

Aufgabe 1 (12 Punkte) Notizen zu Aufgaben in Rot (keine Gewähr)

In den folgenden Multiple Choice Aufgaben sind je 3 Antworten richtig.

(1.1) (4 Punkte):

- Setze $M := \{\emptyset\}$. Es gilt $M \times \emptyset = \{\emptyset, \emptyset\}$.
- Auf der Menge $M := \{1, 2, 3, 4\}$ gibt es $4! = 24$ Relationen.
- hierkreuz** → Sei M eine Menge. Dann ist $M \times M$ im allgemeinen keine Relation.
- Seien M und N Mengen und $R \subseteq M \times N$. Dann ist $R^T \circ R$ eine Relation.
- Sei R eine Relation. Dann folgt aus der Transitivität von R^T auch die Transitivität von R .
- Sei R eine Relation. Dann folgt aus der Asymmetrie von R die Antisymmetrie von R .

(1.2) (4 Punkte):

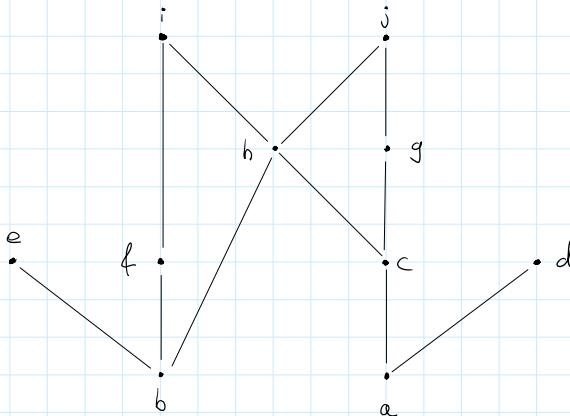
- hierkreuz** → Eine Ordnungsrelation ist immer irreflexiv.
- hierkreuz** → Sei R eine antisymmetrische Relation mit $R^T = R$. Dann ist R eine Ordnungsrelation.
- Die Total-Relation „ $|$ “ auf \mathbb{Z} ist antisymmetrisch.
- Sei M eine Menge und $A \subseteq M$. Weiter sei \leq eine Ordnungsrelation auf M . Jedes kleinste Element von A ist auch minimales Element von A .
- hierkreuz** → Sei M eine Menge und $A \subseteq M$. Weiter sei \leq eine Ordnungsrelation auf M . Die minimalen Elemente von A sind stets mit allen Elementen von A vergleichbar.
- Sei M eine Menge und $A \subseteq M$. Weiter sei \leq eine Ordnungsrelation auf M . Ist $a \in A$ eine obere Schranke von A , so gilt bereits $a = \sup(A)$.

(1.3) (4 Punkte):

- hierkreuz** → Es sei $f: M \rightarrow N$ eine Abbildung.
Dann ist f^{-1} eine Abbildung von $\text{Bild}(f)$ nach M .
- Es sei (G, \circ) eine Gruppe. Definiert man $a * b := b \circ a$ für alle $a, b \in G$, so ist auch $(G, *)$ eine Gruppe.
- Es gibt eine bijektive Abbildung zwischen der Menge $\{0, 1, 2, 3, 4, 5\}$ und der Gruppe $S_3 = \{f: \{1, 2, 3\} \rightarrow \{1, 2, 3\} \mid f \text{ ist bijektiv}\}$.
- Die Gruppe (S_3, \circ) ist zyklisch.
- Die additive Gruppe (\mathbb{Z}_2, \oplus) besitzt keine Untergruppe der Ordnung 2.
- hierkreuz** → Die multiplikative Gruppe $(\mathbb{Z}_2^\times, \otimes)$ besitzt keine Untergruppe der Ordnung 2.

