Mathematische Methoden in der Kommunikationstheorie
(Sommersemester 2018)

Dr. Tobias Moede
t.moede@tu-bs.de
Universitätsplatz 2, Raum 515
0531 391-7516

Alexander Cant, M.Sc.
a.cant@tu-bs.de
Universitätsplatz 2, Raum 515
0531 391-7516

Technische Universität Braunschweig

Übungsblatt 4
(Abgabe: 03.05.2018 in der VL)

Aufgabe 1. (Carmichael-Zahlen)
Eine zusammengesetzte natürliche Zahl n heißt **Carmichael-Zahl**, falls für alle $a \in \mathbb{Z}$ mit $\mathrm{ggT}(a, n) = 1$ gilt, dass $a^{n-1} \equiv 1 \bmod n$ ist. Beweisen Sie folgende Aussagen:

a) Jede Carmichael-Zahl n ist ungerade.

b) Jede Carmichael-Zahl n ist quadratfrei, d.h. es gibt keine Quadratzahl > 1, welche die Zahl n teilt.

c) Ist n Carmichael-Zahl, so gilt für jeden Primteiler p von n, dass $(p - 1) \mid (n - 1)$.

d) Jede Carmichael-Zahl n hat mindestens drei Primfaktoren.

e) Eine natürliche Zahl n ist genau dann eine Carmichael-Zahl, wenn $n = p_1 \cdots p_r$, $r \geq 3$ mit verschiedenen ungeraden Primzahlen p_i, für die jeweils $(p_i - 1) \mid (n - 1)$ gilt.

Hinweis: Verwenden Sie (ohne Beweis) die Existenz eines erzeugenden Elements von $\mathbb{Z}_{p^k}^*$ für ungerade Primzahlen p und den chinesischen Restsatz.

Aufgabe 2. (Faktorisierungsmethoden)
a) Bestimmen Sie einen Faktor der Zahl 25 mit

- der Faktorisierungsmethode von Fermat,
- der Pollard-Rho-Methode mit Polynom $f(x) = x^2 + 1$,
- der Pollard-Rho-Methode mit Polynom $f(x) = x^2 - 1$.

b) Bestimmen Sie einen Faktor der Zahl 1875 mit

- der Faktorisierungsmethode von Fermat,
- der Pollard-Rho-Methode mit Polynom $f(x) = x^2 + 1$.

Aufgabe 3. (Diedergruppen)
Sei $n \geq 3$ und sei G die Untergruppe von S_n, welche von den folgenden Permutationen erzeugt wird

$$\alpha = \begin{pmatrix} 1 & 2 & \cdots & n \\ 2 & 3 & \cdots & 1 \end{pmatrix} \qquad \text{und} \qquad \beta = \begin{pmatrix} 1 & 2 & 3 & \cdots & n-1 & n \\ 1 & n & n-1 & \cdots & 3 & 2 \end{pmatrix}$$

Zeigen Sie:

$$\alpha^n = \mathrm{id},\ \beta^2 = \mathrm{id},\ \beta\alpha\beta^{-1} = \alpha^{-1} \text{ und } |G| = 2n.$$

Aufgabe 4. (Ein gruppentheoretisches Verschlüsselungsverfahren)
Angenommen Y möchte eine Nachricht an X senden, dann wird wie folgt vorgegangen. Y und X einigen sich zunächst auf eine nicht-kommutative Gruppe G, die zwei elementweise kommutierende Untergruppen A und B enthält, d.h. es gilt $gh = hg$ für alle $g \in A$ und $h \in B$. Dann passiert folgendes:

- Y identifiziert seine Nachricht mit einem $m \in G$ und wählt zwei zufällige Element $a, b \in A$ und sendet amb an X.
- X wählt zwei zufällige Elemente $c, d \in B$ und sendet $cambd$ an Y.
- Y multipliziert $cambd$ von links mit a^{-1} und von rechts mit b^{-1} und erhält cmd, welche er zurück an X sendet.
- X multipliziert cmd von links mit c^{-1} und von rechts mit d^{-1} und erhält die Nachricht m.

Sei $n = 2k$ mit $k \geq 2$ und G wie in Aufgabe 3 definiert.

a) Beweisen Sie: Die Untergruppen $A = \langle \alpha^k \rangle$ und $B = \langle \beta \rangle$ kommutieren elementweise.

b) Angenommen X erhält als erstes das Wort $\alpha^4\beta$ und sendet α^4 an Y zurück. Zuletzt erhält X das Wort α^9 zurück. Entschlüsseln Sie die Nachricht.