Brzezinski, Christiansen, Ullmann, Zimmermann

NORDAKADEMIE
HOCHSCHULE DER WIRTSCHAFT

Klausur

Diskrete Mathematik 2 I168

3. Quartal 2018

Name des Prüflings: **Matrikelnummer:** **Zenturie:**

Dauer: 90 min Seiten ohne Deckblatt 13 Datum: 1. Oktober 2018

Hilfsmittel: Nordakademie Taschenrechner, Stifte, aber kein roter Stabilo 88/40.

Bemerkungen: Diese Klausur enthält 10 Aufgaben. Es können 100 Punkte erreicht werden. Zum Bestehen der Klausur benötigen Sie 50 Punkte. **Überprüfen Sie zuerst** die Anzahl der Seiten. Liegen Ihnen 13 Seiten (ohne Titelseite) vor?

Trennen Sie nicht die Heftung. Bitte schreiben Sie Ihre Lösungen auf die jeweiligen Aufgabenblätter. Falls Sie mit dem Platz nicht auskommen, verwenden sie auch die Rückseiten oder die Zusatzseiten am Ende des Klausurheftes.

Aufgabe:	1	2	3	4	5	6	7	8	9	10	Prozent:
Punktzahl:	8	5	10	17	7	13	6	11	9	14	100
Erreicht:											

Datum: _____ Note: _____ Ergänzungsprüfung: _____

Unterschrift: _____ Unterschrift: _____

Aufgabe 1 (8 Punkte)

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

Tipp: Nehmen Sie sich für das Lesen und Verstehen der Aufgabenstellung viel Zeit, ansonsten verlieren Sie unnötig viele Punkte.

Bewertungshinweis:

- Es gibt maximal vier Punkte pro Frage.
- Wenn Sie mehr als drei Kreuze pro Frage ankreuzen, erhalten Sie keine Punkte.
- Haben Sie ein Kreuz in einer Frage falsch gesetzt, erhalten Sie die halbe Punktzahl.
- Haben Sie mehr als ein Kreuz in einer Frage falsch gesetzt, erhalten Sie keine Punkte.

(1.1) (4 Punkte) Kreuzen Sie die drei richtigen Antworten an:

- ☐ Setze $M := \{0\}$. Es gilt: $M \times \emptyset = \{(0, \emptyset)\}$.
- ☐ Auf der Menge $M := \{1, 2, 3, 4\}$ gibt es $4! = 24$ Relationen.
- ☐ 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 $R^{-1} \circ R$ eine Relation.
- ☐ Sei R eine Relation. Dann folgt aus der Transitivität von R^{-1} auch die Transitivität von R.
- ☐ Sei $R \neq \emptyset$ eine Relation. Dann folgt aus der Asymmetrie von R die Antisymmetrie von R.

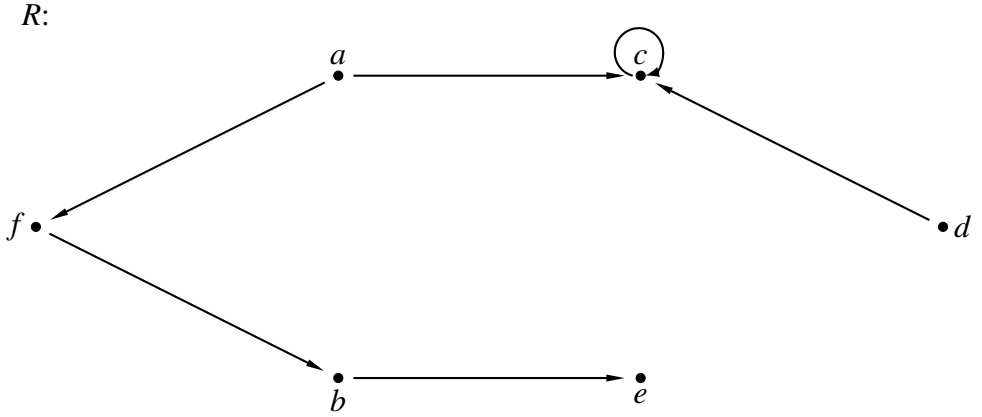
(1.2) (4 Punkte) Kreuzen Sie die drei richtigen Antworten an:

- ☐ Eine Ordnungsrelation ist immer irreflexiv.
- ☐ Sei R eine antisymmetrische Relation mit $R^* = R$. Dann ist R eine Ordnungsrelation.
- ☐ Die teilt-Relation „|“ auf $\mathbb{Z}$ ist antisymmetrisch.
- ☐ Sei M eine Menge und $A \subseteq M$. Weiter sei $\sqsubseteq$ eine Ordnungsrelation auf M. Jedes kleinste Element von A ist auch minimales Element von A.
- ☐ Sei M eine Menge und $A \subseteq M$. Weiter sei $\sqsubseteq$ 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 $\sqsubseteq$ eine Ordnungsrelation auf M. Ist $a \in A$ eine obere Schranke von A, so gilt bereits $a = \sup(A)$.

