W.Knapp Tübingen, den 5. Januar 2007

37. 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 $\ell \in \{0, \ldots, r-1\}$.

(4 Punkte)

38. (a) Beweisen Sie das folgende *Kriterium von Artjuhov-Selfridge* :
Sei p eine ungerade Primzahl, $p - 1 = 2^r q$ mit ungeradem q. Dann gilt für jedes $x \in \mathbb{Z} \setminus p\mathbb{Z}$ folgendes:
(i) $x^q \equiv 1 \pmod{p}$ oder
(ii) $x^{q2^\ell} \equiv -1 \pmod{p}$ für genau ein $\ell \in \{0, \ldots, r-1\}$.

(b) Bestimmen Sie die relative Häufigkeit („Wahrscheinlichkeit“), mit welcher der Fall (i) und mit welcher der Fall (ii) auftritt.
(Warum ist es dabei kein wirkliches Problem, dass die Menge $\mathbb{Z} \setminus p\mathbb{Z}$ unendlich ist ?)

(4 Punkte)

Hinweis: Das Kriterium von Artjuhov-Selfridge bildet die Grundlage für die berühmten Primzahltests von Miller und Rabin.

39. Sei $G = G_1 \times G_2 \times \cdots \times G_s$ ein direktes Produkt lauter zyklischer Gruppen gerader Ordnungen $|G_j| = n_j, 1 \leq j \leq s$. Bestimmen Sie die Anzahl der Involutionen (d. s. die Elemente der Ordnung 2) in G.

(4 Punkte)

Die Übungsaufgaben sind schriftlich zu bearbeiten und vor der Vorlesung am Dienstag, dem 16. Januar 2007, abzugeben.