Aufgabe H13T2A4 (6 Punkte)

Sei K ein endlicher Körper. Sei $a \in K$. Zeigen Sie, dass es Elemente $x, y \in K$ gibt, so dass $x^2 + y^2 = a$ gilt.
Hinweis: Wie viele Quadrate gibt es in K ?

Lösung:

Sei Q die Menge der Quadrate in K und $(K^\times)^2$ die Menge der Quadrate in $K^\times$. Wegen $0 = 0^2 \in Q$ gilt $Q = (K^\times)^2 \cup \{0\}$, also $|Q| = |(K^\times)^2| + 1$. Dem Hinweis folgend bestimmen wir zunächst die Mächtigkeit $|(K^\times)^2|$. Die Abbildung $\phi : K^\times \to (K^\times)^2$, $x \mapsto x^2$ ist ein Gruppenhomomorphismus, denn für alle $x, y \in K^\times$ gilt $\phi(xy) = (xy)^2 = x^2y^2 = \phi(x)\phi(y)$. Außerdem ist ϕ offenbar surjektiv. Wir können nun den Homomorphiesatz anwenden und erhalten

$$\frac{|K^\times|}{|\ker(\phi)|} \quad = \quad (K^\times : \ker(\phi)) \quad = \quad |(K^\times)^2|.$$

Der Kern $\ker(\phi)$ besteht genau aus den Elementen $x \in K$ mit $x^2 = 1$, denn 1 ist das Neutralelement der Gruppe $K^\times$. Dies sind genau die Nullstellen des Polynoms $X^2 - 1 \in K[X]$. Ist $\mathrm{char}(K) = 2$, dann gilt $(X^2 - 1) = (X - 1)^2$, also ist 1 die einzige Nullstelle und $\ker(\phi) = \{1\}$. Ansonsten sind durch ± 1 zwei verschiedene Nullstellen von $X^2 - 1$ gegeben, und wegen $\mathrm{grad}(X^2 - 1) = 2$ gibt es keine weiteren. Dann gilt also $\ker(\phi) = \{\pm 1\}$. In jedem Fall gilt also $|\ker(\phi)| \leq 2$ und auf Grund der Gleichung von oben somit $|(K^\times)^2| \geq \frac{1}{2}|K^\times| = \frac{1}{2}(q - 1)$, wobei q die Elementezahl von K bezeichnet. Es folgt $|Q| = |(K^\times)^2| + 1 \geq \frac{1}{2}(q + 1)$.

Wir betrachten nun neben Q noch die Menge $N = \{a - x^2 \mid x \in K\}$, wobei $a \in K$ das Element aus der Aufgabenstellung ist. Durch $\phi : Q \to N$, $z \mapsto a - z$ ist eine Bijektion zwischen Q und N gegeben, deren Umkehrabbildung durch $\psi : N \to Q$, $z \mapsto a - z$ definiert ist, denn für alle $c \in Q$ gilt $(\psi \circ \phi)(c) = \psi(a - c) = a - (a - c) = c$, und ebenso erhält man $(\phi \circ \psi)(d) = d$ für alle $d \in N$. Aus der Existenz der Bijektion folgt $|N| = |Q| \geq \frac{1}{2}(q + 1)$. Wären Q und N disjunkte Teilmengen von K, dann würde $|Q \cup N| = |Q| + |N| = 2|Q| \geq q + 1$ folgen, was aber wegen $Q \cup N \subseteq K$ und $|K| = q$ unmöglich ist. Es gibt also ein $z \in Q \cap N$ und somit $x, y \in K$ mit $x^2 = z = a - y^2$. Damit erhalten wir $x^2 + y^2 = a$ wie gewünscht.