H18-T1-A3

Sei 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 $x, y \in \mathbb{F}_q$ existieren, sodass $\alpha = x^2 + y^2$ gilt. Hinweis: Betrachten Sie den Schnitt der Mengen $\{\alpha - x^2 \in \mathbb{F}_q \mid x \in \mathbb{F}_q\}$ und $\{y^2 \in \mathbb{F}_q \mid y \in \mathbb{F}_q\}$.

Lösungsvorschlag. Zu a). Es sei $M = \{x^2 \mid x \in \mathbb{F}_q\}$. Betrachte den Gruppenhomomorphismus $\varphi : \mathbb{F}_q^* \to \mathbb{F}_q^*, \quad x \mapsto x^2$. Dann ist das Bild offensichtlich gegeben durch $\mathrm{Im}(\varphi) = M \setminus \{0\}$. Wegen

$$x \in \ker(\varphi) \Leftrightarrow \varphi(x) = x^2 = 1 \Leftrightarrow x^2 - 1 = 0 \Leftrightarrow (x-1)(x+1) = 0 \Leftrightarrow x = \pm 1$$

und $1 \neq -1$ (da $\mathrm{char}(\mathbb{F}_q) = p \neq 2$) erhält man $|\ker(\varphi)| = 2$. Mit dem Homomorphiesatz folgt $\mathbb{F}_q^*/\ker(\varphi) \cong \mathrm{Im}(\varphi)$ und damit insbesondere

$$|M| - 1 = |M \setminus \{0\}| = |\mathrm{Im}(\varphi)| = |\mathbb{F}_q^*/\ker(\varphi)| = \frac{|\mathbb{F}_q^*|}{|\ker(\varphi)|} = \frac{q-1}{2},$$

also $|M| = \frac{q+1}{2}$, was zu zeigen war.
Zu b). Sei $A = \{\alpha - x^2 \mid x \in \mathbb{F}_q\}$ und $B = \{y^2 \mid y \in \mathbb{F}_q\}$. Nach a) gilt $|B| = \frac{q+1}{2}$. Betrachtet man die Bijektion

$$\begin{aligned} \{x^2 \mid x \in \mathbb{F}_q\} &\longrightarrow \{\alpha - x^2 \mid x \in \mathbb{F}_q\}, \\ x^2 &\longmapsto \alpha - x^2 \end{aligned}$$

so sieht man $|A| = \frac{q+1}{2}$.
Angenommen es wäre $A \cap B = \emptyset$, dann folgt $|A \cup B| = |A| + |B| = q + 1$, was einen Widerspruch zu $A \cup B \subseteq \mathbb{F}_q$ und $|\mathbb{F}_q| = q$ darstellt.
Es muss folglich ein $z \in A \cap B$ existieren, also $z = \alpha - x^2 = y^2$ für $x, y \in \mathbb{F}_q$ und somit $\alpha = x^2 + y^2$.