FH AACHEN
UNIVERSITY OF APPLIED SCIENCES

Fachbereich Elektrotechnik
und Informationstechnik

Prof. Georg Hoever

WS 2023/24
04.10.2023

Musterlösung zum 1. Übungsblatt zur Vorlesung Kryptologie

Übung 1

Sei $z = d_n \cdot 10^n + \cdots + d_1 \cdot 10 + d_0$ eine ganze Zahl.

a) Es gilt:

$$z \text{ ist durch 3 teilbar } \Leftrightarrow \; z \;=\; 0 \bmod 3.$$

Wegen $10 \bmod 3 = 1$ folgt

$$10^n \bmod 3 = (10 \bmod 3 \cdot \ldots \cdot 10 \bmod 3) \bmod 3 = 1^n \bmod 3 = 1.$$

Damit ergibt sich:

$$\begin{aligned} & z \bmod 3 \\ = \; & \left(d_n \cdot 10^n + \cdots + d_1 \cdot 10 + d_0\right) \bmod 3 \\ = \; & \left(d_n \cdot (10^n \bmod 3) + \cdots + d_1 \cdot (10 \bmod 3) + d_0\right) \bmod 3 \\ = \; & (d_n \cdot 1 + \cdots + d_1 \cdot 1 + d_0) \bmod 3 \\ = \; & (d_n + \cdots + d_1 + d_0) \bmod 3. \end{aligned}$$

Also:

$$\begin{aligned} & z \text{ ist durch 3 teilbar} \\ \Leftrightarrow \; & 0 \;=\; z \bmod 3 = (d_n + \cdots + d_1 + d_0) \bmod 3 \\ \Leftrightarrow \; & \text{die Quersumme von } z \text{ ist durch 3 teilbar.} \end{aligned}$$

b) analog zu a) $(10 \bmod 9 = 1)$

c) Aus $10 \bmod 11 = -1$ folgt allgemein $10^n \bmod 11 = (-1)^n$. Damit ergibt sich:

$$\begin{aligned} & z \bmod 11 \\ = \; & \left(d_n \cdot 10^n + \cdots + d_1 \cdot 10 + d_0\right) \bmod 11 \\ = \; & \left(d_n \cdot (10^n \bmod 11) + \cdots + d_1 \cdot (10 \bmod 11) + d_0\right) \bmod 11 \\ = \; & \left(d_n \cdot (-1)^n + \cdots + d_1 \cdot (-1)^1 + d_0\right) \bmod 11 \\ = \; & \left(d_0 - d_1 + d_2 + - \ldots d_n\right) \bmod 11 \end{aligned}$$

Also:

$$\begin{aligned} & z \text{ ist durch 11 teilbar} \\ \Leftrightarrow \; & 0 \;=\; z \bmod 11 = (d_0 - d_1 + d_2 + - \ldots d_n) \bmod 3 \\ \Leftrightarrow \; & \text{die alternierende Quersumme von } z \text{ ist durch 11 teilbar.} \end{aligned}$$

Übung 2

a) Sei $a_1 = a_2 \bmod m$ und $b_1 = b_2 \bmod m$.
Dann gibt es $k_1, k_2 \in \mathbb{Z}$ mit $a_1 = a_2 + k_1 \cdot m$ und $b_1 = b_2 + k_2 \cdot m$, und es gilt:

$$\begin{aligned} a_1 \cdot b_1 &= (a_2 + k_1 \cdot m) \cdot (b_2 + k_2 \cdot m) \\ &= a_2 \cdot b_2 + a_2 \cdot k_2 \cdot m + k_1 \cdot m \cdot b_2 + k_1 \cdot k_2 \cdot m^2 \\ &= a_2 \cdot b_2 + \underbrace{(a_2 \cdot k_2 + k_1 \cdot b_2 + k_1 \cdot k_2 \cdot m)}_{\in \mathbb{Z}} \cdot m \end{aligned}$$

$$\Rightarrow a_1 \cdot b_1 = a_2 \cdot b_2 \bmod m.$$

b) Nein. Gegenbeispiel: $2 = 5 \bmod 3,\ 6 = 3 \bmod 3$, aber:

$$\begin{aligned} 2^6 &= 64 = 1 \bmod 3 \\ 5^3 &= 125 = 2 \bmod 3 \end{aligned}$$

c) 1. Ja, denn ist $a = b \bmod (m_1 \cdot m_2)$, so gibt es ein $k \in \mathbb{Z}$ mit

$$a = b + k \cdot (m_1 \cdot m_2) = b + m_1 \cdot \underbrace{(k \cdot m_2)}_{\in \mathbb{Z}},$$

also $a = b \bmod m_1$, entsprechend wegen $a = b + m_2 \cdot (k \cdot m_1)$ auch $a = b \bmod m_2$.

