F12-T1-A4

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

a) die Nullstellen von P mod 5,

b) die Nullstellen von P mod 11,

c) die Nullstellen von P mod 11^2,

d) die Nullstellen von P mod 605.

Lösungsvorschlag. a) $P(0) = 1$, $P(1) \equiv 0 \mod 5$, $P(2) = 4 + 6 + 1 \equiv 1 \mod 5$, $P(3) = 9 + 9 + 1 \equiv 4 \mod 5$, $P(4) \equiv 1 - 3 + 1 \equiv 4 \mod 5$. Die einzige Nullstelle mod 5 ist also 1.
b) Unter Auslassung einiger bereits aus a) bekannter Fälle testen wir: $P(2) \equiv 0$ (aus a)), $P(4) = 16 + 12 + 1 \equiv 5 + 1 + 1 = 7$, $P(5) = 25 + 15 + 1 \equiv 3 + 4 + 1 = 8$, $P(6) = 36 + 18 + 1 \equiv 3 + 7 + 1 \equiv 0$. Damit haben wir zwei Nullstellen gefunden und weitere Tests erübrigen sich, das ein Polynom über dem Körper $\mathbb{F}_{11}$, welches nicht das Nullpolynom ist, höchstens zwei verschiedene Nullstellen besitzen kann. Die Nullstellen mod 11 sind also 2 und 6.
c) Da eine Nullstelle mod 11^2 insbesondere eine Nullstelle mod 11 ist, muss für eine Nullstelle a von P mod 11^2 also gelten

$$a \in \{2 + k \cdot 11 \ : \ k = 0, \dots, 10\} \cup \{6 + l \cdot 11 \ : \ l = 0, \dots, 10\}.$$

Wir berechnen

$$\begin{aligned} P(2 + k \cdot 11) &= (2 + k \cdot 11)^2 + 3 \cdot (2 + k \cdot 11) + 1 = \\ &= P(2) + 4k \cdot 11 + k^2 \cdot 11^2 + 3 \cdot k \cdot 11 \equiv (1 + 7 \cdot k) \cdot 11 \mod 11^2 \end{aligned}$$

und analog

$$\begin{aligned} P(6 + l \cdot 11) &= P(6) + 12 \cdot l \cdot 11 + l^2 \cdot 11^2 + 3 \cdot l \cdot 11 = \\ &= (5 + 15 \cdot l) \cdot 11 + l^2 \cdot 11^2 \equiv (5 + 4 \cdot l) \cdot 11 \mod 11^2. \end{aligned}$$

Es soll also gelten $1 + 7k \equiv 0 \mod 11$ und $5 + 9l \equiv 0 \mod 11$. Mit $7^{-1} = 8$ und $4^{-1} = 3$ in $\mathbb{F}_{11}$ ist dies äquivalent zu $k \equiv -8 \equiv 3 \mod 11$ und $l \equiv -15 \equiv 7 \mod 11$. Die Nullstellen mod 11^2 sind also $2 + 3 \cdot 11 = 35$ und $6 + 7 \cdot 11 = 83$.
d) Es ist $605 = 5 \cdot 11^2$ und nach dem chinesischen Restsatz ist die kanonische Abbildung

$$\begin{aligned} \pi \colon \mathbb{Z}_{605} &\to \mathbb{Z}_5 \times \mathbb{Z}_{11^2} \\ x &\mapsto (x, x) \end{aligned}$$

ein Isomorphismus von Ringen. Insbesondere gilt also $\pi(P(x)) = P(\pi(x)) = (P(x), P(x))$ und $x \in \mathbb{Z}_{605}$ ist eine Nullstelle von P genau dann, wenn $x \in \mathbb{Z}_5$ und $x \in \mathbb{Z}_{11^2}$ Nullstellen von P sind. Nach a) und c) sind die Nullstellen von P in $\mathbb{Z}_{605}$ also $\pi^{-1}((1, 35))$ und

$\pi^{-1}((1,84))$. Um diese Elemente genauer anzugeben müssen wir die Umkehrabbildung von π bestimmen, welche bekanntlich durch

$$(x,y) \mapsto x \cdot e_1 + y \cdot e_2$$

gegeben ist für Elemente e_1, e_2 mit $\pi(e_1) = (1,0)$ und $\pi(e_2) = (0,1)$. Wir finden $e_1 = 121$ und $e_2 = 485$ und erhalten als Nullstellen $1 \cdot 121 + 25 \cdot 485 \equiv 156 \mod 605$ und $1 \cdot 121 + 83 \cdot 485 \equiv 446 \mod 605$.