Prof. Dr. Zimmermann

Klausur

Diskrete Mathematik 2 I168

2. Quartal 2021

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

Dauer: 90 min Seiten ohne Deckblatt 3 Datum: 23. Juni 2021

Hilfsmittel: Nordakademie Taschenrechner, Stifte (nicht rot).

Bemerkungen:

- Verwenden Sie zur Lösung der Aufgaben leere, bereitliegende Blätter.
- Bitte schreiben Sie auf jedes Lösungenblatt Ihren Namen die Matrikelnummer und Zenturie.
- Nummerieren Sie alle verwendeten Blätter!
- Geben Sie immer an zu welcher Aufgabe eine Lösung auf einem Blatt gehört!
- Bitte beachten Sie die gesondert zur Verfügung gestellten Hinweise für die Prüfungsdurchführung und für die Abgabe der Prüfungsleistung.
- Prüfungssprache ist Deutsch.
- Das Klausuraufgabenheft umfasst exkl. Deckblatt 3 Seiten. Bitte überprüfen Sie Ihr Aufgabenheft auf Vollständigkeit!
- Diese Klausur enthält 7 Aufgaben. Es können 100 Punkte erreicht werden. Zum Bestehen der Klausur benötigen Sie 50 Punkte.

Aufgabe:	1	2	3	4	5	6	7	Prozent:
Punktzahl:	18	11	13	22	10	13	13	100
Erreicht:								

Datum: _____ Note: _____ Ergänzungsprüfung: _____

Unterschrift: _____ Unterschrift: _____

Aufgabe 1 (18 Punkte)

In den folgenden Multiple Choice Aufgaben sind je 3 Aussagen richtig. Nennen Sie diese.

Bewertungshinweis: Es gibt maximal sechs Punkte pro Teilaufgabe.

- Wenn Sie mehr als drei Aussagen pro Teilaufgabe angeben, erhalten Sie keine Punkte.
- Finden Sie nur zwei richtige Aussagen pro Teilaufgabe, erhalten Sie drei Punkte.
- Finden Sie weniger als zwei richtige Aussagen pro Teilaufgabe, erhalten Sie keinen Punkt.

(1.1) (6 Punkte) Geben Sie die drei richtigen Aussagen an:

A) Sei M eine beliebige nichtleere Menge und $R \subseteq M \times M$. Dann gilt: $R \circ Id_M = Id_M$.

B) Seien M, N endliche Mengen. Es gilt: $|M \times N| = |M| \cdot |N|$.

C) Sei M eine Menge. Es gilt: $Id_M^{-1} = Id_M$.

D) Seien eine M eine Menge und $R \subseteq M \times M$.
Es gilt: R symmetrisch $\Rightarrow$ R reflexiv .

E) $\{(1,2),(3,2)\} \subseteq \{1,2,3\} \times \{1,2,3\}$ ist transitiv.

F) Die Teilbarkeits-Relation $| \subseteq \mathbb{Z} \times \mathbb{Z}$ ist antisymmetrisch.

(1.2) (6 Punkte) Geben Sie die drei richtigen Aussagen an:

A) Sei $\sqsubseteq$ eine Ordnungsrelation auf einer Menge M. Dann ist die Nachbarschaftsrelation $\sqsubseteq^N$ die kleinste transitive Relation, die in $\sqsubseteq$ enthalten ist.

B) Sei $\sqsubseteq$ eine Ordnungsrelation auf einer nichtleeren Menge M, dann sind alle Elemente von M obere Schranken von $\emptyset$.

C) Sei $M = \{1,2,3\}$. Es gilt: $\{(1,2),(1,3)\} \subseteq M \times M$ ist linkseindeutig.

D) Seien M, N endliche Mengen und $f : M \to N$ eine Abbildung.
Es gilt: f surjektiv $\Rightarrow$ f injektiv.

E) Sei M eine endliche Menge und $f : M \to M$ eine Abbildung.
Es gilt: f surjektiv $\Rightarrow$ f injektiv.

F) Seien M und N endliche Mengen mit $|M| = |N|$. Dann ist jede Abbildung $f : M \to N$ bijektiv.

(1.3) (6 Punkte) Geben Sie die drei richtigen Antworten an:

A) Die (additive!) Gruppe $(\mathbb{Z}_{17}, \oplus)$ hat ein Element der Ordnung 2.

B) $\left(\mathbb{Z}_{561} \setminus \left\{[0]_{561}\right\}, \otimes\right)$ ist eine Gruppe.

C) $(\mathbb{N}_0, +)$ ist keine Gruppe, aber eine algebraische Struktur.

D) Die Gleichung $a \otimes x = b$ ist für beliebige $a, b \in \mathbb{Z}_6 \setminus \{[0]_6\}$ lösbar.

