F18-T1-A5

Es sei p eine ungerade Primzahl, und es sei $a \in \mathbb{Z}$. Zeigen Sie, dass folgende Aussagen äquivalent sind:

a) Es gibt genau eine Zahl $b \geq 0$ mit $a^2 + b^2 = (b+p)^2$.

b) Es ist $a \equiv p \mod 2p$.

Lösungsvorschlag. Zu a)⇒b). Wir setzen also voraus, dass ein $b \geq 0$ existiert, so dass gilt

$$a^2 + b^2 = b^2 + 2bp + p^2 \quad \Longleftrightarrow \quad a^2 = 2bp + p^2. \tag{1}$$

Insbesondere bedeutet dies ja $a^2 = p^2 = 1 \mod 2$ und $a^2 = 0 \mod p$. Nach dem chinesischen Restsatz existiert ein Ringisomorphismus

$$\pi \colon \mathbb{Z}_{2p} \longrightarrow \mathbb{Z}_2 \times \mathbb{Z}_p, \quad [a] \longmapsto ([a], [a]),$$

und obige Beobachtung ist äquivalent zu $\pi([a^2]) = ([1], [0])$. Mit

$$([a]^2, [a]^2) = \pi([a])^2 = \pi([a^2]) = ([1], [0])$$

muss also gelten $[a]^2 = [1] \in \mathbb{Z}_2$ und $[a]^2 = [0] \in \mathbb{Z}_p$, also (mit $X^2+1 = (X+1)^2 \in \mathbb{F}_2[X]$) wissen wir bereits $[a] = [1] \in \mathbb{Z}_2$ und $[a] = [0] \in \mathbb{Z}_p$, also $\pi([a]) = ([1], [0])$. Da aber auch $\pi([p]) = ([1], [0])$ gilt und π ein Isomorphismus ist, folgt also $[a] = [p] \in \mathbb{Z}_{2p}$, was ja gerade die Aussage von b) ist.
Alternative: Wir betrachten

$$a^2 + b^2 = b^2 + 2bp + p^2 \quad \Longleftrightarrow \quad (a-p)(a+p) = a^2 - p^2 = 0 \mod 2p.$$

Nun unterscheiden wir zwei Fälle:

- Fall 1: $[a-p] = [0]$ oder $[a+p] = [0]$ in $\mathbb{Z}_{2p}$ in diesem Fall folgt sofort $[a] = [p] \in \mathbb{Z}_{2p}$ bzw. $[a] = -[p] = [p] \in \mathbb{Z}_{2p}$.
- Fall 2: $[a-p]$ und $[a+p]$ sind Nullteiler in $\mathbb{Z}_{2p}$ die einzigen Nullteiler in $\mathbb{Z}_{2p}$ sind aber $[2]$ und $[p]$. Wir wollen diesen Fall zu einem Widerspruch führen. Sowohl aus $a - p = p \mod 2p$ als auch aus $a + p = p \mod 2p$ folgt jeweils $[a] = [0] \in \mathbb{Z}_{2p}$, woraus aber sofort der Widerspruch $[0] = [a^2] = [p^2] \in \mathbb{Z}_{2p}$ folgt.

Zu b)⇒a). Angenommen $a = p \mod 2p$, also $a = p + x2p$ für ein $x \in \mathbb{Z}$. Dann erhalten wir

$$a^2 = (p + x2p)^2 = p^2 + 4xp^2 + 4x^2p^2 = p^2 + 2p(2xp + 2x^2p).$$

Nach Vergleich mit (1) ist b damit eindeutig bestimmt zu $b := 2p(x + x^2)$. Dass $b \geq 0$ gilt folgt dabei aus der Tatsache, dass das Polynom $f(X) = X^2 + X = X(X+1) \in \mathbb{R}[X]$ die Nullstellen -1 und 0 besitzt, und offensichtlich gilt $f(x) < 0$ genau dann, wenn $x \in (-1, 0)$.