Aufgabe F12T1A4 (6 Punkte)

Gegeben ist das Polynom $f = x^2 + 3x + 1 \in \mathbb{Z}[x]$. Bestimmen Sie

(a) die Nullstellen von f modulo 5,

(b) die Nullstellen von f modulo 11,

(c) die Nullstellen von f modulo 11^2,

(d) die Nullstellen von f modulo 605.

Lösung:

zu (a) Durch Einsetzen der Elemente $\bar{0}, \bar{1}, ..., \bar{4} \in \mathbb{Z}/5\mathbb{Z}$ sieht man, dass $\bar{1}$ die einzige Nullstelle von f in $\mathbb{Z}/5\mathbb{Z}$ ist.

zu (b) Einsetzen von $\bar{0}, \bar{1}, ..., \bar{9}, \overline{10} \in \mathbb{Z}/11\mathbb{Z}$ zeigt, dass $\bar{2}$ und $\bar{6}$ die einzigen beiden Nullstellen von f in $\mathbb{Z}/11\mathbb{Z}$ sind.

zu (c) Ist $a + 121\mathbb{Z}$ eine Nullstelle von f in $\mathbb{Z}/121\mathbb{Z}$, dann ist $a + 11\mathbb{Z}$ eine Nullstelle von f in $\mathbb{Z}/11\mathbb{Z}$. Denn $f(a + 121\mathbb{Z}) = \bar{0}$ in $\mathbb{Z}/121\mathbb{Z}$ ist gleichbedeutend mit $f(a) \equiv 0 \bmod 121$, Aus $f(a) \equiv 0 \bmod 121$ folgt $f(a) \equiv 0 \bmod 11$, und dies wiederum ist gleichbedeutend mit $f(a+11\mathbb{Z}) = \bar{0}$ in $\mathbb{Z}/11\mathbb{Z}$. Nachh Teil (b) gilt $f(a+11\mathbb{Z}) = \bar{0}$ nur, falls $a + 11\mathbb{Z} = 2 + 11\mathbb{Z}$ oder $a + 11\mathbb{Z} = 6 + 11\mathbb{Z}$ ist, wenn also $a \equiv 2 \bmod 11$ oder $a \equiv 6 \bmod 11$ gilt. Dies bedeutet, dass ein $k \in \mathbb{Z}$ mit $a = 2 + 11k$ oder $a = 6 + 11k$ existiert.

Wir überprüfen nun, unter welcher Bedingung $2 + 11k + 121\mathbb{Z}$ eine Nullstelle von f ist. Es gilt die Äquivalenz

$$f(2 + 11k + 121\mathbb{Z}) = \bar{0} \quad \Leftrightarrow \quad f(2 + 11k) \equiv 0 \bmod 121 \quad \Leftrightarrow \quad (2 + 11k)^2 + 3(2 + 11k) + 1 \equiv 0 \bmod 121$$

$$\Leftrightarrow \quad 4 + 44k + 121k^2 + 6 + 33k + 1 \equiv 0 \bmod 121 \quad \Leftrightarrow \quad 11 + 77k \equiv 0 \bmod 121 \quad \Leftrightarrow$$

$$77k \equiv -11 \bmod 121 \quad \Leftrightarrow \quad 7k \equiv -1 \bmod 11 \quad \overset{(*)}{\Leftrightarrow} \quad k \equiv 3 \bmod 11 \quad \Leftrightarrow \quad \exists\, \ell \in \mathbb{Z} : k = 3 + 11\ell$$

$$\Leftrightarrow \quad \exists\, \ell \in \mathbb{Z} : 2 + 11k + 121\mathbb{Z} = 2 + 11(3 + 11\ell) + 121\mathbb{Z} \quad \Leftrightarrow \quad 2 + 11k + 121\mathbb{Z} = 35 + 121\mathbb{Z}$$

wobei der Umformungsschritt (*) durch die Rechnung $\bar{7}\bar{k} = -\bar{1} \Rightarrow \bar{k} = \bar{7}^{-1}(-\bar{1}) = \bar{8} \cdot (-\bar{1}) = -\bar{8} = \bar{3}$ in $\mathbb{Z}/11\mathbb{Z}$ zu Stande kommt.

Durch eine analoge Rechnung überprüfen wir, wann $6 + 11k + 121\mathbb{Z}$ eine Nullstelle von f ist. Es gilt

$$f(6 + 11k + 121\mathbb{Z}) = \bar{0} \quad \Leftrightarrow \quad f(6 + 11k) \equiv 0 \bmod 121 \quad \Leftrightarrow \quad (6 + 11k)^2 + 3(6 + 11k) + 1 \equiv 0 \bmod 121$$

$$\Leftrightarrow \quad 36 + 132k + 121k^2 + 18 + 33k + 1 \equiv 0 \bmod 121 \quad \Leftrightarrow \quad 55 + 165k \equiv 0 \bmod 121 \quad \Leftrightarrow$$

$$165k \equiv -55 \bmod 121 \quad \Leftrightarrow \quad 15k \equiv -5 \bmod 11 \quad \Leftrightarrow \quad 4k \equiv -5 \bmod 11 \quad \overset{(*)}{\Leftrightarrow} \quad k \equiv 7 \bmod 11$$

