Behauptung:

Sei $(G, \cdot, e)$ eine endliche Gruppe und $s \in G$

Für $k \in \mathbb{Z}$ mit $s^k = e$ gilt: $\operatorname{ord} s \mid k$

Beweis:

Wir teilen k durch $\operatorname{ord} s$ mit Rest r ($\mathbb{Z}$ ist ein euklidischer Ring!)

$\rightarrow \quad \exists\, m \in \mathbb{Z} \quad \exists\, r \in \{0, 1 \ \ldots \operatorname{ord} s - 1\}$:

$k = m \cdot \operatorname{ord} s + r$

$\rightarrow \quad e = s^k = s^{m \cdot \operatorname{ord} s + r} = \left(s^{\operatorname{ord} s}\right)^m \cdot s^r = e^m \cdot s^r = s^r$

Da $r \in \{0, \ldots, \operatorname{ord} s - 1\}$ und $\operatorname{ord} s = \min\{n \in \mathbb{N} \mid s^n = e\}$,

folgt zwingend $r = 0$

$\rightarrow \quad k = m \cdot \operatorname{ord} s$

$\Rightarrow \quad \operatorname{ord} s \mid k$