2. Nein. Gegenbeispiel: $2 = 7 \bmod (2 + 3)$, aber $2 \neq 7 \bmod 2$.

Übung 3

$\oplus$	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

$\odot$	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

Übung 4

a) In $\mathbb{Z}_9$ ist $(6 \oplus 8) \odot (7 \oplus 5) = 5 \odot 3 = 6$.

b) In $\mathbb{Z}_{11}$ ist $(7 \odot 5) \oplus (5 \odot 10) \oplus (7 \odot 8 \odot 9) = 2 \oplus 6 \oplus (1 \odot 9) = 8 \oplus 9 = 6$.

c) In $\mathbb{Z}_9$ ist $7 \odot 7 \odot 7 \odot 7 \odot 7 = 4 \odot 4 \odot 7 = 7 \odot 7 = 4$.

d) In $\mathbb{Z}_{69}$ ist $67 \odot 68 = -2 \odot -1 = 2$.

Übung 5

a) Nein, $2 \odot 3 = 0 \notin \mathbb{Z}_6 \setminus \{0\}$.

b) Ja: Die Verknüpfung ist assoziativ und sogar kommutativ, wie man durch Zurückführung auf die Definition in $\mathbb{Z}$ zeigen kann. Die Verknüpfung ist wohldefiniert (d.h., zu $a, b \in \mathbb{Z}_7 \setminus \{0\}$ ist auch $a \odot b \in \mathbb{Z}_7 \setminus \{0\}$, wie man an der Verknüpfungstabelle ablesen kann), 1 ist offensichtlich neutrales Element, und an der Verknüpfungstafel kann man ablesen, dass in jeder Zeile eine 1, also das neutrale Element auftaucht, so dass jedes Element ein inverses Element hat.

c) Nein, denn:

$$(\diamondsuit \circ \diamondsuit) \circ \spadesuit \;=\; \clubsuit \circ \spadesuit \;=\; \spadesuit$$
$$\diamondsuit \circ (\diamondsuit \circ \spadesuit) \;=\; \diamondsuit \circ \heartsuit \;=\; \diamondsuit$$

d) Ja:

- 0 ist offensichtlich neutrales Element.
- Jedes Element ist zu sich selbst invers ($a + a = 0$).
- Die Verknüpfung ist assoziativ. Um dies vollständig zu prüfen muss man mehrere Fälle untersuchen:

  Zu zeigen ist: $\forall a, b, c \in \{0, 1, 2, 3\} : (a \oplus b) \oplus c = a \oplus (b \oplus c)$.

  Wenn a, b oder c gleich 0 ist, ist die Aussage klar. Da $\oplus$ offensichtlich kommutativ ist (symmetrische Verknüpfungsmatrix), ist die Aussage auch für $a = c$ richtig. Da jedes Element zu sich selbst invers ist, gilt sie auch für $a = b = c$, denn dann folgt:

  $$(a \oplus a) \oplus a = 0 \oplus a = a = a \oplus 0 = a \oplus (a \oplus a).$$

  Wegen der Kommutativität sind die Rollen von a und c vertauschbar, so dass es reicht, die Fälle mit $a < c$ zu untersuchen. Damit bleiben die folgenden Fälle:

a	b	c	$a \oplus b$	$b \oplus c$	$(a \oplus b) \oplus c$	$a \oplus (b \oplus c)$
1	1	2	0	3	2	2
1	1	3	0	2	3	3
1	2	2	3	0	1	1
1	2	3	3	1	0	0
1	3	2	2	1	0	0
1	3	3	2	0	1	1
2	1	3	3	2	0	0
2	2	3	0	1	3	3
2	3	3	1	0	2	2

  In der folgenden Interpretation ist die Assoziativität klar: Stellt man die Zahlen 0, 1, 2 und 3 jeweils als zweistellige Binärzahlen dar, z.B. $1 = 01_2$, $3 = 11_2$, so

ergibt sich die Verknüpfungstabelle durch bitweises XOR, z.B.

$$1 \oplus 3 \;=\; 01_2 \text{ XOR } 11_2 \;=\; 10_2 \;=\; 2.$$

Da XOR das Gleiche wie eine modulo 2-Addition ist, ist klar, dass XOR und damit auch die vorgegebene Verknüpfung assoziativ ist.

Die Gruppe ist kommutativ, was man direkt an der Symmetrie der Verknüpfungstabelle ablesen kann.

Zusatzaufgabe 1

Die Mengen aller Caesar-Verschiebungen und die Mengen aller monoalphabetischer Verschlüsselungen sind jeweils Gruppen. Dazu muss man sich folgendes überlegen:

- Die Hintereinanderausführung zweier entsprechender Verschlüsselungen ergibt wieder eine Verschlüsselung der entsprechenden Art:

  Die Caesar-Verschiebung „dreht“ alle Buchstaben um einen bestimmten Wert weiter. Tut man dies zweimal hintereinander, so erhält man wieder eine Caesar-Verschiebung mit Verschiebungswert als Summe der beiden einzelnen Verschiebungswerte.