Aufgabe 2 (10 Punkte)

Gegeben sei das folgende Hasse-Diagramm der zehn-elementigen Menge $M := \{a, b, c, d, e, f, g, h, i, j\}$:



	{c, g, h}	{a, b, c}	{c, g, h}	{a, b, c}
größte Elemente	/	/	c	/
maximale Elemente	h, g		c	b, a
obere Schranken	h, i, j		/	

größte Elemente	/	/	kleinste Elemente	/	/
maximale Elemente	b, g		minimale Elemente	c	b, a
obere Schranken	b, i, j		untere Schranken	/	/
obere Grenzen	b		untere Grenzen	/	/
Supremum	b		Infimum		/

Aufgabe 3 (17 Punkte)

Gegeben sei die Relation \equiv auf \mathbb{Z} , die durch $a \equiv b : \Leftrightarrow a^2 - b^2 = 2 \cdot a - 2 \cdot b$ definiert wird.

(3.1) (10 Punkte) Zeigen Sie, dass \equiv eine Äquivalenzrelation auf \mathbb{Z} ist.

(3.2) (4 Punkte) Geben Sie die Äquivalenzklassen $[0]_{\equiv}, [1]_{\equiv}, [2]_{\equiv}$ explizit an.
 Hinweis: Nutzen Sie dazu aus, dass man obige Äquivalenz auch wie folgt darstellen kann: $a \equiv b \Leftrightarrow (a-b) \cdot (a+b-2) = 0$.

(3.3) (3 Punkte) Zeigen Sie, dass $[a]_{\equiv} \oplus [b]_{\equiv} := [a+b]_{\equiv}$ für alle $a, b \in \mathbb{Z}$ nicht wohldefiniert bzw. nicht unabhängig vom Repräsentanten ist.

Hinweis: Nutzen Sie dazu die Äquivalenzklassen $[0]_{\equiv}$ und $[1]_{\equiv}$.

Aufgabe 4 (5 Punkte)

Gegeben sei die Äquivalenzrelation \equiv auf \mathbb{Z} , die durch $a \equiv b : \Leftrightarrow |a| = |b|$ definiert wird. Zeigen Sie, dass die Relation $f := \{([a]_{\equiv}, a^a) \mid a \in \mathbb{Z}\}$ auf $(\mathbb{Z}/\equiv) \times \mathbb{Z}$ eine Abbildung ist.

Erinnerung: $\mathbb{Z}/\equiv := \{[a]_{\equiv} \mid a \in \mathbb{Z}\}$

Aufgabe 5 (17 Punkte)

Wir betrachten die algebraische Struktur $(\mathbb{Z}_{25725}, \otimes)$

(5.1) (11 Punkte) Weitere der Gleichungen

$$1. [627]_{25725} \otimes x = [8575]_{25725}$$

$$2. [627]_{25725} \otimes x = [3675]_{25725}$$

besitzt eine Lösung x in \mathbb{Z}_{25725} ? Falls Lösungen existieren, berechnen Sie alle Lösungen mit dem in der Vorlesung verwendeten Verfahren. Falls keine Lösungen existieren, begründen Sie dies.

(5.2) (2 Punkte) Gibt es ein $a \in \mathbb{N}$ mit $1 < a < 11$, für das die Gleichung $[a]_{25725} \otimes x = [8575]_{25725}$ genau eine Lösung besitzt? Begründen Sie Ihre Antwort.

Aufgabe 6 (7 Punkte)

Geben Sie an, ob folgende Aussagen wahr oder falsch sind.

1. Das Schutzziel „Authentizität“ besagt, dass die Nachricht tatsächlich von der angegebenen Quelle stammt.

wahr	falsch
X	
	X

2. Seien P, C und K nichtleere Mengen und $e: P \times K \rightarrow C, d: C \times K \rightarrow P$ Funktionen. Ein kryptografisches System ist ein Quintupel (P, C, K, e, d) mit der Eigenschaft: $\forall k \in K \forall k' \in K \forall x \in P: d(e(x, k), k') = x$.

Funktionen. Ein kryptografisches System ist ein Quintupel (P, C, K, e, d) mit der Eigenschaft: $\exists k \in K \forall k' \in K \forall x \in P: d(e(x, k), k') = x$.

