H15-T3-A1

Seien $x, y, z \in \mathbb{Z}$ mit $x^2 + y^2 = z^2$. Zeigen Sie, dass das Produkt xyz durch 60 teilbar ist. (12 Punkte)

Lösungsvorschlag. Nach dem chinesischen Restsatz gilt

$$[xyz] = [0] \in \mathbb{Z}_{60} \quad \Leftrightarrow [xyz] = [0] \in \mathbb{Z}_3 \text{ und } [xyz] = [0] \in \mathbb{Z}_4 \text{ und } [xyz] = [0] \in \mathbb{Z}_5.$$

Seien nun also $x, y, z \in \mathbb{Z}$ mit $x^2 + y^2 = z^2$ gegeben.

1. Zuerst betrachten wir die Gleichung $[x]^2 + [y]^2 = [z]^2$ in $\mathbb{Z}_3$. In $\mathbb{Z}_3$ gibt es die Quadrate $[0] = [0]^2$ und $[1] = [1]^2 = [2]^2$, und wir finden also die Möglichkeiten
   - $[x] \in \{[1], [2]\}$, $[y] = [0]$, und $[z] \in \{[1], [2]\}$,
   - $[x] = [0]$, $[y] \in \{[1], [2]\}$ und $[z] \in \{[1], [2]\}$, und
   - $[x] = [y] = [z] = [0]$.

   In jedem Fall gilt also $3|x$ oder $3|y$, insbesondere $3|xyz$.

2. Betrachten wir nun $[x]^2 + [y]^2 = [z]^2$ in $\mathbb{Z}_5$. In $\mathbb{Z}_5$ gibt es die Quadrate $[0] = [0]^2$, $[1] = [1]^1 = [4]^2$, $[4] = [2]^2 = [3]^2$ und wir wollen die Fälle $[x] \neq [0] \in \mathbb{Z}_5$ und $[x] = [0] \in \mathbb{Z}_5$ unterscheiden. Im zweiten Fall haben wir offensichtlich schon $5|xyz$ gezeigt. Im ersten Fall sind noch die Möglichkeiten $[x] \in \{[1], [4]\}$ und $[x] \in \{[2], [3]\}$ zu betrachten.
   - Sei $[x] \in \{[1], [4]\}$, dann haben wir die Möglichkeiten

     $$[y] \in \{[2], [3]\},\ [z] = [0] \text{ oder } [y] = [0],\ [z] \in \{[1], [4]\},$$

     in jedem Falle gilt also auch hier $[xyz] = [0] \in \mathbb{Z}_5$, das heißt $5|xyz$.
   - Ist $[x] \in \{[2], [3]\}$, so bleiben die Optionen

     $$[y] = [0],\ [z] \in \{[2], [3]\} \text{ oder } [y] \in \{[1], [4]\},\ [z] = 0,$$

     und wieder folgt $5|xyz$.

3. Es bleibt noch, $4|xyz$ zu zeigen. Betrachten wir die Gleichung $[x]^2 + [y]^2 = [z]^2$ in $\mathbb{Z}_2$, so erhalten wir die Möglichkeiten
   (i) $[x] = [y] = [z] = [0] \in \mathbb{Z}_2$,
   (ii) $[x] = [y] = [1] \in \mathbb{Z}_2$ und $[z] = [0] \in \mathbb{Z}_2$,
   (iii) $[x] = [1]$ und $[y] = 0$ (oder $[x] = [0]$ und $[y] = [1]$) und $[z] = [1]$.

   Im Fall (i) gilt offensichtlich $2^3|xyz$, insbesondere also $4|xyz$. Für die beiden letzten Punkte überlegen wir uns, dass es in $\mathbb{Z}_4$ die Quadrate $[0] = [0]^2 = [2]^2$ und $[1] = [1]^2 = [3]^2$ gibt. Im Fall (ii) wären also ungerade $x, y \in \mathbb{Z}$ und ein gerades $z \in \mathbb{Z}$ gesucht, so dass $[x]^2 + [y]^2 = [z]^2$ in $\mathbb{Z}_4$ gilt. Nun gilt aber

   $$x, y \text{ ungerade} \quad \Rightarrow \quad x, y \in \{[1], [3]\} \subset \mathbb{Z}_4 \quad \Rightarrow \quad [x]^2 = [1] = [y]^2 \in \mathbb{Z}_4,$$

und z gerade impliziert $[z]^2 = 0$, so dass der Fall (ii) ausgeschlossen ist. Im Fall (iii) nehmen wir ohne Einschränkung an, dass $[x] = [1]$ und $[y] = [0] \pmod 2$ gilt (der andere Fall funktioniert vollkommen analog), es sind also ungerade $x, z \in \mathbb{Z}$ und ein gerades $y \in \mathbb{Z}$ gesucht, so dass $[x]^2 + [y]^2 = [z]^2$ in $\mathbb{Z}_4$ gilt. Mit $[x], [z] \in \{[1], [3]\} \subset \mathbb{Z}_4$ erhalten wir diesmal $[y] \in \{[0], [2]\} \subset \mathbb{Z}_4$. Wir müssen also noch zeigen, dass wirklich bereits $[y] = [0] \in \mathbb{Z}_4$ folgt. Dazu bedenken wir, dass nach Voraussetzung ja $x^2 + y^2 = z^2$ gilt, also

$$y^2 = z^2 - x^2 = (z - x)(z + x)$$

für ungerade x, z. Da also $z - x$ und $z + x$ sicher beide gerade sind, genügt es, zu zeigen, dass gilt:

Für ungerade $z, x \in \mathbb{Z}$ gilt $[z + x] = [0] \in \mathbb{Z}_4$ oder $[z - x] = [0] \in \mathbb{Z}_4$.

Da ja aber x, z ungerade sind, gilt $[2z] = [2] \in \mathbb{Z}_4$, also

$$[2] = [2z] = [z + x] + [z - x],$$

was die Möglichkeit $[z + x] = [2] = [z - x]$ ausschließt. Somit haben wir $2^3 | y^2$ gezeigt, es muss also schon $2^2 | y$ (und damit im Nachhinein natürlich schon $2^4 | y^2$) gelten, also $4 | xyz$ wie gewünscht.

Bezeichnen wir nun mit $\pi\colon \mathbb{Z}_{60} \xrightarrow{\sim} \mathbb{Z}_3 \times \mathbb{Z}_4 \times \mathbb{Z}_5$ den kanonischen Isomorphismus aus dem chinesischen Restsatz, so haben wir also insgesamt gezeigt:

$$\pi([xyz]) = ([0], [0], [0]),$$

also $[xyz] = [0] \in \mathbb{Z}_{60}$, das heißt $60 | xyz$.