Aufgabe 2 (5 Punkte)

Gegeben sei das vereinfachte Pfeildiagramm der Relation R auf der sechs-elementigen Menge $M := \{a, b, c, d, e, f\}$:

R:



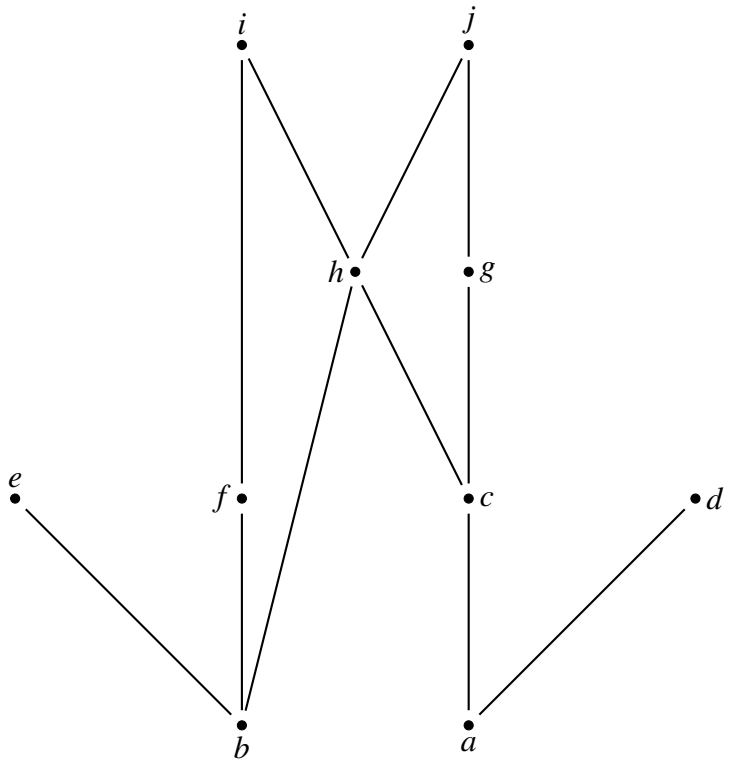
(2.1) (1 Punkt) Warum ist R keine strikte Ordnungsrelation? Begründen Sie Ihre Antwort.

(2.2) (3 Punkte) S sei die strikte Ordnungsrelation auf M, die entsteht, wenn Sie aus R genau ein Paar entfernen und genau drei Paare hinzufügen. Geben Sie das Hasse-Diagramm von S an.

(2.3) (1 Punkt) Gilt für die Relation S aus (2.2) die Gleichung $(S^N)^* = S$? Begründen Sie Ihre Antwort.

Aufgabe 3 (10 Punkte)

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



Geben Sie größte/ kleinste und maximale/ minimale Elemente sowie obere/ untere Scharanken, obere/ untere Grenzen und Supremum/ Infimum von $\{c, g, h\}$ und $\{a, b, c\}$ an, falls existent.

	$\{c, g, h\}$	$\{a, b, c\}$		$\{c, g, h\}$	$\{a, b, c\}$
größte Elemente			kleinste Elemente		
maximale Elemente			minimale Elemente		
obere Schranken			untere Schranken		
obere Grenzen			untere Grenzen		
Supremum			Infimum		

Aufgabe 4 (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.

(4.1) (10 Punkte) Zeigen Sie, dass $\equiv$ eine Äquivalenzrelation auf $\mathbb{Z}$ ist.

(4.2) (4 Punkte) Geben Sie die Äquivalenzklassen $[0]_{\equiv}, [1]_{\equiv}, [2]_{\equiv}$ und $[3]_{\equiv}$ explizit an.

Hinweis: Nutzen Sie dazu aus, dass man obige Äquivalenz auch wie folgt darstellen kann: $a \equiv b \Leftrightarrow (a - b) \cdot (a + b - 2) = 0$.

