KLAUSUR

NORDAKADEMIE
HOCHSCHULE DER WIRTSCHAFT

Prüfer:
Brzezinski, Christiansen, Ullmann, Zimmermann

Studiengang:	Modul:	
AINF / WINF	Diskrete Mathematik 2 I168	
Datum:	Uhrzeit:	Dauer:
25.2.2021	9:15 Uhr - 10:45 Uhr	90

Zugelassene Hilfsmittel: Nordakademie Taschenrechner.

Aufgabenheft

Wichtige Hinweise:

- Verwenden Sie zur Lösung der Aufgaben leere, bereitliegende Blätter.
- Bitte schreiben Sie auf jedes Lösungenblatt Ihren Namen / Ihre Matrikelnummer und Ihre 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 inkl. 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.

Viel Erfolg!

1. Relationen allgemein (Gesamtpunkte für die Aufgabe: 13)

   (1.1) (5 Punkte) Gegeben ist die Menge $M = \{1, 2, 3, 4, 5\}$ und die Relation

   $$R = \{(1, 2), (1, 3), (3, 5), (5, 1), (2, 4)\}.$$

   Erstellen Sie ein vereinfachtes Pfeildiagramm der transitiven Hülle R^+.

   (1.2) (4 Punkte) Sei M eine beliebige zweielementige Menge. Wie viele symmetrische und wie viele asymmetrische Relationen $R \subseteq M \times M$ gibt es?

   (1.3) (4 Punkte) Sei M eine beliebige endliche Menge. Wie viele symmetrische Relationen gibt es? Begründen sie Ihre Antwort.

2. Ordnungsrelationen (Gesamtpunkte für die Aufgabe: 14)

   (2.1) (6 Punkte) Sei M eine nichtleere durch die Ordnungsrelation $\sqsubseteq$ geordnete Menge und $A \subseteq M$. Beweisen oder widerlegen Sie

   1. Wenn g größtes Element von A ist, dann ist g nicht untere Schranke von A.
   2. Wenn g gleichzeitig größtes und kleinstes Element von A ist, dann sind alle Elemente von A gleich g.

   (2.2) (8 Punkte) Konstruieren Sie eine Menge M mit vier Elementen, eine Ordnungsrelation $\sqsubseteq$ auf M und eine zweielementige Teilmenge $A \subseteq M$ mit der folgenden Eigenschaft:

   - A hat zwei maximale Elemente,
   - A hat zwei minimale Elemente,
   - A hat ein Supremum aber
   - A hat kein Infimum

   Ihre Antwort zu der Aufgabe besteht aus einem Hasse Diagramm mit Markierungen der Menge A, der minimalen und maximalen Elemente und des Supremums.

3. Äquivalenzrelationen und Unabhängigkeit vom Repräsentanten (Gesamtpunkte für die Aufgabe: 25)

   Gegeben sei die Menge $\mathbb{R}^2$ und die Relation $\equiv$ die durch

   $$\forall (x_1, x_2), (y_1, y_2) \in \mathbb{R}^2 : (x_1, x_2) \equiv (y_1, y_2) :\Leftrightarrow \exists c \in \mathbb{R} \setminus \{0\} : x_1 = c \cdot y_1 \wedge x_2 = c \cdot y_2$$

   (3.1) (4 Punkte) Geben Sie die Definition einer Äquivalenzrelation $\equiv$ in einer Menge M sowie die Definition einer Äquivalenzklasse.

   (3.2) (4 Punkte) Zeichen Sie in ein kartesisches Koordinatensystem die Punkte $(0, 1), (0, 2), (0, 3)$ und $(2, 1), (4, 2), (6, 3)$ ein und kennzeichnen Sie die zueinander äquivalenten Punkte. Was haben die Punkte einer Äquivalenzklasse geometrisch gemein?

   (3.3) (8 Punkte) Beweisen Sie, dass $\equiv$ eine Äquivalenzrelation auf $\mathbb{R}^2$ ist.

   (3.4) (4 Punkte) Geben Sie die Äquivalenzklassen $[(0, 0)]_\equiv$, $[(0, 1)]_\equiv$ an.

   (3.5) (5 Punkte) Zeigen Sie dass die Definition

   $$[(x_1, x_2)]_\equiv \otimes [(y_1, y_2)]_\equiv := [(x_1 \cdot y_1 - x_2 \cdot y_2, x_1 \cdot y_2 + x_2 \cdot y_1)]_\equiv$$

   unabhängig vom Repräsentanten ist.

4. Restklassengleichungen (Gesamtpunkte für die Aufgabe: 12)

   Gehen Sie zum Lösen der Gleichungen nach dem in der Vorlesung vermittelten Verfahren vor. Stellen Sie die Gleichungen dafür zunächst in eine aus der Vorlesung bekannte Form um.

   1. $([x]_{700} \otimes [273]_{700}) \oplus [5]_{700} = [25]_{700}$
   2. $([x]_{700} \otimes [273]_{700}) \oplus [5]_{700} = [26]_{700}$

   (4.1) (4 Punkte) Welche der Restklassengleichungen hat mindestens eine Lösung?

   (4.2) (8 Punkte) Wenn mindestens eine Lösung existiert, berechnen Sie alle.

5. Restklassengruppen (Gesamtpunkte für die Aufgabe: 9)

   (5.1) (2 Punkte) Ermitteln Sie die Ordnung von $[5]_{13}$ in $\left(\mathbb{Z}_{13} \setminus \{[0]_{13}\}, \otimes\right)$. Geben Sie dabei alle Rechenwege an.

   (5.2) (4 Punkte) Geben Sie eine dreielementige Untergrupppe von $\left(\mathbb{Z}_7 \setminus \{[0]_7\}, \otimes\right)$ an.

   (5.3) (3 Punkte) Geben Sie für $n = 501$ und $n = 941$ jeweils die Anzahl der teilerfremden natürlichen Zahlen kleiner als n an. Geben Sie die Zwischenschritte Ihrer Berechnung an.

6. Kyptographie allgemein (Gesamtpunkte für die Aufgabe: 9)

   (6.1) (6 Punkte) Notieren Sie bei dieser Aufgabe zu jeder Aussagen-Nummer ein „w“ für wahr oder ein „f“ für falsch.

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

   1. Bei symmetrischen Verschlüsselungsverfahren kann man aus dem Schlüssel zum Entschlüsseln in annehmbarer Zeit den Schlüssel zum Verschlüsseln berechnen.
   2. Das Kerckhoffs'sche Prinzip besagt, dass die Sicherheit des Verschlüsselungsverfahrens nur von der Geheimhaltung des Schlüssels abhängen darf.
   3. Permutations-Chiffren sind polyalphabetische Substitutionsverfahren.
   4. Die Sicherheit des RSA-Verfahrens basiert darauf, dass die Multiplikation zweier (sehr großer) Primzahlen ein nicht in annehmbarer Zeit lösbares Problem ist.
   5. Beim RSA-Verfahren verschlüsselt der Absender einer Nachricht mit dem öffentlichen Schlüssel des Empfängers der Nachricht.
   6. Das Ergebnis des Miller-Rabin-Tests lautet entweder „n ist eine Primzahl“oder „n ist wahrscheinlich keine Primzahl“.

   (6.2) (3 Punkte) Begründen Sie, welche der folgenden Geheimtexte aus dem Klartext `CORONA` bei Anwendung des Caesar-Chiffre-Verfahrens resultieren können und welche nicht.

   (a) `AMPMLY` (b) `DPSNOB` (c) `BNQNM`

7. RSA Verfahren (Gesamtpunkte für die Aufgabe: 18)

   Für das RSA-Verfahren werden folgende Werte gewählt: $p = 7$, $q = 29$ und $e = 5$.
   Geben Sie in den folgenden Teilaufgaben stets einen nachvollziehbaren Rechenweg an:

   (7.1) (5 Punkte) Überprüfen Sie mit dem Miller–Rabin–Test, ob q eine Primzahl ist. Verwenden Sie dabei die Basen $a = 3$ und $a = 8$. Geben Sie sämtliche Zwischenschritte an.

   (7.2) (6 Punkte) Bestimmen Sie den öffentlichen und den privaten Schlüssel für das RSA-Verfahren.

   (7.3) (2 Punkte) Verschlüsseln Sie die Nachricht $m = 42$.

   (7.4) (5 Punkte) Entschlüsseln Sie die Nachricht $c = 35$ mit dem Square-and-Multiply-Algorithmus.