

Notem que $\chi(\sigma \circ \tau) = \chi(\sigma) \cdot \chi(\tau)$ i que $\chi(\sigma) = 1 \to \sigma = 1$. O sigui que χ és un morfisme de grups injectiu. A més a més, donat $k \in (\mathbb{Z}/n\mathbb{Z})^*$, l'assignació

$$\sigma_k : G \to G$$
$$a \mapsto a^k$$

és un automorfisme de G (i tal que $\chi(\sigma_k) = k$); o sigui, χ és exhaustiu.

En resum, $\chi : Aut(G) \to (\mathbb{Z}/n\mathbb{Z})^*$ és un isomorfisme de grups i $Aut(G) \cong (\mathbb{Z}/n\mathbb{Z})^*$