Brzezinski, Christiansen, Ullmann, Zimmermann

Klausur

Diskrete Mathematik 2 I168

3. Quartal 2017

Name des Prüflings: ______________________ **Matrikelnummer:** ______________ **Zenturie:** __________

Dauer: 90 min Seiten ohne Deckblatt 12 Datum: 9. Oktober 2017

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

Bemerkungen: Diese Klausur enthält 9 Aufgaben. Es können 100 Punkte erreicht werden. Zum Bestehen der Klausur benötigen Sie 50 Punkte. **Überprüfen Sie zuerst** die Anzahl der Seiten. Liegen Ihnen 12 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	Prozent:
Punktzahl:	12	8	10	14	9	12	11	14	10	100
Erreicht:										

Datum: ______________ Note: __________ Ergänzungsprüfung: __________

Unterschrift: ______________________ Unterschrift: ______________________

Aufgabe 1 (12 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 $M := \{1\}$. Es gilt: $M \times \emptyset = \{(1, \emptyset)\}$.
- ☐ Auf der Menge $M := \{1, 2, 3\}$ gibt es $2^3 = 8$ Relationen.
- ☒ $\emptyset^{-1}$ ist eine Relation.
- ☒ Seien M und N Mengen. Seien weiter $R \subseteq M \times N$ und $S \subseteq N \times M$. Dann ist $S \circ R$ eine Relation.
- ☒ Sei R eine Relation. Dann folgt aus der Symmetrie von R^{-1} auch die Symmetrie von R.
- ☐ Sei $R \neq \emptyset$ eine Relation. Dann folgt aus der Antisymmetrie von R die Asymmetrie von R.

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

- ☐ Jedes maximale Element ist auch größtes Element.
- ☐ Die Teilt-Relation „|" auf $\mathbb{N}$ ist asymmetrisch.
- ☒ Sei M eine Menge und $A \subseteq M$. Weiter sei $\sqsubseteq$ eine Ordnungsrelation auf M. Alle kleinsten Elemente von A sind mit allen Elementen von A vergleichbar.
- ☒ Sei M eine Menge und $A \subseteq M$. Weiter sei $\sqsubseteq$ eine Ordnungsrelation auf M. Die Menge der oberen Schranken von A kann leer sein.
- ☒ Der Schnitt zweier verschiedener Äquivalenzklassen ist immer leer.
- ☐ Es gilt: $\mathbb{Z}_3 \subseteq \mathbb{Z}_6$.

(1.3) (4 Punkte) Kreuzen Sie die drei richtigen Antworten an:

- ☒ Sei R eine Relation. Ist R^{-1} linkstotal, so ist R rechtstotal.
- ☒ Seien M, N Mengen und $f : M \to N$ eine Abbildung. f ist injektiv genau dann, wenn jedes Element aus N höchstens mit einem Element aus M in Beziehung steht.
- ☒ Seien M, N Mengen und $f : M \to N$ eine Abbildung. f ist surjektiv, wenn jedes Element aus N mit genau einem Element aus M in Beziehung steht.
- ☐ $f : \mathbb{Z}_3 \to \mathbb{N}_0, [x]_3 \mapsto x^2$ ist injektiv.
- ☐ Eine Abbildung ist keine Relation.
- ☐ Sei $m \in \mathbb{N}$. $\oplus : \mathbb{Z}_m \times \mathbb{Z}_m \to \mathbb{Z}_m, ([x]_m, [y]_m) \mapsto [x + y]_m$ ist keine Abbildung.

Aufgabe 2 (8 Punkte)

(2.1) (3 Punkte) Geben Sie die Eigenschaften einer Ordnungsrelation $\sqsubseteq$ auf M quantorisiert an.

transitiv

$\forall x, y, z \in M: (x, y) \in R \wedge (y, z) \in R \Rightarrow (x, z) \in R$

reflexiv

$\forall x \in M: (x, x) \in R$

antisymmetrisch

$\forall x, y \in M: (x, y) \in R \wedge (y, x) \in R \Rightarrow x = y$

(2.2) (5 Punkte) Setze $M := \{1, 2\}$. Geben Sie alle Ordnungsrelationen auf M an.

