F12-T2-A2

Es seien G eine endliche Gruppe und p eine Primzahl. Begründen Sie, dass die Anzahl der Elemente der Ordnung p in G durch $p-1$ teilbar ist, d.h.

$$|\{a \in G | \text{ord}(a) = p\}| = (p-1) \cdot k \text{ für ein } k \in \mathbb{N}.$$

(Hinweis: Betrachten Sie die Mengen $M_a = \{a, a^2, \ldots, a^{p-1}\}$ für $a \in G$ mit $\text{ord}(a) = p$.)

Lösungsvorschlag. Dem Hinweis folgend betrachten wir für $a \in G$ mit $\text{ord}(a) = p$ die Menge $M_a := \{a, a^2, \ldots, a^{p-1}\}$. Wir beobachten, dass jedes Element der Form a^i in M_a ebenfalls Ordnung p besitzt (wegen $M_a \subset \langle a \rangle$ und $|\langle a \rangle| = p$, nach dem Satz von Lagrange). Es bleibt mit $|M_a| = p-1$ also nur zu zeigen, dass für ein Element $b \in G$ mit $\text{ord}(b) = p$ und $b \notin M_a$ bereits gilt $M_b \cap M_a = \emptyset$. Angenommen also, $b^i = a^j$ für $i, j \in \mathbb{N}$. Dann könnten wir aber $l \in \mathbb{N}$ wählen, so dass $il \equiv 1 \mod p$ (dies ist möglich wegen $\text{ggT}(i, p) = 1$), dann aber wäre $b = b^{il} = a^{jl}$ und also $b \in M_a$ im Widerspruch zur Annahme.