Hausaufgaben

Eric Kunze
Matr.-Nr. 4679202

Mathematische Methoden – Übungsblatt 6

Seien $f_1(x) = x^4 + x + 1$ und $f_2(x) = x^4 + x^3 + x^2 + x + 1$ über $\mathbb{Z}_2$ gegeben.

(zu a) Es gilt

$$\begin{aligned}
x^1 &\equiv x^1 && \mod f_1(x) \\
x^2 &\equiv x^2 && \mod f_1(x) \\
x^3 &\equiv x^2 && \mod f_1(x) \\
x^4 &\equiv x + 1 && \mod f_1(x) \\
x^5 &\equiv x^2 + x && \mod f_1(x) \\
x^6 &\equiv x^3 + x^2 && \mod f_1(x) \\
x^7 &\equiv x^3 + x + 1 && \mod f_1(x) \\
x^8 &\equiv x^2 + 1 && \mod f_1(x)
\end{aligned}
\qquad
\begin{aligned}
x^9 &\equiv x^3 + x && \mod f_1(x) \\
x^{10} &\equiv x^2 + x + 1 && \mod f_1(x) \\
x^{11} &\equiv x^3 + x^2 + x && \mod f_1(x) \\
x^{12} &\equiv x^3 + x^2 + x + 1 && \mod f_1(x) \\
x^{13} &\equiv x^3 + x^2 + 1 && \mod f_1(x) \\
x^{14} &\equiv x^3 + 1 && \mod f_1(x) \\
x^{15} &\equiv 1 && \mod f_1(x)
\end{aligned}$$

Damit ist $\min\left\{\ell \in \mathbb{N} \setminus \{0\} : x^\ell \equiv 1 \mod f_1(x)\right\} = 15 = 2^4 - 1$ und f_1 also primitv.

Weiter gilt

$$\begin{aligned}
x^1 &\equiv x^1 && \mod f_2(x) \\
x^2 &\equiv x^2 && \mod f_2(x) \\
x^3 &\equiv x^3 && \mod f_2(x)
\end{aligned}
\qquad
\begin{aligned}
x^4 &\equiv x^3 + x^2 + x + 1 && \mod f_2(x) \\
x^5 &\equiv 1 && \mod f_2(x)
\end{aligned}$$

Damit ist $\min\left\{\ell \in \mathbb{N} \setminus \{0\} : x^\ell \equiv 1 \mod f_1(x)\right\} = 5 \neq 2^4 - 1$ und f_2 also nicht primitv.

(zu b) Es ist

$$(x^8)^{-1} \equiv x^{-8} \equiv x^{15-8} \equiv x^7 \equiv x^3 + x + 1 \mod f_1(x)$$

und $(x^3 + x)^{-1} \equiv (x^9)^{-1} \equiv x^6 \mod f_1(x)$, was uns schließlich

$$(x^2 + x + 1)(x^3 + x)^{-1} \equiv x^{10}x^6 \equiv x^{16} \equiv x^{15}x \equiv x \mod f_1(x).$$

Für f_2 ist

$$(x^8)^{-1} \equiv x^{-8} \equiv x^{-3} \equiv x^2 \mod f_2(x)$$

und $(x^3 + x)^{-1}$ erhalten wir mit dem erweiterten euklidischen Algorithmus als $x + 1$, denn $(x^3 + x)(x + 1) = x^4 + x^2 + x^3 + x \equiv 1 \mod f_2(x)$. Somit ist

$$(x^2+x+1)(x^3+x)^{-1} \equiv (x^2+x+1)(x+1) \equiv x^3+x^2+x+x^2+x+1 \equiv x^3+1 \mod f_2(x)$$