$$\Leftrightarrow \quad \exists\, \ell \in \mathbb{Z} : k = 7 + 11\ell \quad \Leftrightarrow \quad \exists\, \ell \in \mathbb{Z} : 6 + 11k + 121\mathbb{Z} = 6 + 11(7 + 11\ell) + 121\mathbb{Z}$$

$$\Leftrightarrow \quad 6 + 11k + 121\mathbb{Z} = 83 + 121\mathbb{Z}$$

wobei an der Stelle (*) $\bar{4}\bar{k} = -\bar{5} \Rightarrow \bar{k} = \bar{4}^{-1}(-\bar{5}) = \bar{3} \cdot (-\bar{5}) = -\overline{15} = -\bar{4} = \bar{7}$ verwendet wurde. Insgesamt haben wir damit gezeigt, dass $\overline{35}$ und $\overline{83}$ die einzigen Nullstellen von f in $\mathbb{Z}/121\mathbb{Z}$ sind.

zu (d) Wegen $605 = 5 \cdot 121$ und $\mathrm{ggT}(5, 121) = 1$ existiert nach dem Chinesischen Restsatz ein Isomorphismus $\phi : \mathbb{Z}/605\mathbb{Z} \to \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/121\mathbb{Z}$ von Ringen mit $\phi(a + 605\mathbb{Z}) = (a + 5\mathbb{Z}, a + 121\mathbb{Z})$ für alle $a \in \mathbb{Z}$. Sei $\bar{a} \in \mathbb{Z}/605\mathbb{Z}$ und $(\bar{b}, \bar{c}) = \phi(\bar{a})$. Genau dann ist $\bar{a}$ eine Nullstelle von f, wenn $\bar{b}$ und $\bar{c}$ Nullstellen von f sind, denn weil ϕ eine Bijektion und ein Ringhomomorphismus ist, gilt die Äquivalenz

$$\begin{aligned} f(\bar{a}) = \bar{0} \quad &\Leftrightarrow \quad \phi(f(\bar{a})) = \phi(\bar{0}) \quad \Leftrightarrow \quad \phi(\bar{a}^2 + 3\bar{a} + \bar{1}) = (\bar{0}, \bar{0}) \quad \Leftrightarrow \quad \phi(\bar{a})^2 + 3\phi(\bar{a}) + \phi(\bar{1}) = (\bar{0}, \bar{0}) \\ &\Leftrightarrow \quad (\bar{b}, \bar{c})^2 + 3(\bar{b}, \bar{c}) + (\bar{1}, \bar{1}) = (\bar{0}, \bar{0}) \quad \Leftrightarrow \quad (\bar{b}^2 + 3\bar{b} + \bar{1}, \bar{c}^2 + 3\bar{c} + \bar{1}) = (\bar{0}, \bar{0}) \\ &\Leftrightarrow \quad \bar{b}^2 + 3\bar{b} + \bar{1} = \bar{0} \text{ und } \bar{c}^2 + 3\bar{c} + \bar{1} = \bar{0} \quad \Leftrightarrow \quad f(\bar{b}) = \bar{0} \text{ und } f(\bar{c}) = \bar{0}. \end{aligned}$$

Nach Teil (a) und Teil (c) ist $f(\bar{b}) = \bar{0} \wedge f(\bar{c}) = \bar{0}$ äquivalent zu $(\bar{b}, \bar{c}) \in \{(\bar{1}, \overline{35}), (\bar{1}, \overline{83})\}$. Die beiden einzigen Nullstellen von f in $\mathbb{Z}/605\mathbb{Z}$ sind also $\phi^{-1}(\bar{1}, \overline{35})$ und $\phi^{-1}(\bar{1}, \overline{83})$. Wir bestimmen diese beiden Urbilder mit dem bekannten Verfahren. Wegen $\mathrm{ggT}(5, 121) = 1$ besitzt die Gleichung $5k + 121\ell = 1$ eine Lösung, zum Beispiel mit $k = -20$ und $\ell = 1$. Durch Umstellen dieser Gleichung zu $121 \cdot 1 = 1 + 5 \cdot 20$ sieht man $\phi(\overline{121}) = (\bar{1}, \bar{0})$. Durch $1 - 121 \cdot 1 = 5 \cdot 20$ findet man entsprechend $\phi(-\overline{120}) = (\bar{0}, \bar{1})$. Ein Urbild von $(\bar{1}, \overline{35}) = 1 \cdot (\bar{1}, \bar{0}) + 35 \cdot (\bar{0}, \bar{1})$ in $\mathbb{Z}/605\mathbb{Z}$ ist damit gegeben durch $1 \cdot \overline{121} + 35 \cdot (-\overline{120}) = -\overline{4079} = \overline{156}$, und ein Urbild von $(\bar{1}, \overline{83}) = 1 \cdot (\bar{1}, \bar{0}) + 83 \cdot (\bar{0}, \bar{1})$ erhält man durch $1 \cdot \overline{121} + 83 \cdot (-\overline{120}) = -\overline{9839} = \overline{446}$. Also sind $\overline{156}$ und $\overline{446}$ die einzigen Nullstellen von f in $\mathbb{Z}/605\mathbb{Z}$.