W.Knapp Tübingen, den 18. Januar 2007

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

Erinnerung:
Ist n eine ungerade natürliche Zahl ≥ 3, so ist die („starke“) Selfridge-Testmenge $\mathrm{ST}(n)$ definiert durch

$$\mathrm{ST}(n) := \{x \mid x \in \{1, \ldots, n-1\} \text{ und } x^m \equiv 1 \pmod{n} \text{ oder } x^{m2^\ell} \equiv -1 \pmod{n} \text{ für ein } \ell \in \{0, \ldots, k-1\}\},$$

wobei $n - 1 = 2^k m$ mit ungeradem m gesetzt ist.

44. (a) Bestimmen sie die Selfridge-Testmengen $\mathrm{ST}(9)$ und $\mathrm{ST}(45)$ explizit.
(b) Berechnen Sie die Anzahl von $\mathrm{ST}(561)$ für die kleinste Carmichael-Zahl 561. Gilt $\mathrm{ST}(561) \subseteq \mathrm{ET}(561)$? (6 Punkte)

45. 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 $\log_a(x) = (-R + \sum_{i=1}^{s} k_i m_i) \bmod (p-1)$. (2 Punkte)

Hinweis: Auf einem sehr ähnlichen Sachverhalt gründet ein wesentlicher Einwand gegen die Aussage, dass das DL-Problem in $\mathbb{F}_p^*$ schwierig sei.

Die Übungsaufgaben sind schriftlich zu bearbeiten und vor der Vorlesung am Dienstag, dem 30. Januar 2007, abzugeben.