1) $Id_M = \{(1,1), (2,2)\}$

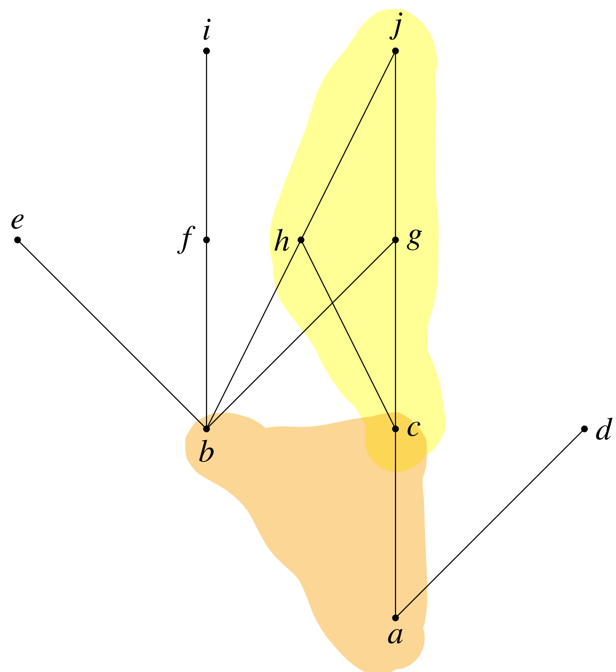
2) $Id_M \cup \{(1,2)\}$

3) $Id_M \cup \{(2,1)\}$

4) $\emptyset$

Aufgabe 3 (10 Punkte)

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



(3.1) (10 Punkte) Geben Sie größte/ kleinste und maximale/ minimale Elemente sowie obere/ untere Scharanken, obere/ untere Grenzen und Supremum/ Infimum von $\{c, g, h, j\}$ und $\{a, b, c\}$ an, falls existent.

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

Aufgabe 4 (14 Punkte)

Gegeben sei die Relation $R := \{(a,b) \in \mathbb{Z} \times \mathbb{Z} \mid 2 \mid (a+b)\}$ auf $\mathbb{Z}$. Beweisen Sie, dass R eine Äquivalenzrelation auf $\mathbb{Z}$ ist.

reflexiv Sei $a \in \mathbb{Z}$ so gilt

$(a,a) \Leftrightarrow 2 \mid (a+a) = 2 \mid 2a$ ✓

transitiv

Seien $a,b,c \in \mathbb{Z}$ da R transitiv ist gelte:

$2 \mid (a+b) \wedge 2 \mid (b+c)$ dann gilt

$2 \cdot x = a+b \wedge 2 \cdot y = b+c$ mit $x,y \in \mathbb{Z}$

$a+b-2x = 2y-b-c$

$a+c+2b-2x = 2y$

$a+c = 2(y+x-b) \Rightarrow 2 \mid a+c$ ✓

Symmetrisch

Seien $a,b \in \mathbb{Z}$ da R symmetrisch is gelte

$a \equiv b \Leftrightarrow 2 \mid (a+b) = 2 \mid (b+a) \Leftrightarrow b \Leftrightarrow a$

Aufgabe 5 (9 Punkte)

Gegeben sei die Äquivalenzrelation $\equiv$ auf $\mathbb{Z}$, die durch $a \equiv b :\Leftrightarrow (3 \mid a \;\wedge\; 3 \mid b) \;\vee\; a = b$ definiert wird.

(5.1) (6 Punkte) Geben Sie die Äquivalenzklassen $[0]_\equiv, [1]_\equiv, [2]_\equiv, [3]_\equiv$ und $[4]_\equiv$ explizit an.

$[0]_\equiv = \{0, 3, 6, 9, \ldots\}$

$[1]_\equiv = \{1\}$

$[2]_\equiv = \{2\}$,

$[3]_\equiv = \{0, 3, 6, 9, \ldots\}$

$[4]_\equiv = \{4\}$

(5.2) (3 Punkte) Zeigen Sie, dass $[x]_\equiv \oplus [y]_\equiv := [x + y]_\equiv$ für alle $x, y \in \mathbb{Z}$ nicht wohldefiniert bzw. nicht unabhängig vom Repräsentaten ist.

Hinweis: Nutzen Sie dazu die Äquivalenzklassen $[1]_\equiv$ und $[3]_\equiv$.

$[1]_\equiv \oplus [3]_\equiv = [4]_\equiv \neq [7]_\equiv = [7]_\equiv + [0]_\equiv$

Aufgabe 6 (12 Punkte)
Wir betrachten die algebraische Struktur $(\mathbb{Z}_{3675}, \otimes)$.

(6.1) (10 Punkte) Welche der Gleichungen

1. $[726]_{3675} \otimes x = [35]_{3675}$
2. $[726]_{3675} \otimes x = [9]_{3675}$

besitzt eine Lösung x in $\mathbb{Z}_{3675}$? Falls Lösungen existieren, berechnen Sie alle Lösungen mit den in der Vorlesung verwendeten Verfahren. Falls keine Lösungen existieren, begründen Sie das.

