Universität Tübingen
Mathematisches Institut Tübingen, den 11.11.2007

## Übungen zur Elementaren Zahlentheorie (5)

**(17)** Man gebe eine explizite Formel für $u_n$ an, wenn die Folge $\{u_n\}_{n\in\mathbb{N}}$ gegeben ist durch die lineare Rekursion $u_0 = 2, u_1 = 0, u_2 = -2$ sowie

$$u_{n+3} - 6u_{n+2} + 11u_{n+1} - 6u_n = 0 \quad (n \in \mathbb{N}).$$

Hinweis: $\alpha = 1$ ist Wurzel des zugeordneten Polynoms.

**(18)** Die Folge $\{v_n\}_{n\in\mathbb{N}}$ reeller Zahlen erfülle $v_0 = 1$ und $v_{n+1} = \frac{v_n}{v_n - 2}$ für jedes $n$. Durch Betrachten der Folge $\{u_n\}$ mit $u_{n+1}/u_n = v_n - 2$, die einer homogenen linearen Rekursion genügt, berechne man die $v_n$ explizit.

**(19)** Die Folge $\{u_n\}$ genüge der Rekursion $u_0 = 1$ sowie $u_{n+1} - 2u_n = 4^n$ ($n \in \mathbb{N}$). Man zeige, dass $U = \frac{1-3X}{(1-2X)(1-4X)}$ die zugeordnete erzeugende Funktion (formale Potenzreihe) ist. Man folgere durch Partialbruchzerlegung, dass $u_n = 2^{2n-1} + 2^{n-1}$ gilt für jedes $n$.

**(20)** Sei $p \in \mathbb{P}$ und $f \in \mathbb{F}_p[X]$ ein normiertes irreduzibles Polynom vom Grade $n$. Sei $K = \mathbb{F}_p[X]/(f)$ *der* Körper mit $p^n$ Elementen. Ist $K^*$ erzeugt von der Restklasse von $X \bmod f$, so heißt $f$ ein *primitives* Polynom (für $K$).
Man zeige:
(a) $f = X^2 + 2X + 2$ ist primitiv (und irreduzibel) in $\mathbb{F}_3[X]$. (Dies macht das Rechnen im Körper $K = \mathbb{F}_3[X]/(f)$ der Ordnung 9 recht angenehm !)
(b) $f = X^4 + X^3 + X^2 + X + 1$ ist irreduzibel in $\mathbb{F}_2[X]$ aber nicht primitiv.