Mathematik für Computer Science 1
WS 2025/26

Übungsaufgaben zu Thema 3
Elemente der Zahlentheorie

(mit Lösungen der Selbstcheck-Aufgaben)

Aufgaben, die mit dem Symbol ☑ gekennzeichnet sind, können Sie für den nächsten Übungstermin „ankreuzen“. Damit erklären Sie, die Bearbeitung der Aufgabe an der Tafel präsentieren zu können.

Mit einem * gekennzeichnete Aufgaben betreffen weiterführende Themen oder sind ein bisschen schwierig. Sie sind nicht prüfungsrelevant.

Aufgabe 1

Berechnen Sie den größten gemeinsamen Teiler von 96 und 186...

(a) mithilfe des Euklid'schen Algorithmus

(b) mithilfe der Primfaktorenzerlegung.

Lösung:

(a) Euklid'scher Algorithmus:

$$186 = 1 \cdot 96 + 90$$
$$96 = 1 \cdot 90 + \mathbf{6}$$
$$90 = 15 \cdot 6 + 0$$

Der letzte nichtverschwindende Rest ist 6, daher ist $\mathrm{ggT}(186, 96) = 6$.

(b) Primfaktorzerlegung: $186 = 2 \cdot 3 \cdot 31$, $96 = 2^5 \cdot 3$, daher $\mathrm{ggT}(186, 96) = 2 \cdot 3 = 6$

Aufgabe 2 ☑

Ermitteln Sie den größten gemeinsamen Teiler von 84 und 385 ...

(a) mithilfe des Euklid'schen Algorithmus sowie

(b) mithilfe der Primfaktorenzerlegung.

Aufgabe 3

Auf Büchern findet sich (seit 2007) eine dreizehnstellige *Internationale Standard-Buchnummer* (ISBN-13) der Form $abc\text{-}d\text{-}efghi\text{-}jkl\text{-}p$.

Dabei ist abc je nach Buch 978 oder 979, d steht für die Sprache ($d = 3$ bedeutet zum Beispiel „deutschsprachig“), $efghi$ kennzeichnet den Verlag und jkl den Buchtitel. Schließlich ist p die Prüfziffer, die

$$a + 3b + c + 3d + e + 3f + g + 3h + i + 3j + k + 3l + p = 0 \pmod{10}$$

erfüllen muss.

Ist 978 - 3 - 662 - 49296 - 3 eine gültige ISBN-13?

Lösung:
Einsetzen in die Vorschrift ergibt:

$$9+3\cdot 7+8+3\cdot 3+6+3\cdot 6+2+3\cdot 4+9+3\cdot 2+9+3\cdot 6+3=130=0 \mod 10.$$

Somit ist die ISBN gültig. Es handelt sich um das Buch „Kryptografie verständlich“ von Ch. Paar und J. Pelzl, Springer Verlag.

Aufgabe 4

Bestimmen Sie das additive Inverse und (wenn vorhanden) das multiplikative Inverse von 8 in:
a) $\mathbb{Z}_{10}$ b) $\mathbb{Z}_{11}$ c) $\mathbb{Z}_{12}$ d) $\mathbb{Z}_{91}$

Lösung:
• additives Inverses:
a) 2 (Begründung: $8+2=0 \pmod{10}$) b) 3 c) 4 d) 83

• multiplikatives Inverses:
a) gibt es nicht, da $\text{ggT}(8,10)\neq 1$

b) $\frac{1}{8}=\frac{1+11}{8}=\frac{1+2\cdot 11}{8}=\frac{1+3\cdot 11}{8}=\frac{1+4\cdot 11}{8}=\frac{1+5\cdot 11}{8}=7$

Alternative Berechnung von $\frac{1}{8}$ mit dem erweiterten Euklid'schen Algorithmus:

$$\begin{aligned} 11 &= 1\cdot 8+3\\ 8 &= 2\cdot 3+2\\ 3 &= 1\cdot 2+1\\ 2 &= 2\cdot 1+0 \end{aligned}$$

Nun lösen wir jeweils nach dem Rest auf und setzen rekursiv ein:

$$\begin{aligned} 3 &= 11-8\\ 2 &= 8-2\cdot 3=8-2\cdot(11-8)=3\cdot 8-2\cdot 11\\ 1 &= 3-1\cdot 2=(11-8)-(3\cdot 8-2\cdot 11)=3\cdot 11-4\cdot 8 \end{aligned}$$

Somit: $\frac{1}{8}=-4=7 \pmod{11}$

c) gibt es nicht, da $\text{ggT}(8,12)\neq 1$

d) 57 ($=\frac{1+5\cdot 91}{8}$ bzw. erhält man mit dem EEA als letzte Zeile $3\cdot 91-34\cdot 8=1$, wovon dann $\frac{1}{8}=-34=57 \pmod{91}$ abgelesen werden kann)

Aufgabe 5

Nennen Sie (falls existent) jeweils ein Beispiel für einen Modul $n\in\mathbb{N}$ (mit $n>7$), sodass 7 in $\mathbb{Z}_n$ ...

