Prof. Georg Hoever

1. Übungsblatt zur Vorlesung Kryptologie

Übung 1

a) Begründen Sie mit Hilfe der Modulo-Rechnung, dass gilt:

Eine Zahl ist durch 3 teilbar

⇔ ihre Quersumme (bei Dezimalschreibweise) ist durch 3 teilbar

(Tipp: Schreiben Sie die Zahl als $d_n \cdot 10^n + \ldots + d_1 \cdot 10 + d_0$.)

- b) Begründen Sie entsprechend die 9er-Teilbarkeitsregel.
- c) Leiten Sie eine ähnliche 11er-Teilbarkeitsregel ab. (Tipp: Es gilt $10 = -1 \mod 11$.)

Übung 2

Sei $a_1 = a_2 \mod m$ und $b_1 = b_2 \mod m$.

- a) Zeigen Sie, dass gilt: $a_1 \cdot b_1 = a_2 \cdot b_2 \mod m$.
- b) Gilt auch $a_1^{b_1} = a_2^{b_2} \mod m$? Beweis oder Gegenbeispiel!
- c) Gelten folgende Zusammenhänge?
 - 1. $a = b \mod (m_1 \cdot m_2) \implies a = b \mod m_1 \text{ und } a = b \mod m_2$
 - 2. $a = b \mod (m_1 + m_2) \implies a = b \mod m_1 \text{ und } a = b \mod m_2$

Übung 3

Stellen Sie eine Verknüpfungstabelle für \oplus und \odot in \mathbb{Z}_6 auf!

Übung 4

Berechnen Sie (ohne Taschenrechner)

- a) $(6 \oplus 8) \odot (7 \oplus 5)$ in \mathbb{Z}_9 ,
- b) $(7 \odot 5) \oplus (5 \odot 10) \oplus (7 \odot 8 \odot 9)$ in \mathbb{Z}_{11} ,
- c) $7^5 = 7 \odot 7 \odot 7 \odot 7 \odot 7$ in \mathbb{Z}_9 ,
- d) $67 \odot 68 \text{ in } \mathbb{Z}_{69}$.

Übung 5

- a) Ist $\mathbb{Z}_6 \setminus \{0\}$ mit " \odot " eine Gruppe?
- b) Ist $\mathbb{Z}_7 \setminus \{0\}$ mit " \odot " eine Gruppe?
- c) Ist $M = \{ \spadesuit, \spadesuit, \heartsuit, \diamondsuit \}$ mit der folgenden Verknüpfung \circ eine Gruppe?

0	•	^	Q	♦
	*	^	Q	♦
^	^	Q	•	Q
\Diamond	Q	•	♦	♦
♦	♦	Q	♦	•

d) Ist $M = \{0, 1, 2, 3\}$ mit der folgenden Verknüpfungen \oplus eine Gruppe?

\oplus	0	1	2	3
0	0	1	2	3
1	1	0	3	2
2	2	3	0	1
3	3	2	1	0

Falls ja: Ist die Gruppe auch kommutativ?

Zusatzaufgabe 1

Sind

- a) die Menge aller Caesar-Verschiebungen,
- b) die Menge aller monoalphabetischen Verschlüsselungen

(kommutative) Gruppen, wenn man als Verknüpfung die Hintereinanderausführung der jeweiligen Verschlüsselung nimmt?

Zusatzaufgabe 2

Wenn Sie bei $\mathbb{Z}_5 \setminus \{0\}$ mit " \odot " bzw. bei der entsprechenden Verknüpfungstabelle folgende Umbenennungen durchführen,

1 ersetzen durch 0 2 ersetzen durch 1 4 ersetzen durch 2 (3 bleibt 3)

erhalten Sie genau die Gruppe Z₄ mit der durch "⊕" definierten Verknüpfung.

Gibt es eine andere Gruppe mit vier Elementen, die *nicht* durch Umbenennung auf \mathbb{Z}_4 mit " \oplus " zurückgeführt werden kann?

Zusatzaufgabe 3 (für Knobler)

Zeigen Sie:

- a) Ist G eine Gruppe, so ist zu jedem $a \in G$ das inverse Element eindeutig bestimmt.
- b) Ist G eine Gruppe, so gilt für jedes $a \in G$: $\bar{a} = a$.
- c) Zeigen Sie: Sei " \circ " auf G eine assoziative Verknüpfung. Gibt es ein rechtsneutrales und rechtsinverse Elemente, so ist G schon eine Gruppe, d.h., gilt

```
\exists n \in G : \forall a \in G : a \circ n = a \text{ und } \exists \bar{a} \in G : a \circ \bar{a} = n,
```

so folgt

 $\exists n \in G : \forall a \in G : a \circ n = n \circ a = a.$ und $\exists \bar{a} \in G : a \circ \bar{a} = \bar{a} \circ a = n.$

(Schwierig! Tipp: Bringen Sie \bar{a} ins Spiel.)