Esercizio 8.11 Sia n un intero maggiore di 1. Proviamo che allora, per ogni $\alpha \in \mathbb{Z}_n$ non nullo, α è regolare se e solo se α è invertibile.

Dimostrazione: Se α è invertibile, allora è regolare in base alla Proposizione 5.17. Viceversa, supponiamo che α sia regolare. Sia $a \in \mathbb{Z}$ tale che $\alpha = [a]_n$. Allora, essendo $\alpha \neq 0$, si ha che $n \nmid a$. Sia $d = \mathrm{MCD}(a, n)$. Ora, il numero intero

$$a\frac{n}{d} = n\frac{a}{d}$$

è multiplo di n, e quindi

$$\left[a\frac{n}{d}\right]_n = [a]_n\left[\frac{n}{d}\right]_n = [0]_n.$$

Essendo $[a]_n$ regolare, ne consegue che $\left[\frac{n}{d}\right]_n = [0]_n$, ossia che $\frac{n}{d}$ è un multiplo di n. Poiché $0 < \frac{n}{d} \leq n$, ciò è possibile solo se $d = 1$. Dunque a e n sono coprimi, e pertanto, per la Proposizione 8.7, $[a]_n$ è invertibile.