(a) kein additives Inverses besitzt.

(b) ein additives Inverses, aber kein multiplikatives Inverses besitzt.

(c) ein additives Inverses und ein multiplikatives Inverses besitzt.

Lösung:

(a) ein additives Inverses gibt es immer (d.h. für jedes n)

(b) zum Beispiel $n = 14$: Wegen $\text{ggT}(7, 14) \neq 1$ existiert kein multiplikatives Inverses für 7 in $\mathbb{Z}_{14}$

(c) zum Beispiel $n = 8$: Das Element 7 besitzt ein multiplikatives Inverses in $\mathbb{Z}_8$, weil 7 und 8 teilerfremd sind (also $\text{ggT}(7, 8) = 1$ gilt).

Aufgabe 6

Es seien $m \in \mathbb{N}$ und $a, b \in \mathbb{Z}_m$.

- Sind die Gleichungen $a + x = b \pmod m$ und $a \cdot x = b \pmod m$ immer lösbar? Begründen Sie Ihre Antwort.
- Geben Sie alle Lösungen $x \in \mathbb{Z}_m$ an, wobei m der jeweilige Modul ist:

a) $18x = 24 \pmod{30}$ b) $6x = 4 \pmod 9$ c) $9x = 1 \pmod{13}$
d) $9x + 3 = 1 \pmod 7$ e) $8x + 1 = 4 \pmod{12}$

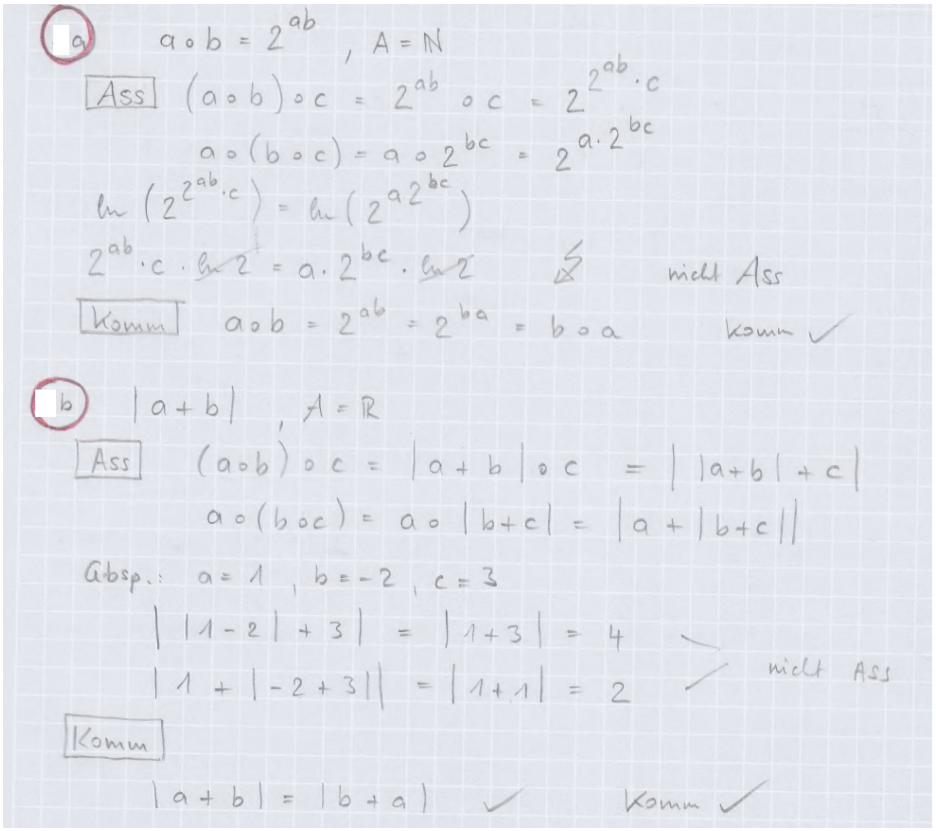
Aufgabe 7

Gegeben seien die folgenden Verknüpfungen $\circ$ in der Menge A. Begründen Sie, welche davon assoziativ und welche kommutativ sind!

(a) $a \circ b = 2^{ab}$, $A = \mathbb{N}$

(b) $a \circ b = |a + b|$, $A = \mathbb{R}$

Lösung:



Aufgabe 8

Gegeben seien die folgenden Verknüpfungen $\circ$ in der Menge A. Begründen Sie, welche davon assoziativ und welche kommutativ sind!

(a) $a \circ b = ab + 1$, $A = \mathbb{Q}$

(b) $a \circ b = a$, $A \neq \emptyset$

Aufgabe 9

Bildet $\{a, b, c\}$ mit der im Folgenden definierten Verknüpfung „$\circ$“ eine Gruppe?

