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 $\{y^2 \in \mathbb{F}_q \mid y \in \mathbb{F}_q\}$.

Lösung:

zu (a) Zunächst bestimmen wir die Anzahl der Quadrate in $\mathbb{F}_q^\times$ durch Anwendung des Homomorphiesatzes. Dazu betrachten wir die Abbildung $\phi : \mathbb{F}_q^\times \to \mathbb{F}_q^\times$, $a \mapsto a^2$. Offenbar ist $\phi(\mathbb{F}_q^\times)$ die Menge der Quadrate in $\mathbb{F}_q^\times$. Die Abbildung ϕ ist ein Homomorphismus von Gruppen, denn für alle $a, b \in \mathbb{F}_q^\times$ gilt

$$\phi(ab) \quad = \quad (ab)^2 \quad = \quad a^2b^2 \quad = \quad \phi(a)\phi(b).$$

Ein Element $a \in \mathbb{F}_q$ ist genau dann in $\ker(\phi)$ enthalten, wenn $a^2 = \phi(x) = \bar{1}$ gilt, also genau dann, wenn a eine Nullstelle des Polynoms $x^2 - \bar{1}$ ist. Wegen $\mathrm{char}(\mathbb{F}_q) = p \neq 2$ sind $\pm\bar{1}$ zwei verschiedene Nullstellen dieses Polynoms, und wegen $\mathrm{grad}(x^2 - \bar{1}) = 2$ gibt es keine weiteren. Also gilt $\ker(\phi) = \{\pm\bar{1}\}$. Aus dem Homomorphiesatz folgt nun $\phi(\mathbb{F}_q^\times) \cong \mathbb{F}_q^\times/\{\pm\bar{1}\}$, und damit erhalten wir

$$|\phi(\mathbb{F}_q^\times)| \quad = \quad |\mathbb{F}_q^\times/\{\pm\bar{1}\}| \quad = \quad \frac{|\mathbb{F}_q^\times|}{|\{\pm\bar{1}\}|} \quad = \quad \tfrac{1}{2}(q-1).$$

Weil in $\mathbb{F}_q$ auch $\bar{0}^2 = \bar{0}$ ein Quadrat ist, ergibt sich für die Anzahl der Quadrate in $\mathbb{F}_q$ insgesamt der Wert $|\phi(\mathbb{F}_q^\times)| + 1 = \frac{1}{2}(q-1) + 1 = \frac{1}{2}(q+1)$.

zu (b) Auch hier betrachten wir zunächst den Fall $p \neq 2$. Sei $S = \{\alpha - a^2 \in \mathbb{F}_q \mid a \in \mathbb{F}_q\}$ und $T = \{a^2 \mid a \in \mathbb{F}_q\}$. Die Mächtigkeit von T haben wir in Teil (a) schon bestimmt. Um auch $|S|$ zu erhalten, betrachten wir die Abbildung $\psi : T \to S$, $b \mapsto \alpha - b$. Diese Abbildung ist bijektiv, denn durch $\psi_1 : S \to T$, $b \mapsto \alpha - b$ ist eine Umkehrabbildung definiert: Für jedes $b \in T$ gilt $(\psi_1 \circ \psi)(b) = \psi_1(\alpha - b) = \alpha - (\alpha - b) = b$, und ebenso $(\psi \circ \psi_1)(c) = \psi(\alpha - c) = \alpha - (\alpha - c) = c$ für jedes $c \in S$. Aus der Bijektivitiät von ψ folgt $|S| = |T| = \frac{1}{2}(q+1)$.

Laut Angabe soll der Durchschnitt der beiden Menge betrachtet werden. Wäre $S \cap T = \varnothing$, dann wäre durch $S \cup T$ eine Teilmenge von $\mathbb{F}_q$ der Mächtigkeit $|S| + |T| = \frac{1}{2}(q+1) + \frac{1}{2}(q+1) = q+1$ gegeben. Aber dies ist wegen $|\mathbb{F}_q| = q$ unmöglich. Es gibt also ein Element $c \in S \cap T$ und somit Elemente $a, b \in \mathbb{F}_q$ mit $\alpha - a^2 = c = b^2$. Es folgt $a^2 + b^2 = \alpha$.

Nun betrachten wir noch den Fall $p = 2$. Wie in Teil (a) überprüft man, dass $\phi : \mathbb{F}_q^\times \to \mathbb{F}_q^\times$, $a \mapsto a^2$ ein Gruppenhomomorphismus ist, dessen Bild $\phi(\mathbb{F}_q^\times)$ aus den Quadraten in $\mathbb{F}_q^\times$ besteht. Wieder besteht der Kern genau aus den Nullstellen des Polynoms $x^2 - \bar{1}$. Wegen $\mathrm{char}(\mathbb{F}_q) = 2$ gilt hier aber $x^2 - \bar{1} = (x - \bar{1})^2$, d.h. $\bar{1}$ ist eine doppelte Nullstelle des Polynoms, und folglich gilt diesmal $\ker(\phi) = \{\bar{1}\}$. Mit dem Homomorphiesatz folgt $\mathbb{F}_q^\times/\{\bar{1}\} \cong \phi(\mathbb{F}_q^\times)$ und $|\phi(\mathbb{F}_q^\times)| = |\mathbb{F}_q^\times/\{\bar{1}\}| = \frac{|\mathbb{F}_q^\times|}{|\{\bar{1}\}|} = \frac{q-1}{1} = q - 1$. Wegen $\phi(\mathbb{F}_q^\times) \subseteq \mathbb{F}_q^\times$ und $|\phi(\mathbb{F}_q^\times)| = q - 1 = |\mathbb{F}_q^\times|$ folgt $\phi(\mathbb{F}_q^\times) = \mathbb{F}_q^\times$, also ist im Fall $p = 2$ jedes Element in $\mathbb{F}_q^\times$ ein Quadrat! Weil auch $\bar{0}^2 = \bar{0}$ ein Quadrat ist, besteht $\mathbb{F}_q$ also insgesamt nur aus Quadraten. Für jedes $\alpha \in \mathbb{F}_q$ gibt es also ein $a \in \mathbb{F}_q$ mit $\alpha = a^2 = a^2 + \bar{0}^2$.