$ggT(726, 3675) = 3 \qquad 3 \nmid 35$

m	u	y	s	t
3675	726	5	113	-572
726	45	16	-7	113
45	6	7	1	-7
6	3	2	0	1
3			1	0

$q = \frac{m}{ggT} = 1225$

$x_0 = n \cdot t = 1959$

$x_1 = 1959 + 1225 = 3184$

(6.2) (2 Punkte) Begründen Sie mit (6.1) warum $(\mathbb{Z}_{3675}, \otimes)$ keine Gruppe ist.

$x_2 = x_1 + 1225 = 4409 \mod 3675 = 734$

0 hat kein Inverses

Aufgabe 7 (11 Punkte)

(7.1) (3 Punkte) Geben Sie die Anzahl der teilerfremden natürlichen Zahlen von 1400 an. Geben Sie die Zwischenschritte Ihrer Berechnung an.

$\varphi(1400) = 1400 \cdot (1-\frac{1}{2}) \cdot (1-\frac{1}{5}) \cdot [1-\frac{1}{7}] = 480$

(7.2) (3 Punkte) Es wurde das Caesar-Chiffre-Verfahren verwendet um den Klartext

`BALDGESCHAFFT`

zu verschlüsseln. Welche der folgenden Geheimtexte kann dabei entstehen und geben Sie ggf. den Schlüssel dazu an. Begründen Sie Ihre Antwort.

`DCNFIGUEJCHHV, DCNFIGUE, CBNEHFTDIBGGU.`

✓ t 2

zu kurz

erst plus 1 dann +2

(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 Zwischenschritte Ihrer Berechnung an.

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

Aufgabe 8 (14 Punkte)

Für das RSA-Verfahren werden folgende Werte gewählt: $p = 13$, $q = 19$ und $e = 7$.

(8.1) (6 Punkte) Ermitteln Sie den öffentlichen und privaten Schlüssel. Geben Sie die Zwischenschritte Ihrer Berechnung an.

$n = p \cdot q = 13 \cdot 19 = 247$

offentliche Schlüssel: $(n, e) = (247, 7)$

$\varphi(n) = 216$

privater Schlüssel: $(n, d) = (247, 31)$

m	n	q	s	t
216	7	30	-1	31
7	6	1	1	-1
6	1	6	0	1
1			1	0

(8.2) (2 Punkte) Verschlüsseln Sie die Nachricht $m = 42$. Erläutern Sie Ihren Rechenweg.

$c = m^e \bmod n = 42^7 \bmod 247 = 120$

(8.3) (6 Punkte) Entschlüsseln Sie die Nachricht $c = 23$. Für die Berechnung sollen Sie den Square-and- Multiply-Algorithmus benutzen. Erläutern Sie Ihren Rechenweg.

$m = c^d \bmod n = 23^{31} \bmod n = 218$

$23 \bmod 247 = 23$

$23^2 \bmod 247 = 35$

$35^2 \bmod 247 = 237$

$237^2 \bmod 247 = 100$

$100^2 \bmod 247 = 120$

Aufgabe 9 (10 Punkte)

Alice und Bob möchten einen symmetrischen Schlüssel im Geheimen austauschen. Dazu verwenden Sie das Diffie-Hellman-Key-Exchange-Verfahren. Beide einigen sich auf $p = 43$ und $g = 3$.

(9.1) (1 Punkt) Welche Eigenschaft muss g erfüllen, damit dieses Verfahren funktioniert?

g muss erzeugendes Element von p sein

(9.2) (2 Punkte) Alice wählt im Geheimen $a = 11$ und verschickt $x := 30$ an Bob. Bob wiederum verschickt $y := 32$ an Alice. Wie lautet ihr gemeinsamer Schlüssel?

gemeinsamer Schlüssel:

$$g^a \bmod p = 32^{11} \bmod 43 = 22$$

(9.3) (7 Punkte) Berechnen Sie die geheime Zahl b von Bob mit Hilfe des Baby-Step-Giant-Step Algorithmus. Geben Sie alle Zwischenschritte Ihrer Berechnung an.

Hinweis: Das multiplikativ Inverse zu g ist 29 und zu x ist 33.

$$s = \lceil \sqrt{p-1} \rceil = 7 \qquad y \cdot g^{-r} \bmod p = 32 \cdot 29^r \bmod 43$$

$$g^{q \cdot 7} = 37^q \bmod 43$$

q	$37^q \bmod 43$
0	1
1	37
2	36
3	42
4	6
5	7
6	1

r	
0	32
1	25
2	37
3	
4	
5	
6	

$$b = q \cdot s + r = 1 \cdot 7 + 2 = 9$$

Leere Seite für Ihre Notizen

Leere Seite für Ihre Notizen

Viel Erfolg