$\circ$	a	b	c
a	a	b	c
b	b	a	c
c	c	b	a

Hinweis: Prüfen Sie, ob diese Verknüpfung assoziativ ist, ob es ein neutrales Element gibt, und ob es zu jedem Element ein inverses Element gibt. Achtung: für die Prüfung der Assoziativität müssen alle 27 Kombinationen von $x \circ (y \circ z) \stackrel{?}{=} (x \circ y) \circ z$ gelten. Versuchen Sie, dies auf effiziente Weise zu prüfen.

Lösung:
a ist das neutrale Element und zu jedem Element gibt es ein Inverses. Für die Gültigkeit des

Assoziativgesetzes müssten alle 27 Kombinationen von $x \circ (y \circ z) \stackrel{?}{=} (x \circ y) \circ z$ gelten. Für die Kombinationen, bei denen das neutrale Element beteiligt ist, gilt das Assoziativgesetz natürlich (denn Verknüpfung mit a bewirkt nichts), die kann man also von vornherein abhaken. Für die verbleibenden 8 Kombinationen zeigt sich aber, dass z. B. $b \circ (c \circ b) \neq (b \circ c) \circ b$; die Verknüpfung ist daher nicht assoziativ. (Insgesamt funktioniert es für 4 Kombinatione nicht: $b, c, b,\ c, b, b,\ b, c, c,\ c, b, c.$)

Aufgabe 10

Welche der folgenden Strukturen ist **keine** Gruppe? Begründen Sie mittels eines konkreten Beispiels einer Eigenschaft, die nicht erfüllt ist:

a) $(\mathbb{Z}_5, +)$ b) $(\mathbb{Z}_5^*, +)$ c) $(\mathbb{Z}_8, +)$ d) $(\mathbb{Z}_8^*, +)$ e) $(\mathbb{Z}_8, \cdot)$
f) $(\mathbb{Z}_8^*, \cdot)$ g) $(\mathbb{Z}_{11}, \cdot)$ h) $(\mathbb{Z}_{11}^*, \cdot)$

Welche der folgenden Strukturen ist **kein** Körper? Begründen Sie mit einem konkreten Beispiel einer Eigenschaft, die nicht erfüllt ist:

i) $(\mathbb{Z}_5, +, \cdot)$ j) $(\mathbb{Z}_8, +, \cdot)$ k) $(\mathbb{Z}_8^*, +, \cdot)$ l) $(\mathbb{Z}_{11}, +, \cdot)$

Lösungen:
Die Strukturen a), c), f) und h) sind Gruppen.
Keine Gruppen sind:
b) 0 fehlt d) 0 fehlt e) nicht alle Elemente haben ein multiplikatives Inverses
g) 0 hat kein multiplikatives Inverses
Die Strukturen i) und l) sind Körper, für den Rest gilt:
j) kein Körper, weil $\mathbb{Z}_8 \backslash \{0\}$ bzgl. $\cdot$ keine Gruppe ist k) kein Körper, weil 0 fehlt

Aufgabe 11

Gegeben ist die Menge $\mathbb{Z}$ mit (der üblichen) Addition und Multiplikation.
Welche der folgenden Eigenschaften treffen zu?

(a) Jedes Element (außer 0) besitzt ein multiplikatives Inverses.

(b) Jedes Element besitzt ein additives Inverses.

(c) $(\mathbb{Z}, +)$ ist eine kommutative Gruppe.

(d) $(\mathbb{Z}\backslash\{0\}, \cdot)$ ist eine kommutative Gruppe.

(e) Für alle $a, b, c \in \mathbb{Z}$ ist das Distributivgesetz $a \cdot (b + c) = a \cdot b + a \cdot c$ erfüllt.

Bildet $(\mathbb{Z}, +, \cdot)$ einen kommutativen Ring mit 1? Bildet es sogar einen Körper?
Begründen Sie Ihre Antwort.

Aufgabe 12*

Zeigen Sie, dass $K = \{a + b\sqrt{5} \mid a, b \in \mathbb{Q}\}$ bezüglich der Verknüpfungen "+" und "$\cdot$" einen Körper bildet, also einen Unterkörper von $(\mathbb{R}, +, \cdot)$.

Hinweis: Ein Element x_1 von K hat die Darstellung: $x_1 = a_1 + b_1\sqrt{5}$. Berücksichtigen Sie das Distributivgesetz in $\mathbb{R}$ und die Tatsache, dass $\frac{1}{a+b} = \frac{a-b}{a^2-b^2}$ gilt! Assoziativ-, Kommutativ- und Distributivgesetz wird von den reellen Zahlen geerbt. Zu zeigen sind die Abgeschlossenheit (Summe und Produkt solcher Zahlen sind wieder solche Zahlen), die Existenz des neutralen und die Existenz des inversen Elements.

Lösung: