W.Knapp Tübingen, den 31. Mai 2010

33. *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 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)

34. Bestimmen Sie alle natürlichen Zahlen n, für welche der Wert der Eulerschen Phi-Funktion $\varphi(n)$ eine Primzahlpotenz p^m ist.

35. Sei p eine ungerade Primzahl und $1 \leq m \in \mathbb{N}$. Beweisen Sie durch vollständige Induktion nach m, dass Folgendes gilt:

$$(1+p)^{p^{m-1}} \begin{cases} \equiv 1 \pmod{p^m} & , \\ \not\equiv 1 \pmod{p^{m+1}} & . \end{cases}$$

Was ist die Ordnung der Restklasse $(1+p)+p^m\mathbb{Z}$ in der Gruppe der teilerfremden Reste $(\mathbb{Z}/p^m\mathbb{Z})^*$?
Ist dies alles auch für $p = 2$ richtig? (3 Punkte)

36. Sei G eine multipikativ geschriebene zyklische Gruppe der endlichen geraden Ordnung $n = 2m$, etwa $G = \langle a \rangle = \{1, a, \ldots, a^{n-1}\}$. Beweisen Sie:
(1) G besitzt genau ein Element der Ordnung 2, nämlich a^m.
(2) Wenn $n = 2^r n'$ mit ungeradem n' ist, so gilt für alle $x \in G$ folgendes:
$x^{n'} = 1$ oder $x^{n'2^\ell} = a^m$ für genau ein $\ell \in \{0, \ldots, r-1\}$. (3 Punkte)
Hinweis: Dies ist eine der Grundlagen des Primalitätstests von Miller-Rabin.

Die Übungsaufgaben sind schriftlich zu bearbeiten und in der Vorlesungspause am Dienstag, dem 15. Juni 2010, abzugeben.