Aufgabe H19T1A5 (12 Punkte)

Es sei die Gleichung $x^2 + ux + v = 0$ mit $u, v \in \mathbb{F}_q$ betrachtet, wobei $\mathbb{F}_q$ der endliche Körper mit q Elementen ist.

(a) Zeigen Sie für ungerades q: Die Gleichung ist genau dann lösbar über $\mathbb{F}_q$, wenn $u^2 - 4v$ ein Quadrat in $\mathbb{F}_q$ ist.

(b) Zeigen Sie für gerades q und $u \neq 0$: Die Gleichung ist genau dann lösbar über $\mathbb{F}_q$, wenn v/u^2 von der Form $z^2 + z$ für ein $z \in \mathbb{F}_q$ ist.

Hinweis/Kommentar:

Bei (a) versuchen Sie, die Gleichung wie in der Schule mit „quadratischer Ergänzung“ zu lösen, dann ergibt sich die Darstellung von $u^2 - 4v$ als Quadrat ganz von selbst. Der Beweis der umgekehrten Implikationsrichtung ist dann auch kein Problem mehr. Bei (b) reicht es für die erste Implikationsrichtung im Wesentlichen, die Gleichung mit u^{-2} zu multiplizieren; beachten Sie allerdings, dass auf Grund der Voraussetzungen in $\mathbb{F}_q$ hier $-\bar{1} = \bar{1}$ gilt (warum?).