Ludwig-Maximilans-
Universität München
Dr. Pascal Reisert

Wintersemester 2018/2019
Übungsblatt 4
7. November 2018

# Übungen zur Kryptographie
# Lösung

## Aufgabe 14

a) i) Angenommen $a_0 = 0$, dann gilt $F(X) = X \cdot \sum_{\nu=0}^{n-1} a_{\nu+1} X^\nu$ nicht irreduzibel.

ii) Angenommen $a_{i_1}, \ldots, a_{i_{2m}} = 1$ für $i_1 < \ldots < i_{2m}$ und $m \in \mathbb{N}$, dann gilt

$$F(X) = (X+1) \sum_{k=1}^{m} (X^{i_{2k}-1} + \ldots + X^{i_{2k-1}}).$$

Alternativ erkennt man leicht, dass 1 bei gerader Anzahl nicht-verschwindender Komponenten eine Nullstelle ist - dies genügt.[1]

iii) Angenommen $G(X) = \sum_{\nu=0}^{n} a_\nu X^{n-\nu} = P(X)Q(X)$ mit $P(X) = \sum_{\nu=0}^{r} b_\nu X^\nu$, $Q(X) = \sum_{\nu=0}^{s} c_\nu X^\nu$ und $r+s=n$. Man beachte $a_{n-\nu} = \sum_{k=0}^{n} b_k c_{\nu-k} \Rightarrow a_\nu = \sum_{k=0}^{n} b_k c_{n-\nu-k}$, wobei wir durch Nullkoeffizienten ergänzen. Dann gilt für $P'(X) = \sum_{\nu=0}^{r} b'_\nu X^\nu, Q'(X) = \sum_{\nu=0}^{s} c'_\nu X^\nu$ mit $b'_\nu = b_{r-\nu},\ c'_\nu = c_{s-\nu},\ 1 \leq \nu \leq n$

$$P(X)Q(X) = \sum_{\nu=0}^{n} a'_\nu X^\nu$$

mit $a'_\nu = \sum_{k=0}^{n} b'_k c'_{\nu-k}$. Setzen wir die Definition ein, so folgt

$$a'_\nu = \sum_{k=0}^{n} b_{r-k} c_{s-(\nu-k)} = \sum_{k=0}^{n} b_k c_{s-(\nu-(r-k))} = \sum_{k=0}^{n} b_k c_{n-\nu-k} = a_\nu.$$

Damit ist $F(X) = P'(X)Q'(X)$ ebenfalls nicht irreduzibel.

*Bemerkung.* Der folgende elegante Beweis wurde in der Zentralübung vorgeschlagen: Es gilt $\mathbb{F}_2[X] \subset \mathbb{F}_2(X)$ Quotientenkörper. Nun können wir in $\mathbb{F}_2(X)$ rechnen: $G(X) = P(X)Q(X)$ impliziert

$$F(X) = X^n G\left(\frac{1}{X}\right) = X^n P\left(\frac{1}{X}\right) Q\left(\frac{1}{X}\right) = \underbrace{X^{\deg P} P\left(\frac{1}{X}\right)}_{P'(X)} \underbrace{X^{\deg Q} Q\left(\frac{1}{X}\right)}_{Q'(X)}.$$

Da $P'(X), Q'(X) \in \mathbb{F}_2[X]$ haben wir eine Zerlegung gefunden und $F(X)$ ist nicht irreduzibel.

[1] Studentischer Beweis aus der Zentralübung.

**Aufgabe 16**

a) Wegen $\varphi(X)\cdot F(X) \in (F(X))$ ist die Abbildung nach dem Homomorphiesatz wohldefiniert und offensichtlich linear.
Wir ergänzen die $a_i$ trivial für $1 \leq i \leq m-1$. Man beachte, dass

$$\begin{aligned}
\varphi(X)X^k \mod F(X) &= \sum_{i=0}^{m-1} a_i X^{i+k} \mod F(X) = \sum_{i=0}^{m-1-k} a_i X^{i+k} + \sum_{i=m-k}^{m-1} a_i X^{i+k} \mod F(X) \\
&= \sum_{i=0}^{m-1-k} a_i X^{i+k} + \sum_{i=m-k}^{m-1} a_i X^{i+k} - \sum_{i=m-k}^{m-1} a_i X^{i-m+k} F(X) \mod F(X) \\
&= \sum_{i=0}^{m-1-k} a_i X^{i+k} + \sum_{i=m-k}^{m-1} a_i X^{i-m+k} \mod F(X) \\
&= \sum_{i=0}^{k-1} a_{i+m-k} X^i + \sum_{i=k}^{m-1} a_{i-k} X^i \mod F(X)
\end{aligned}$$

Entsprechend ergibt sich die Matrix $A_\varphi = (a_{ik})_{1\leq i,k \leq m-1}$ mit $a_{ik} = \begin{cases} a_{i+m-k}, & \text{für } i < k \\ a_{i-k} & \text{für } i \geq k \end{cases}$.

b) Die darstellende Matrix ist genau dann invertierbar, wenn die lineare Abbildung invertierbar ist. Die Abbildung ist genau dann invertierbar, wenn es ein $\mu_\psi$ gibt mit $\mu_\psi \mu_\varphi = \mathrm{id}_R$. Man beachte $\mu_\varphi(X^k P) = X^k \mu_\varphi(P)$ für alle $P \in R$ und damit $\mu_\varphi \mu_\psi(X^k) = X^k = X^k \mu_\varphi \mu_\psi(1) = \mu_\varphi(X^k \mu_\psi(1)) \Rightarrow \mu_\psi(X^k) = X^k \mu_\psi(1)$ für alle $k$. Also ist $\mu_\psi$ die Multiplikation mit einem $\psi \in K[X]$. Es muss also gelten $\psi\varphi \equiv 1$ bzw. $\psi\varphi + GF = 1$ für ein $G \in K(X)$. Letzteres ist nach dem Lemma von Bézout äquivalent zu $\mathrm{ggT}(\varphi, F) = 1$. Wiederum aus der Linearen Algebra wissen wir, dass das Inverse der darstellenden Matrix die darstellende Matrix der inversen Abbildung ist - also $A_\varphi^{-1} = A_\psi$.