Spezielle Aspekte: Kryptographie *SoSe 2011*
Barbara Baumeister
Tutoren: Patrick Wegener, Philipp Neumann, Patrik Odenbach

2. Übungsblatt

Abgabe: Mittwoch, 20.4.11

Aufgabe 1 *Seien a, b, z ganze Zahlen (d.h in $\mathbb{Z}$) und sei $a \equiv t \bmod z$ und $b \equiv s \bmod z$. Zeigen Sie folgende Kongruenzen:*

(a) $(a + b) \equiv (t + s) \bmod z$.

(b) $(ab) \equiv (ts) \bmod z$.

Aufgabe 2 *Sei die natürliche Zahl m in Dezimalschreibweise gegeben:*

$$m = a_n a_{n-1} \dots a_1 a_0.$$

Zeigen Sie mit Hilfe von Aufgabe 1:

(a) *m ist genau dann durch 9 teilbar, wenn die Quersumme von m, d.h $\sum_{i=0}^{n} a_i$, durch 9 teilbar ist.*

(b) *m ist genau dann durch 11 teilbar, wenn die alternierende Quersumme von m, d.h $\sum_{i=0}^{n} a_i(-1)^i$ durch 11 teilbar ist.*

Aufgabe 3 *VSEGEXBCHJBEBNNSEGGOZOBQXNCMBCZAOOKDANGDKFSHNNFDKO WOMMKGJIENEMDVOBMSO*

Entschlüsseln Sie diesen Text, der mit der Vignere-Chiffre verschlüsselt wurde. Welcher Schlüssel wurde verwendet?

Aufgabe 4 *Gegeben seien die folgenden Matrizen:* $A := \begin{pmatrix} 0 & 1 & 3 & 2 \\ 1 & 4 & 1 & 0 \\ 4 & 3 & 2 & 1 \\ 1 & 2 & 0 & 3 \end{pmatrix} \in M_{4,4}(\mathbb{Z}_5)$, $B := \begin{pmatrix} 0 & 1 & 3 \\ 2 & 1 & 4 \\ 2 & 3 & 4 \end{pmatrix} \in M_{3,3}(\mathbb{Z}_5)$ *und* $C := \begin{pmatrix} 1 & 1 & 1 & 0 \\ 1 & 2 & 3 & 0 \\ 4 & 2 & 0 & 1 \end{pmatrix} \in M_{3,4}(\mathbb{Z}_5)$.

(a) *Überprüfen Sie welche Matrizen miteinander multipliziert werden können und multiplizieren Sie diese dann.*

(b) Berechnen Sie: $A\begin{pmatrix}1\\1\\0\\1\end{pmatrix}$, $B\begin{pmatrix}1\\0\\0\end{pmatrix}$, $B\begin{pmatrix}0\\1\\0\end{pmatrix}$ *und* $C\begin{pmatrix}1\\1\\0\\1\end{pmatrix}$.