Aufgabe H12T3A4 (6 Punkte)

Wieviele Lösungen hat die Gleichung $x^2 + \overline{46}x + \bar{1} = \bar{0}$ in $\mathbb{Z}/2012\mathbb{Z}$? (503 ist eine Primzahl.)

Lösung:

Wegen $2012 = 4 \cdot 503$ und $\mathrm{ggT}(4, 503) = 1$ liefert der Chinesische Restsatz einen Isomorphismus von Ringen

$$\phi : \mathbb{Z}/2012\mathbb{Z} \to \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/503\mathbb{Z} \quad , \quad a + 2012\mathbb{Z} \mapsto (a + 4\mathbb{Z}, a + 503\mathbb{Z}).$$

Sei $\bar{a} \in \mathbb{Z}/2012\mathbb{Z}$ und $(\bar{b}, \bar{c}) = \phi(\bar{a})$. Wir zeigen, dass das Element $\bar{a}$ für das Polynom $f = x^2 + 46x + 1 \in \mathbb{Z}[x]$ genau dann die Gleichung $f(\bar{a}) = \bar{0}$ erfüllt, wenn $f(\bar{b}) = \bar{0}$ und $f(\bar{c}) = \bar{0}$ gilt. (Das Einsetzen von Elementen aus einem Restklassenring $\mathbb{Z}/m\mathbb{Z}$ in ein Polynom $g = \sum_{k=0}^{m} c_k x^k \in \mathbb{Z}[x]$ ist zulässig, wenn man für $\bar{a} \in \mathbb{Z}/m\mathbb{Z}$ unter $g(\bar{a})$ das Element $\sum_{k=0}^{m} c_k \cdot \bar{a}^k = \sum_{k=0}^{m} \bar{c}_k \bar{a}^k$ versteht.) Definieren wir nun für jedes $m \in \mathbb{N}$ jeweils

$$\mathcal{L}_m \quad = \quad \{\bar{u} \in \mathbb{Z}/m\mathbb{Z} \mid f(\bar{u}) = \bar{0}\} \quad ,$$

so folgt aus dieser Äquivalenzaussage, dass durch die Einschränkung von ϕ auf $\mathcal{L}_{2012}$ eine Bijektion zwischen $\mathcal{L}_{2012}$ und $\mathcal{L}_4 \times \mathcal{L}_{503}$ gegeben ist. Insbesondere gilt dann $|\mathcal{L}_{2012}| = |\mathcal{L}_4| \cdot |\mathcal{L}_{503}|$. Die behauptete Äquivalenz folgt nun aus der Rechnung

$$\begin{aligned}
f(\bar{a}) = \bar{0} \quad &\Leftrightarrow \quad \bar{a}^2 + 46 \cdot \bar{a} + \bar{1} = \bar{0} \quad \Leftrightarrow \quad \phi(\bar{a}^2 + 46 \cdot \bar{a} + \bar{1}) = \phi(\bar{0}) \\
\Leftrightarrow \quad \phi(\bar{a})^2 + 46 \cdot \phi(\bar{a}) + \phi(\bar{1}) = \phi(\bar{0}) \quad &\Leftrightarrow \quad (\bar{b}, \bar{c})^2 + 46 \cdot (\bar{b}, \bar{c}) + (\bar{1}, \bar{1}) = (\bar{0}, \bar{0}) \\
\Leftrightarrow \quad (\bar{b}, \bar{c})^2 + (\overline{46}\bar{b}, \overline{46}\bar{c}) + (\bar{1}, \bar{1}) = (\bar{0}, \bar{0}) \quad &\Leftrightarrow \quad (\bar{b}^2 + 46\bar{b} + \bar{1}, \bar{c}^2 + 46\bar{c} + \bar{1}) = (\bar{0}, \bar{0}) \\
\Leftrightarrow \quad \left(\bar{b}^2 + 46\bar{b} + \bar{1} = \bar{0}\right) \wedge (\bar{c}^2 + 46\bar{c} + \bar{1} = \bar{0}) \quad &\Leftrightarrow \quad f(\bar{b}) = \bar{0} \text{ und } f(\bar{c}) = \bar{0}
\end{aligned}$$

wobei im dritten Schritt verwendet wurde, dass ϕ bijektiv, und im vierten, dass ϕ ein Ringhomomorphismus ist.

Durch Einsetzen der Elemente $\bar{0}, \bar{1}, \bar{2}, \bar{3} \in \mathbb{Z}/4\mathbb{Z}$ in das Polynom f sieht man, dass $\mathcal{L}_4$ aus den Elementen $\bar{1}$ und $\bar{3}$ besteht, dass also $|\mathcal{L}_4| = 2$ ist. Für alle $\bar{c} \in \mathbb{Z}/503\mathbb{Z}$ gilt die Äquivalenz

$$\begin{aligned}
\bar{c} \in \mathcal{L}_{503} \quad &\Leftrightarrow \quad f(\bar{c}) = \bar{0} \quad \Leftrightarrow \quad \bar{c}^2 + 46\bar{c} + \bar{1} = \bar{0} \quad \Leftrightarrow \quad \bar{c}^2 + 2 \cdot 23 \cdot \bar{c} + \overline{23}^2 = \overline{23}^2 - \bar{1} \\
\Leftrightarrow \quad (\bar{c} + \overline{23})^2 = \overline{528} = \overline{25} = \bar{5}^2 \quad &\Leftrightarrow \quad (\bar{c} + \overline{23})^2 - \bar{5}^2 = \bar{0} \quad \Leftrightarrow \quad (\bar{c} + \overline{23} + \bar{5})(\bar{c} + \overline{23} - \bar{5}) = \bar{0} \\
&\Leftrightarrow \quad (\bar{c} + \overline{28})(\bar{c} + \overline{18}) = \bar{0} \quad \Leftrightarrow \quad \bar{c} \in \{-\overline{18}, -\overline{28}\}
\end{aligned}$$

also $\mathcal{L}_{503} = \{-\overline{18}, -\overline{28}\}$ und $|\mathcal{L}_{503}| = 2$. Insgesamt ist die Anzahl der Lösungen von $f(\bar{a}) = \bar{0}$ in $\mathbb{Z}/2012\mathbb{Z}$ also gegeben durch $|\mathcal{L}_{2012}| = |\mathcal{L}_4| \cdot |\mathcal{L}_{503}| = 2 \cdot 2 = 4$.