E) Es gilt: $2019^{2021} \equiv_{2020} 2019$.

F) Es gilt: $[5]_5^{2021} = [5]_5$.

Aufgabe 2 (11 Punkte)

(2.1) (5 Punkte) Geben Sie auf der Menge $M := \{1, 2, 3\}$ Relationen R und S an so, dass

(a) R reflexiv, aber weder symmetrisch noch transitiv,

(b) S transitiv und nicht asymmetrisch ist.

(2.2) (6 Punkte) Seien M eine beliebige Menge und $R \subseteq M \times M$ und $S \subseteq M \times M$ beliebige transitive Relationen in M. Beweisen oder widerlegen Sie:

1. $R \cup S$ ist transitiv.
2. $R \cap S$ ist transitiv.

Aufgabe 3 (13 Punkte)

(3.1) (6 Punkte) Sei $M := \{1, 2, 3\}$. Geben Sie alle strikten, totalen Ordnungsrelationen auf M an.

(3.2) (7 Punkte) Es sei $\sqsubseteq$ eine Ordnungsrelation auf der M sowie $A \subseteq M$ und $s \in A$. Zeigen Sie: Ist s obere Schranke von A, so gilt $s = \sup(A)$. Geben Sie dazu die Definition von oberer Schranke und Supremum unter Verwendung von Quantoren an.

Aufgabe 4 (22 Punkte)

(4.1) (4 Punkte) Notieren Sie die Definition einer Äquivalenzrelation $\equiv$ auf einer Menge M mithilfe von Mengeninklusionen sowie die Definition der zugehörigen Äquivalenzklassen.

Sei die Relation $\equiv$ in $\mathbb{Z}$ definiert durch

$$\forall n, m \in \mathbb{Z} : n \equiv m \Leftrightarrow_{Def} n^2 + m = n + m^2 \, .$$

(4.2) (9 Punkte) Zeigen Sie, dass $\equiv$ eine Äquivalenzrelation auf $\mathbb{Z}$ ist.

(4.3) (3 Punkte) Zeigen Sie, dass für alle $n \in \mathbb{Z} : n \equiv -n + 1$.

(4.4) (3 Punkte) Geben Sie die Äquivalenzklassen $[0]_{\equiv}$, $[1]_{\equiv}$ und $[2]_{\equiv}$ explizit in aufzählender Darstellung an.

(4.5) (3 Punkte) Ist die Verknüpfung $[n]_{\equiv} \oplus [m]_{\equiv} := [n + m]_{\equiv}$ für $n, m \in \mathbb{Z}$ auf $\mathbb{Z}/\equiv$ wohldefiniert?

Hinweis: Es reicht, zur Verknüpfung die Äquivalenzklasse $[0]_{\equiv}$ mit verschiedenen Repräsentanten zu betrachten.

Aufgabe 5 (10 Punkte)

Welche der Gleichungen

1. $[9]_{24} \otimes x = [12]_{24}$
2. $[8]_{24} \otimes x = [12]_{24}$

besitzt eine Lösung x in $\mathbb{Z}_{24}$? Falls Lösungen existieren, berechnen Sie alle Lösungen **mit dem in den Vorlesung verwendeten Verfahren**. Falls keine Lösungen existieren, begründen Sie dies.

Aufgabe 6 (13 Punkte)

(6.1) (4 Punkte) Finden Sie in $\left(\mathbb{Z}_7 \setminus \left\{[0]_7\right\}, \otimes\right)$ ein Element mit maximaler Ordnung.

(6.2) (2 Punkte) Geben Sie eine nichttriviale Untergrupppe von $\left(\mathbb{Z}_7 \setminus \left\{[0]_7\right\}, \otimes\right)$ an.

(6.3) (7 Punkte) Geben Sie für $n = 2149$ und $n = 337$ jeweils die zu n **nicht** teilerfremden natürlichen Zahlen an, die kleiner als n sind. Berechnen Sie die Anzahl dieser Zahlen. Begründen sie ihre Berechnung.

Aufgabe 7 (13 Punkte)

Für das RSA-Verfahren werden folgende Werte gewählt: $p = 17$, $q = 19$ und $e = 11$.
Geben Sie in den folgenden Teilaufgaben stets einen nachvollziehbaren Rechenweg an:

(7.1) (6 Punkte) Bestimmen Sie den öffentlichen und den privaten Schlüssel.

(7.2) (2 Punkte) Verschlüsseln Sie die Nachricht $m = 38$.

(7.3) (5 Punkte) Entschlüsseln Sie die Nachricht $c = 21$ mithilfe des Square-and-Multiply-Algorithmus.