  Bei der Hintereinanderausführung zweier monoalphabetischer Verschlüsselungen erhält man wieder eine Zuordnung, durch welchen Buchstaben ein Buchstabe ersetzt wird, also wieder eine monoalphabetische Verschlüsselung.

- Die Hintereinanderausführung ist assoziativ.

  Die einzelnen Verschlüsselungen kann man als Abbildungen auffassen, die jeweils in bestimmter Weise Klartexten Geheimtexte zuordnen. Man kann sich nun überlegen, dass ganz allgemein die Hintereinanderausführungen von Abbildungen assoziativ ist: Seien f_1, f_2 und f_3 Abbildungen. Dann ist zu zeigen, dass $f_1 \circ (f_2 \circ f_3) = (f_1 \circ f_2) \circ f_3$ ist. Für ein abzubildendes x gilt tatsächlich

  $$\big(f_1 \circ (f_2 \circ f_3)\big)(x) \;=\; f_1\big((f_2 \circ f_3)(x)\big) \;=\; f_1\big(f_2(f_3(x))\big)$$

  und

  $$\big((f_1 \circ f_2) \circ f_3\big)(x) \;=\; (f_1 \circ f_2)(f_3(x)) \;=\; f_1\big(f_2(f_3(x))\big).$$

- Es gibt ein neutrales Element.

  Das neutrale Element ist jeweils die „Verschlüsselung“, die nichts ändert: bei der Caesar-Verschiebung die Verschiebung um 0, bei der monoalphabetischen Verschlüsselung die Zuordnung, die jeden Buchstaben sich selbst zuordnet.

- Es gibt inverse Elemente.

  Das inverse Element muss die ursprüngliche Verschlüsselung rückgängig machen. Bei der Caesar-Verschiebung um k Buchstaben ist dies die Caesar-Verschiebung um $26 - k$ Buchstaben, bei der monoalphabetischen Verschlüsselung die entsprechend umgekehrte Ersetzungs-Zuordnung.

Die Menge der Caesar-Verschiebungen ist sogar kommutativ, da man die Verschlüsselung jeweils als Addition von als Zahlen interpretierte Buchstaben auffassen kann, und bei diesen Additionen die Reihenfolge keine Rolle spielt. Entsprechend ist auch die Vigenère-Verschlüsselung kommutativ.

Die Menge der monoalphabetischen Verschlüsselungen ist nicht kommutativ, denn ist beispielsweise V_1 die Ersetzung, bei der A und B vertauscht werden und der Rest gleichbleibt, V_2 die Ersetzung, bei der A zu B, B zu C, C zu A und der Rest gleichbleibt, so wird A bei Verschlüsselung durch V_1 und anschließend von V_2 zu C, bei umgekehrter Reihenfolge, also zunächst V_2, dann V_1 zu A, d.h., die Ersetzungen sind nicht vertauschbar.

Zusatzaufgabe 2

Ja, die Gruppe aus Aufgabe 5d) kann man nicht durch Umbenennung erhalten, dort ist jedes Element zu sich selbst invers, während es in $\mathbb{Z}_4$ Elemente gibt, die nicht zu sich selbst invers sind, und ob ein Element zu sich selbst invers ist, ändert sich durch Umbenennung nicht.

Zusatzaufgabe 3

a) Seien $\bar{a}_1$ und $\bar{a}_2$ inverse Elemente zu a. Dann gilt mit dem neutralen Element n:

$$\bar{a}_1 = \bar{a}_1 \circ n = \bar{a}_1 \circ (a \circ \bar{a}_2) = (\bar{a}_1 \circ a) \circ \bar{a}_2 = n \circ \bar{a}_2 = \bar{a}_2.$$

b) Mit dem neutralen Element n gilt:

$$a = a \circ n = a \circ (\bar{a} \circ \bar{\bar{a}}) = (a \circ \bar{a}) \circ \bar{\bar{a}} = n \circ \bar{\bar{a}} = \bar{\bar{a}}.$$

c) Es gilt

$$\begin{aligned} \bar{a} \circ a &= (\bar{a} \circ a) \circ n = (\bar{a} \circ a) \circ (\bar{a} \circ \bar{\bar{a}}) \\ &= \bar{a} \circ (a \circ (\bar{a} \circ \bar{\bar{a}})) = \bar{a} \circ ((a \circ \bar{a}) \circ \bar{\bar{a}}) \\ &= (\bar{a} \circ (a \circ \bar{a})) \circ \bar{\bar{a}} = (\bar{a} \circ n) \circ \bar{\bar{a}} = \bar{a} \circ \bar{\bar{a}} = n. \end{aligned}$$

Damit gilt weiter

$$n \circ a = (a \circ \bar{a}) \circ a = a \circ (\bar{a} \circ a) = a \circ n = a.$$