TECHNISCHE UNIVERSITÄT DRESDEN

Fachrichtung Mathematik · **Institut für Algebra** · Modul Math Ma ANGALG WiSe 2016/17

Dr. Jens Zumbrägel 17. Nov. 2016

3. Übungsblatt zur Angewandten Algebra

Polynome, schnelle Arithmetik

1. Sei K ein Körper. Für $d \in \mathbb{N}$ sei $P_d := \{f \in K[X] \mid \deg f < d\}$. Seien $f, g \in K[X]$ mit $\deg f = n$, $\deg g = m$. Betrachte die K-lineare Abbildung

$$\varphi : P_m \times P_n \to P_{n+m}\,, \quad (s,t) \mapsto sf + tg\,.$$

   Zeige: Es ist $\mathrm{ggT}(f,g) = 1$ genau dann, wenn φ ein Isomorphismus ist.
   Wie sieht die Matrix von φ bezüglich der Standardbasis $(X^i)_{0 \le i < d}$ von P_d aus? (Deren Determinante wird als *Resultante* $\mathrm{Res}(f,g)$ bezeichnet.)

2. Sei μ die Möbiusfunktion und φ die Eulerfunktion. Zeige für $n \in \mathbb{N}_{>0}$ die Identität

$$\sum_{d \mid n} \frac{\mu(d)}{d} = \frac{\varphi(n)}{n}\,.$$

3. Sei $\mathbb{F}_q$ ein endlicher Körper. Zeige:
   a) Für q ungerade und $\alpha \in \mathbb{F}_q^*$ gilt $\alpha^{(q-1)/2} \in \{1, -1\}$, beide Fälle sind gleich häufig.
   b) Für $q = 2^m$ gerade und $\alpha \in \mathbb{F}_q$ gilt $T_m(\alpha) := \alpha^{2^{m-1}} + \alpha^{2^{m-2}} + \cdots + \alpha^2 + \alpha \in \{0, 1\}$ und beide Fälle sind gleich häufig.

4. Sei q ungerade. Um Nullstellen von Polynomen über $\mathbb{F}_q$ zu berechnen kann man eine Vereinfachung der Cantor-Zassenhaus-Faktorisierung benutzen:
   a) Sei $S := \{a \in \mathbb{F}_q^* \mid a \text{ ist ein Quadrat}\}$. Zeige, dass $X^{(q-1)/2} - 1 = \prod_{a \in S}(X - a)$ und somit $(X - c)^{(q-1)/2} - 1 = \prod_{a \in S}(X - a - c)$ gilt.
   b) Sei $f \in \mathbb{F}_q[X]$ ein quadratisches Polynom mit zwei verschiedenen Nullstellen. Für zufälliges $c \in \mathbb{F}_q$ ist mit Wahrscheinlichkeit $\approx \frac{1}{2}$ ein Linearfaktor bestimmt via

$$\mathrm{ggT}\left((X - c)^{(q-1)/2} - 1\,,\ f\right).$$

   c) Berechne eine Quadratwurzel von 2 in $\mathbb{F}_{17}$. Betrachte hierfür $f := X^2 - 2 \in \mathbb{F}_{17}[X]$ und verwende $c = 3$.

5. Berechne die Polynomprodukte
   a) $(a_2X^2 + a_1X + a_0) \cdot (b_2X^2 + b_1X + b_0)$ mit 6 Multiplikationen,
   b) $(a_3X^3 + a_2X^2 + a_1X + a_0) \cdot (b_3X^3 + b_2X^2 + b_1X + b_0)$ mit 9 Multiplikationen.

6. Hat ein Integritätsring R (mit $2 \in R^*$) nicht genügend primitive Einheitswurzeln für die diskrete Fourier-Transformation, kann folgende Konstruktion helfen. Betrachte

$$S := R[X]/(X^m + 1)\,.$$

   Zeige: Es ist S nicht notwendig ein Integritätsring, aber $\omega := [X] \in S$ ist primitive n-te Einheitswurzel für $n = 2m$, und es gilt $\sum_{i=0}^{n-1} \omega^{ki} = 0$ für alle $0 < k < n$.