Prof. C. P. Schnorr Sommersemester 2006

Diskrete Mathematik

Blatt 9, 16.06.2006, Abgabe 23.06.2006

Definiere zu $f = \sum_i a_i x^i \in \mathbf{Z}[x]$, $\mathrm{cont}(f) := \mathrm{ggT}(a_i \mid i)$.

Aufgabe 1. Zeige für $f, g \in \mathbf{Z}[x]$:

a) $\mathrm{cont}(f), \mathrm{cont}(g) = 1 \;\Rightarrow\; \mathrm{cont}(fg) = 1$

b) $\mathrm{cont}(f \cdot g) = \mathrm{cont}(f) \cdot \mathrm{cont}(g)$.

Aufgabe 2. Zeige für $f \in \mathbf{Z}[x]$:

a) f irred. in $\mathbf{Z}[x] \Leftrightarrow (f$ irred. in $\mathbf{Q}[x], \mathrm{cont}(f) = 1)$.

b) f irred. in $\mathbf{Z}[x] \Rightarrow f$ prim in $\mathbf{Z}[x]$. (Damit ist $\mathbf{Z}[x]$ faktoriell.)

Aufgabe 3. Sei $C \subset \mathbf{F}_q^n \cong \mathbf{F}_q[x]/(x^n - 1)$ zyklischer Code mit Generatorpolynom $g(x) \in \mathbf{F}_q[x]$ und $x^n - 1 = g(x) \cdot h(x)$ mit $h = h_0 + \cdots + h_k x^k$, $h_k \neq 0$. Zeige C hat die PCH–Matrix

$$H = \begin{pmatrix} h_k & \cdots & h_0 & & \\ & \ddots & & \ddots & O \\ O & & h_k & \cdots & h_0 \end{pmatrix} \in \mathbf{F}_q^{(n-k)\times n}$$

Aufgabe 4. Seien C, g, h wie in Aufgabe 3.

1. Gebe ein Schieberegister $\mathcal{S}$ an, welches zur Eingabe $(a_0, \ldots, a_{n-1}) \in \mathbf{Z}_q^n$ prüft, ob $(a_0, \ldots, a_{n-1}) \in C$.

2. Erläutere die Ausgabe von $\mathcal{S}$ pro Takt.

Hinweis: $a(x) \sim (a_0, \ldots, a_{n-1}) \in C \Leftrightarrow h(x) \cdot a(x) = 0 \bmod (x^n - 1)$.

(6 Punkte pro Aufgabe)