Aufgabe F18T1A5 (12 Punkte)

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

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

(ii) Es ist $a \equiv p \bmod 2p$.

Lösung:

Zunächst bemerken wir, dass sich die Gleichung in Teil (i) umstellen lässt zu

$$a^2 + b^2 = (b+p)^2 \quad \Leftrightarrow \quad a^2 + b^2 = b^2 + 2bp + p^2 \quad \Leftrightarrow \quad a^2 = 2bp + p^2 \quad \Leftrightarrow \quad a^2 = p(p+2b).$$

Wir können die Gleichung in Aussage (i) also durch $a^2 = p(p+2b)$ ersetzen.

„(i) $\Rightarrow$ (ii)" Aus $a^2 = p(p+2b)$ folgt $p \mid a^2$ und somit auch $p \mid a$. Es gibt also ein $k \in \mathbb{Z}$ mit $a = kp$. Betrachten wir zunächst den Fall, dass k gerade ist. Dann wäre a^2, und somit auch $p(p+2b)$, durch 4 teilbar. Aber dies ist unmöglich, weil die Faktoren p und $p+2b$ beide ungerade sind. Also ist k ungerade, $k = 2\ell + 1$ für ein $\ell \in \mathbb{Z}$. Daraus folgt

$$a \quad = \quad (2\ell+1)p \quad = \quad \ell \cdot 2p + p \quad \equiv \quad p \bmod 2p.$$

„(ii) $\Rightarrow$ (i)" Wegen $a \equiv p \bmod 2p$ gibt es ein $k \in \mathbb{Z}$ mit $a = p + 2kp$. Daraus folgt

$$a^2 \quad = \quad p^2(2k+1)^2 \quad = \quad p^2(1+4k+4k^2) \quad = \quad p(p+4kp+4k^2p) \quad = \quad p(p+2b)$$

mit $b = 2kp + 2k^2p = 2pk(k+1)$. Wäre $b < 0$, dann müssten k und $k+1$ beide ungleich Null sein und unterschiedliche Vorzeichen haben, was aber wegen $k \in \mathbb{Z}$ unmöglich ist. Also ist $b \geq 0$. Außerdem ist b durch die Gleichung $a^2 = p(p+2b)$ eindeutig bestimmt. Ist nämlich c eine weitere ganze Zahl mit $a^2 = p(p+2c)$, dann folgt $p(p+2b) = p(p+2c) \Rightarrow p+2b = p+2c \Rightarrow 2b = 2c \Rightarrow b = c$.