Übung 10 Aufgabe 1 Lösung

a) Sei $f(x) = 1+x^2+x^3+x^6+x^7+x^9+x^{11} \in \mathbb{Z}_2[x]$. Um f in quadratfreie Faktoren zu zerlegen, verwenden wir die formale Ableitung $f'(x) = x^2 + x^6 + x^8 + x^{10}$ von $f(x)$ und berechnen mit Hilfe des euklidschen Algorithmus $\gcd(f, f') = 1 + x^2 + x^6$. Insbesondere ist f nicht quadratfrei. Wir schreiben

$$f(x) = \frac{f(x)}{\gcd(f, f')} \cdot \gcd(f, f') = (1 + x^3 + x^5) \cdot (1 + x^2 + x^6).$$

Bleibt zu prüfen, ob $h(x) := \gcd(f, f')$ quadratfrei ist oder nicht. Die formale Ableitung von h ist $h'(x) = 0$. D.h. $h(x)$ ist von der Form $h(x) = g(x^2) = g(x)^2$ (Frobeniushomomorphismus!) mit $g(x) = 1 + x + x^3$. Für g berechnen wir $\gcd(g, g') = 1$, somit ist $g(x)$ quadratfrei. Es folgt die Zerlegung von f in quadratfreie Faktoren:

$$f(x) = (1 + x^3 + x^5) \cdot (1 + x + x^3)^2.$$

b) Sei $f(x) = 1+x+x^4+x^5+x^8 \in \mathbb{Z}_2[x]$ und $n := \deg(f) = 8$. Wegen $\gcd(f, f') = 1$ ist $f(x)$ quadratfrei. Wir verwenden nun den Algorithmus aus der Vorlesung.

$$\textit{Berechne die Matrix } (\beta_{ik}) \in \mathbb{Z}_2^{n\times n} \textit{ mit } x^{2k} = \textstyle\sum_{i=0}^{n-1} \beta_{ik}\, x^i \mod f(x)$$

Dies kann mit einfacher Polynomdivision durchgeführt werden. Wir berechnen die Matrix:

	1	x^2	x^4	x^6	x^8	x^{10}	x^{12}	x^{14}
1	1	0	0	0	1	0	1	1
x	0	0	0	0	1	0	0	1
x^2	0	1	0	0	0	1	1	1
x^3	0	0	0	0	0	1	0	0
x^4	0	0	1	0	1	0	0	0
x^5	0	0	0	0	1	0	1	1
x^6	0	0	0	1	0	1	1	0
x^7	0	0	0	0	0	1	0	1

(Am Rand sind für die Spalten die x^{2k} und für die Zeilen eine Basis von $Z_2[X]/(f)$ eingetragen.)

Berechne eine $\mathbb{Z}_2$-Basis von $B = \ker((\beta_{ik} - I_{n\times n})$.

Mittels Gauss-Elimination berechnen wir $B = \text{Span}\{(0,1,0,0,1,0,1,0)^T, (1,0,0,0,0,0,0,0)^T\}$.
$\rightarrow$ Ausgabe: $t = \dim_{Z_2}(B) = 2$.

Falls $t > 1$, finde Basiselement $a \notin \mathbb{Z}_2$ und berechne für $s = 0, 1$ $d = \gcd(a - s, f)$ bis $d \neq 1$.

Wir schreiben zunächst der Übersicht halber die Basiselemente von B als Polynome:

$$B = \text{Span}\{x + x^4 + x^6, 1\}.$$

Offenbar ist $x+x^4+x^6 \notin \mathbb{Z}_2$. Wir berechnen $d = \gcd(x+x^4+x^6, f(x)) = 1+x^3+x^5$.
$\rightarrow$ Ausgabe: $f = d \cdot \frac{f}{d} = (1 + x^3 + x^5) \cdot (1 + x + x^3)$.