(4.3) (3 Punkte) Zeigen Sie, dass $[a]_{\equiv} \oplus [b]_{\equiv} := [a + b]_{\equiv}$ für alle $x, y \in \mathbb{Z}$ nicht wohldefiniert bzw. nicht unabhängig vom Repräsentaten ist.

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

Aufgabe 5 (7 Punkte)

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

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

Aufgabe 6 (13 Punkte)

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

(6.1) (11 Punkte) Welche 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 den in der Vorlesung verwendeten Verfahren. Falls keine Lösungen existieren, begründen Sie dies. Zeigen Sie dazu mit dem erweiterten Euklidischen Algorithmus, dass $t = -1436$.

(6.2) (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 7 (6 Punkte)

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

Hinweis: Inkorrekte Antworten führen nicht zu Abzügen. Punkte werden ab drei korrekten Antworten vergeben.

	Aussage	wahr	falsch
1.	Das Schutzziel „Authentizität“ besagt, dass die Nachricht tatsächlich von der angegebenen Quelle stammt		
2.	Seien P, C und K nichtleere Mengen und $e : P \times K \to C$, $d : C \times K \to P$ Funktionen. Ein kryptografisches System ist ein Quintupel (P, C, K, e, d) mit der Eigenschaft: $\exists k \in K\ \forall k' \in K\ \forall x \in P : d(e(x, k), k') = x$.		
3.	A priori Wahrscheinlichkeit ist die Wahrscheinlichkeit, mit der ein bestimmter Klartext übertragen wurde, wenn zusätzlich der Geheimtext bekannt ist.		
4.	Das Skytale-Verfahren ist ein monoalphabetisches Substitutionsverfahren.		
5.	Sollen bei einem symmetrischen Kryptosystem 51 Teilnehmer mit jeweils unterschiedlichen Schlüsseln kommunizieren, so benötigt man 1275 Schlüssel.		
6.	Das Vigenère-Chiffre-Verfahren besitzt theoretisch unendlich viele Schlüssel		
7.	Das One-Time-Pad-Verfahren ist kein perfekt sicheres Kryptosystem.		

Aufgabe 8 (11 Punkte)

(8.1) (3 Punkte) Ermitteln Sie, ob $[4]_7$ und $[5]_7$ in $\left(\mathbb{Z}_7 \setminus \{[0]_7\}, \otimes\right)$ erzeugende Elemente sind. Geben Sie dabei alle Rechenwege an.

(8.2) (3 Punkte) Geben Sie die Anzahl der teilerfremden natürlichen Zahlen von 125 und 126 an. Geben Sie die Zwischenschritte Ihrer Berechnung an.

(8.3) (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 Zwischenschritte Ihrer Berechnung an.

Hinweis: Sie dürfen annehmen, dass der $\text{ggT}(5, 89) = 1$ ist.

Aufgabe 9 (9 Punkte)

Bob möchte zur Verschlüsselung das RSA-Verfahren verwenden. Bei der Schlüsselgenerierung wählt er $p = 31$ und $q = 43$.

(9.1) (4 Punkte) Als nächstes muss Bob einen Wert für e festlegen. Welche Bedingung muss e erfüllen? Welches ist das kleinstmögliche e, das Bob verwenden kann?

(9.2) (2 Punkte) Bob wählt e = 17. Ermitteln Sie den öffentlichen und privaten Schlüssel. Geben Sie die Zwischenschritte Ihrer Berechnung an.

Hinweis: Das multiplikative Inverse von $[17]_{1260}$ in $\mathbb{Z}_{1260}$ ist $[593]_{1260}$.

(9.3) (3 Punkte) Verschlüsseln Sie die Nachricht $m = 4$. Erläutern Sie Ihren Rechenweg.

Aufgabe 10 (14 Punkte)

Alice und Bob verwenden das ElGamal-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 $(5, 2)$.

Hinweis: Geben Sie bei allen folgenden Teilaufgaben auch die zur Berechnung notwendigen Formeln und Zwischenschritte an.

(10.1) (3 Punkte) Erläutern Sie, wie Bob die verschlüsselte Nachricht $(5, 2)$ berechnet hat.

(10.2) (3 Punkte) Eve fängt die von Bob verschickte Nachricht ab. Beschreiben Sie, was Eve theoretisch tun muss, um die Nachricht zu entschlüsseln.

(10.3) (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 $[15]_{19}$.

Leere Seite für Ihre Notizen

Leere Seite für Ihre Notizen

Viel Erfolg