Satz: Sei $(G, \cdot, e)$ eine Gruppe, sei $s \in G$ mit $ords = n \in \mathbb{N}$. Dann gilt für alle $k \in \mathbb{Z}$:

$$ord\ s^k = \frac{ord\ s}{ggT(k,\ ord\ s)} = \frac{n}{(k,n)}$$

Beweis:

Wir verwenden folgende Notationen:

$ggT(k,n) =: t$

$\Rightarrow (\exists\, \tilde{k} \in \mathbb{Z}: \quad k = t \cdot \tilde{k}) \wedge (\exists\, \tilde{n} \in \mathbb{N}: \quad n = t \cdot \tilde{n})$

(1) $\left(s^k\right)^{\frac{n}{(k,n)}} = \left(s^k\right)^{\frac{n}{t}} = \left(s^{t\cdot\tilde{k}}\right)^{\tilde{n}} = \left(s^{t\cdot\tilde{n}}\right)^{\tilde{k}} = \left(s^n\right)^{\tilde{k}} = e^{\tilde{k}} = e$

$\Rightarrow \quad ord\ s^k \leq \frac{n}{(k,n)} = \tilde{n}$

(2) Annahme: $ord\ s^k = m < \tilde{n}$

Wir teilen $\tilde{n}$ durch m mit Rest r :

$\tilde{n} = q \cdot m + r \quad (q \in \mathbb{N}_0,\ r \in \{0, \ldots m-1\})$

$$\begin{aligned}
\text{Aus (1):}\quad e &= \left(s^k\right)^{\tilde{n}} \\
&= \left(s^k\right)^{q\cdot m + r} \\
&= \left(\left(s^k\right)^m\right)^q \cdot \left(s^k\right)^r \\
&\overset{ord\, s^k = m}{=} e^q \cdot s^{k\cdot r} \\
&= \left(s^k\right)^r
\end{aligned}$$

$ord\, s^k \leq r < m \quad \lightning$ Minimalität von m.

(1), (2) $\Rightarrow \quad ord\, s^k = \tilde{n}$