W.Knapp Tübingen, den 25. November 2006

31. Es bezeichne $F_n = 2^{2^n} + 1$ $(n \in \mathbb{N})$ die Folge der Fermat-Zahlen.
   (a) Beweisen Sie: Für alle Fermatzahlen $F_n = 2^{2^n} + 1$ gilt die Kongruenz
   $$2^{F_n - 1} \equiv 1 \pmod{F_n}.$$
   (b) Beweisen Sie für diese Folge die Rekursionsformel :
   $$F_0 = 3 \text{ und } F_{n+1} = (F_n - 1)^2 + 1 \text{ für alle } n \in \mathbb{N}.$$

(6 Punkte)

32. *Das Problem der schnellen Potenzberechnung*
   Es sei H ein multiplikativ geschriebenes Monoid mit Neutralelement 1 und x ein beliebiges Element von H.
   Bekanntlich lassen sich die Potenzen von x in H auf die folgende Weise für $n \in \mathbb{N}$ rekursiv definieren:
   $$x^n := \begin{cases} 1 & \text{, wenn } n = 0, \\ x^{n-1} \cdot x & \text{, wenn } n \geq 1. \end{cases}$$
   Nach dieser Definition erfordert die Berechnung der Potenz x^n für $1 \leq n \in \mathbb{N}$ genau $n - 1$ Multiplikationen in H.
   Nun definieren wir eine Funktion $m \mapsto \mathrm{pot}(x, m)$ rekursiv auf die folgende Art und Weise:
   $$\mathrm{pot}(x, 0) := 1,$$
   $$\mathrm{pot}(x, m+1) := \begin{cases} \mathrm{pot}(x, \frac{m+1}{2}) \cdot \mathrm{pot}(x, \frac{m+1}{2}) & \text{, falls } m \text{ ungerade,} \\ x \cdot \mathrm{pot}(x, \frac{m}{2}) \cdot \mathrm{pot}(x, \frac{m}{2}) & \text{, falls } m \text{ gerade.} \end{cases}$$
   (a) Beweisen Sie, dass für alle $x \in H$ und alle $n \in \mathbb{N}$ die Gleichung $x^n = \mathrm{pot}(x, n)$ gilt.
   (b) Zeigen Sie, dass für die Berechnung von x^n in H nicht mehr als $2 \log_2 n$ Multiplikationen in H erforderlich sind, wenn man die Funktion $m \mapsto \mathrm{pot}(x, m)$ verwendet.
   (c) Vergleichen Sie die Werte von $n - 1$ und von $2 \log_2 n$ für $n = 100$, $n = 1000$ und $n = 10^6$.

(6 Punkte)

Die Übungsaufgaben sind schriftlich zu bearbeiten und vor der Vorlesung am Dienstag, dem 12. Dezember 2006, abzugeben.