Aufgabe H18T1A3 (12 Punkte)

Seien p eine Primzahl, $q = p^n$ $(n \geq 1)$ eine Primzahlpotenz und $\mathbb{F}_q$ der endliche Körper mit q Elementen.

(a) Zeigen Sie im Falle $p \neq 2$: $|\{x^2 \mid x \in \mathbb{F}_q\}| = \frac{q+1}{2}$.

(b) Sei $\alpha \in \mathbb{F}_q$ gegeben. Zeigen Sie, dass $x, y \in \mathbb{F}_q$ so existieren, dass $\alpha = x^2 + y^2$ gilt.
Hinweis: Betrachten Sie den Schnitt der Mengen $\{\alpha - x^2 \in \mathbb{F}_q \mid x \in \mathbb{F}_q\}$ und $\{y^2 \in \mathbb{F}_q \mid y \in \mathbb{F}_q\}$.

Anmerkungen/Hinweise:

Diese Aufgabe wurde in ähnlicher Form schon früher gestellt. Die entscheidende Idee besteht darin, den Homomorphiesatz auf die multiplikative Gruppe $\mathbb{F}_q^\times$ anzuwenden. Welchen Homomorphismus mit Definitionsbereich $\mathbb{F}_q^\times$ sollte man naheliegenderweise betrachten? Bei Teil (b) ist zu beachten, dass für beliebige endliche Mengen S, T jeweils $|S \cup T| = |S| + |T| - |S \cap T|$ gilt. Sind S und T disjunkt, dann gilt insbesondere $|S \cup T| = |S| + |T|$.