X

3. A priori Wahrscheinlichkeit ist die Wahrscheinlichkeit, mit der ein bestimmter Klartext übertragen wurde, wenn zusätzlich der Geheimtext bekannt ist.

X

4. Sollen bei einem symmetrischen Kryptosystem 51 Teilnehmer mit jeweils unterschiedlichen Schlüsseln kommunizieren, so benötigt man 1275 Schlüssel.

X

5. Das Vignère-Chiffre-Verfahren besitzt theoretisch unendlich viele Schlüssel.

X

6. Das One-Time-Pad-Verfahren ist kein perfekt sicheres Kryptosystem.

X

7. Beim RSA-Verfahren ist es unmöglich, den privaten aus dem öffentlichen Schlüssel zu berechnen.

X

Aufgabe 7 (11 Punkte)

(7.1) (3 Punkte) Ermitteln Sie ob $[E]_3$ und $[S]_3$ in $(\mathbb{Z}_7, \{[0], 3\}, \otimes)$ erzeugende Elemente sind.
Richtig auf Fotos!

Geben Sie dabei alle Rechenschritte an.

(7.2) (3 Punkte) Geben Sie jeweils die Anzahl der kleineren und teilerfremden natürlichen Zahlen zu 125 und 126 an. Geben Sie ohne Zwischenrechnung Ihre Berechnung an.

(7.3) (5 Punkte) Prüfen Sie mit Hilfe des Miller-Rabin-Algorithmus, ob $n=89$ eine Primzahl ist. Nutzen Sie hierfür die Basis $a=5$. Geben Sie alle Zwischenrechnungen Ihrer Berechnung an.
Hinweis: Sie dürfen annehmen, dass $\text{ggT}(5, 89)=1$ ist.

Aufgabe 8 (11 Punkte)

Bob möchte zur Verschlüsselung des RSA-Verfahrens verwenden. Bei der Schlüsselgenerierung wählt er $p=31$ und $q=93$.

- (8.1) (4 Punkte) Als nächstes muss Bob einen Wert für e festlegen. Welche Bedingungen muss e erfüllen? Welches ist das kleinste mögliche e , das Bob verwenden kann?

- (8.2) (2 Punkte) Bob wählt $e=17$. Ermitteln Sie den öffentlichen und privaten Schlüssel.
(2/2) auf Fotos
Geben Sie die Zwischenschritte Ihrer Berechnung an.
Hinweis: Das multiplikative Inverse von $[17]_{1260}$ in \mathbb{Z}_{1260} ist $[593]_{1260}$.

- (8.3) (5 Punkte) Verschlüsseln Sie die Nachricht $m=4$ unter Verwendung des Square & Multiply-
(5/5) auf Fotos Algorithmus.

Aufgabe 9 (14 Punkte)

Alice und Bob verwenden El Gamal-Verschlüsselungsverfahren mit $p=19$ und $g=14$. Der öffentliche Schlüssel von Alice ist 3. Bob möchte die Nachricht m an Alice senden. Er wählt zur Verschlüsselung geheim und zufällig eine Zahl b und sendet Alice anschließend die verschlüsselte Nachricht $(5, ?)$.

Hinweis: alle Formeln und Zwischenschritte angeben!

(9.1) (3 Punkte) Erläutern Sie, wie Bob die verschlüsselte Nachricht $(5, 2)$ berechnet hat.
(2/3)

(9.2) (3 Punkte) Eve fängt die von Bob verschickte Nachricht ab. Beschreiben Sie, was Eve theoretisch tun muss, um die Nachricht zu entschlüsseln.

(9.3) (8 Punkte) Entschlüsseln Sie Bobs Nachricht, indem Sie unter Zuhilfenahme des Baby-Step-Giant-Step-Algorithmus zunächst den öffentlichen Schlüssel von Alice angreifen.
Hinweis: Das multiplikative Inverse von $[14]_{19}$ in \mathbb{Z}_{19} ist $[15]_{19}$