Aufgabe H16T2A5 (10 Punkte)

Sei p eine Primzahl. Wir betrachten in $\mathbb{F}_p[x]$ die Polynome $g_1 = x^2 + x + \bar{1}$ und $g_2 = x^3 + x^2 + x + \bar{1}$. Bestimmen Sie die Lösungsmenge $L \subseteq \mathbb{F}_p[x]$ des Kongruenzsystems

$$f \equiv x - \bar{1} \bmod g_1 \qquad \text{und} \qquad f \equiv \bar{1} \bmod g_2 \ , \ f \in \mathbb{F}_p[x].$$

Lösung:

Zunächst bestimmen wir mit dem Euklidischen Algorithmus den größten gemeinsamen Teiler d von g_1, g_2 sowie Polynome $h_1, h_2 \in \mathbb{F}_p[x]$ mit $h_1 g_1 + h_2 g_2 = d$.

q	a_n	x_n	y_n
$-$	$x^3 + x^2 + x + \bar{1}$	$\bar{1}$	$\bar{0}$
$-$	$x^2 + x + 1$	$\bar{0}$	$\bar{1}$
x	$\bar{1}$	$\bar{1}$	$-x$
$x^2 + x + 1$	$\bar{0}$	$-$	$-$

An der vorletzten Zeile kann abgelesen werden, dass $d = \bar{1}$ und die Gleichung $h_1 g_1 + h_2 g_2 = \bar{1}$ mit $h_2 = \bar{1}$ und $h_1 = -x$ erfüllt ist.

Die Gleichung $(-x)g_1 + 1 \cdot g_2 = \bar{1}$ kann umgestellt werden zu $1 \cdot g_2 = 1 + x g_1$. Dies zeigt, dass das Polynom $k_1 = 1 \cdot g_2 = x^3 + x^2 + x + 1$ die Kongruenzen $k_1 \equiv \bar{1} \bmod g_1$ und $k_1 \equiv \bar{0} \bmod g_2$ erfüllt. Ebenso können wir die Ausgangsgleichung auch umstellen zu $(-x)g_1 = \bar{1} - 1 \cdot g_2$. Dies zeigt, dass $k_2 = (-x)g_1 = -x^3 - x^2 - x$ eine Lösung des Kongrenzsystems $k_2 \equiv \bar{0} \bmod g_1$ und $k_2 \equiv \bar{1} \bmod g_2$ darstellt. Definieren wir nun $k = (x - \bar{1}) \cdot k_1 + \bar{1} \cdot k_2 = (x - \bar{1})(x^3 + x^2 + x + \bar{1}) + (-x_3 - x^2 - x) = x^4 - x^3 - x^2 - x - \bar{1}$, dann gilt

$$k \equiv (x - \bar{1}) \cdot k_1 + \bar{1} \cdot k_2 \equiv (x - \bar{1}) \cdot \bar{1} + \bar{1} \cdot \bar{0} \equiv x - \bar{1} \bmod g_1$$

und

$$k \equiv (x - \bar{1}) \cdot k_1 + \bar{1} \cdot k_2 \equiv (x - \bar{1}) \cdot \bar{0} + \bar{1} \cdot \bar{1} \equiv \bar{1} \bmod g_2.$$

Also ist k *ein* Element der Lösungsmenge L des in der Aufgabenstellung angegebenen Kongrenzsystems. Wir zeigen nun, dass $L = k + (g_1 g_2)$ gilt, wobei $(g_1 g_2)$ das von $g_1 g_2$ im Ring $\mathbb{F}_p[x]$ erzeugte Hauptideal bezeichnet. Nach dem Chinesischen Restsatz existiert ein Isomorphismus $\phi : \mathbb{F}_p[x]/(g_1 g_2) \to \mathbb{F}_p[x]/(g_1) \times \mathbb{F}_p[x]/(g_2)$ von Ringen mit $\phi(f + (g_1 g_2)) = (f + (g_1), f + (g_2))$ für alle $f \in \mathbb{F}_p[x]$. Aus $k \equiv x - \bar{1} \bmod k_1$ und $k \equiv \bar{1} \bmod k_2$ folgt $\phi(k + (g_1 g_2)) = (k + (g_1), k + (g_2)) = (x - \bar{1} + (g_1), \bar{1} + (g_2))$. Für alle $f \in \mathbb{F}_p[x]$ gilt nun die Äquivalenz

$$f \in L \quad \Leftrightarrow \quad f \equiv x - \bar{1} \bmod g_1 \text{ und } f \equiv \bar{1} \bmod g_2 \quad \Leftrightarrow$$

$$(f + (g_1), f + (g_2)) = (x - \bar{1} + (g_1), \bar{1} + (g_2)) \quad \Leftrightarrow \quad \phi(f + (g_1 g_2)) = \phi(k + (g_1 g_2)) \quad \Leftrightarrow$$

$$f + (g_1 g_2) = k + (g_1 g_2) \quad \Leftrightarrow \quad f \in k + (g_1 g_2).$$

Dabei wurde im vierten Schritt verwendet, dass ϕ eine Bijektion ist. Damit ist die Gleichung $k + (g_1 g_2)$ bewiesen.