W.Knapp Tübingen, den 3. Juni 2010

37. Gelte $n = n_1 n_2$ für zwei teilerfremde ungerade Zahlen n_1 und n_2 ungleich 1.
Beweisen Sie, dass die prime Restklassengruppe $\Pr(n) = (\mathbb{Z}/n)^*$ mindestens 3 verschiedene Involutionen besitzt, eine davon ist $\overline{n-1} = -1 + n\mathbb{Z}$.
Zeigen Sie durch Beispiele, dass die Voraussetzung der Teilerfremdheit von n_1 und n_2 unentbehrlich ist für die Gültigkeit der Behauptung.

(3 Punkte)

38. Bestimmen Sie die Anzahlen der Fermat-Testmengen FT(33) und FT(51).
Dabei ist für $2 \leq n \in \mathbb{N}$ definiert
$\mathrm{FT}(n) = \{x \mid x \in \mathbb{N} \text{ und } x < n \text{ und } x^{n-1} \equiv 1 \pmod{n}\}$
nach (5.1) der Vorlesung.

39. Die kleinste Carmichael-Zahl ist $561 = 3 \cdot 11 \cdot 17$.
Bestimmen Sie die Anzahl der Euler-Testmenge ET(561).
Dabei ist nach (5.12) der Vorlesung für eine ungerade natürliche Zahl $n > 1$ definiert
$\mathrm{ET}(n) = \{x \mid x \in \mathbb{N}, x < n, \mathrm{ggT}(x,n) = 1 \text{ und } x^{\frac{n-1}{2}} \equiv \left(\frac{x}{n}\right) \pmod{n}\}$.

(5 Punkte)

40. Beweisen Sie, dass alle Vielfachen von $21, 39, 55$ oder 57 keine Carmichael-Zahlen sind. (4 Punkte)

41. Sei p eine (große) Primzahl und a eine Primitivwurzel modulo p. Es seien s verschiedene Zahlen $k_i \in \{2, \ldots, p-2\}$ vorgegeben (z.B. zufällig gewählt). Wir setzen $q_i := a^{k_i} \bmod p$.

Mit $\log_a(x)$ bezeichnen wir den diskreten Logarithmus von x zur Basis a. Es gilt also für alle $x \in \{1, \ldots, p-1\}$ $a^{\log_a(x)} \equiv x \pmod{p}$; demnach gilt insbesondere $k_i = \log_a(q_i)$ für alle i.
Beweisen Sie:
Wenn für $x \in \{1, \ldots, p-1\}$ und (zufällig gewählte) Zahlen $R, m_1, \ldots, m_s$ die Kongruenz

$$a^R x \equiv \prod_{i=1}^{s} q_i^{m_i} \pmod{p}$$

gilt, so ist $\log_a(x) = (-R + \sum_{i=1}^{s} k_i m_i) \bmod (p-1)$.
Hinweis: Auf diesem Sachverhalt beruht ein kryptanalytischer Angriff auf Systeme, welche auf der Schwierigkeit beruhen, solche diskreten Logarithmen zu berechnen.

Die Übungsaufgaben 37, 39 und 40 sind schriftlich zu bearbeiten und in der Vorlesungspause am Dienstag, dem 22. Juni 2010, abzugeben.