Nachklausur zur Vorlesung „Diskrete Mathematik für Informatiker“

SS 16, 08. September 2016

Vorname: _____

Nachname: _____

Matrikelnummer: _____

Aufgabe	**Punktzahl**	**Erreicht**
1	20	
2	6	
3	8	
4	4	
5	8	
6	6	
7	11	
8	10	
9	4	
10	5	
11	10	
12	9	
13	10	
14	9	
Σ	120	

Generelle Hinweise:

- Prüfungsdauer: **180 Minuten**
- Wenn Sie in der Klausur **60 Punkte** erreichen, haben Sie mit Sicherheit bestanden.
- Hilfsmittel: Ein beidseitig beschriebenes DIN-A4-Blatt.
- Benutzen Sie ein **dokumentenechtes Schreibgerät**.
- Überprüfen Sie die Ihnen ausgehändigte Klausur auf Vollständigkeit (**14 Aufgaben** auf 18 Seiten inkl. Deckblatt, Punkte und Hinweise).
- Tragen Sie **auf jedes Blatt** Ihren **Namen** und Ihre **Matr.-Nr.** in die entsprechenden Felder ein.
- Schreiben Sie Ihre Lösungen in die dafür vorgesehenen Felder. Reicht der Platz in einem Feld nicht aus, so benutzen Sie die Rückseite des entsprechenden Blattes und vermerken Sie dies auf der Vorderseite. Reicht der Platz dennoch nicht aus, können Sie die Aufsicht nach zusätzlichen Blättern fragen.
- Schreiben Sie bitte **deutlich**. Unleserliche Lösungen sind ungültig.
- Ein **Täuschungsversuch** führt umgehend zum Ausschluss und **Nicht-bestehen**. Es erfolgt keine Vorwarnung.
- Alle mitgeführten **elektronischen Geräte** sind vor der Klausur bzw. spätestens jetzt auszuschalten. Auch angeschaltete Mobiltelefone werden als Betrugsversuch gewertet.

Aufgabe 1. (20 Punkte) In jeder der 10 Teilaufgaben gibt es drei mögliche Antworten, von denen eins, zwei oder auch alle drei Antworten richtig sein können. Für jede Teilaufgabe gibt es 2 Punkte, die nur vergeben werden, wenn **alle** Kreuze innerhalb der Teilaufgabe richtig gesetzt wurden.

(1) Für zwei disjunkte Mengen A und B gilt:
- ◯ $A \setminus B$ und $B \setminus A$ sind disjunkt
- ◯ Das Komplement von A und das Komplement von B sind disjunkt.
- ◯ $B \subseteq B \setminus A$

(2) Für alle unendlich abzählbaren Mengen A gilt:
- ◯ Es gibt eine Menge $B \neq A$, so dass $A = A \cup B$ und $|B| = |A|$
- ◯ Es gibt eine Menge $B \neq A$, so dass $A = A \cup B$ und $|B| \neq |A|$
- ◯ $|A| = |A \times A|$

(3) Seien G_1 und G_2 Gruppen und $f : G_1 \to G_2$ ein injektiver Gruppenhomomorphismus und sei e das neutrale Element von G_2.

◯ $|\ker(f)| = 1$ ◯ $\ker(f) = G_1$ ◯ $f(\ker(f)) = \{e\}$

(4) Es gibt eine Relation R, die...
- ◯ ...reflexiv und irreflexiv ist.
- ◯ ...weder reflexiv noch irreflexiv ist.
- ◯ ...symmetrisch und antisymmetrisch ist.

(5) Der vollständige Graph K_n besitzt...
- ◯ ...$\binom{n}{2}$ Kanten
- ◯ ...ein Matching der Größe $n/2$, falls n gerade ist, und $(n-1)/2$, falls n ungerade ist.
- ◯ ...ein perfektes Matching genau dann, wenn n gerade ist.

(6) Für jeden planaren Graphen G gilt

◯ $\mu(G) = \gamma(G)$ ◯ G enthält keine Unterteilung des K_5. ◯ $\chi(G) \leq 3$

(7) $(\{1, -1\}, \cdot)$ ist isomorph zu einer Untergruppe von

◯ $(\mathbb{Z}, +)/4\mathbb{Z}$ ◯ S_3 ◯ $(\mathbb{Z}_3, +_3)$

(8) Seien G_1 und G_2 isomorphe Gruppen. Dann gilt:
- ◯ $|G_1| = |G_2|$
- ◯ Es gibt einen bijektiven Homomorphismus von G_1 nach G_2.
- ◯ Jeder Homomorphismus von G_1 nach G_2 ist bijektiv.

(9) Seien k und $n = p \cdot q$ der Kodierungsschlüssel und l der Dekodierungsschlüssel im RSA-Verfahren und φ die Eulersche φ -Funktion. Eine kodierte Nachricht kann mit folgender Kenntnis effizient dekodiert werden:

◯ n, k und p ◯ n, k und $n \cdot k$ ◯ n, k und $\varphi(n)$

(10) Für jeden Körper $(K, +, \cdot)$ gilt
- ◯ $K \setminus \{0\}$ ist bezüglich $\cdot$ eine abelsche Gruppe.
- ◯ K ist bezüglich $+$ eine abelsche Gruppe.
- ◯ K ist bezüglich $+$ eine zyklische Gruppe.

Aufgabe 2. (6 Punkte)
Sei $A_i = \{n \in \mathbb{N} \mid n < i\}$.

(a) Bestimmen Sie A_4.

(b) Zeigen Sie, dass $\bigcup_{i \in \mathbb{N}} A_i = \mathbb{N}$.

(c) Zeigen Sie, dass $\bigcap_{i \in \mathbb{N}} A_i = \emptyset$.

Aufgabe 3. (8 Punkte) Geben Sie für jede der folgenden Funktionen an, ob sie injektiv bzw. surjektiv ist. Begründen Sie Ihre Antwort, falls eine Eigenschaft nicht erfüllt ist.

(a) $f : \mathbb{Z} \to \mathbb{N}$ mit $f(x) = |x|$

(b) $g : \mathbb{N} \to \mathbb{Z}$ mit $g(x) = \begin{cases} x/2 & \text{falls } x \text{ gerade} \\ (x-1)/2 & \text{falls } x \text{ ungerade} \end{cases}$

(c) $h : \{2x \mid x \in \mathbb{N}\} \to \mathbb{N}$ mit $h(x) = x/2$

(d) $i : \emptyset \to \{0\}$

Aufgabe 4. (4 Punkte) Geben Sie jeweils an, ob es sich bei folgenden Relationen um eine symmetrische bzw. transitive Relation handelt. Begründen Sie jede nicht zutreffende Eigenschaft mit einem konkreten Gegenbeispiel.

(a) $R_1 = \{(a, b) \in \mathbb{Z} \times \mathbb{Z} \mid a|b\}$

(b) $R_2 = \{(a, b) \in \mathbb{Z} \times \mathbb{Z} \mid |a - b| > 1\}$

(c) $R_3 = \{(a, b) \in \mathbb{Z} \times \mathbb{Z} \mid a \cdot b = 1\}$

Aufgabe 5. (8 Punkte) Zeigen Sie folgende Aussagen für alle $n \in \mathbb{N}$ mittels vollständiger Induktion:

(a) $2^n \leq (n+1)!$

(b) $n^2 + n$ ist gerade

Aufgabe 6. (6 Punkte) Bei den folgenden kombinatorischen Aufgaben genügt es, die Berechnungsvorschrift mit entsprechenden Zahlen anzugeben. Die Rechnungen müssen also nicht ausgeführt werden.

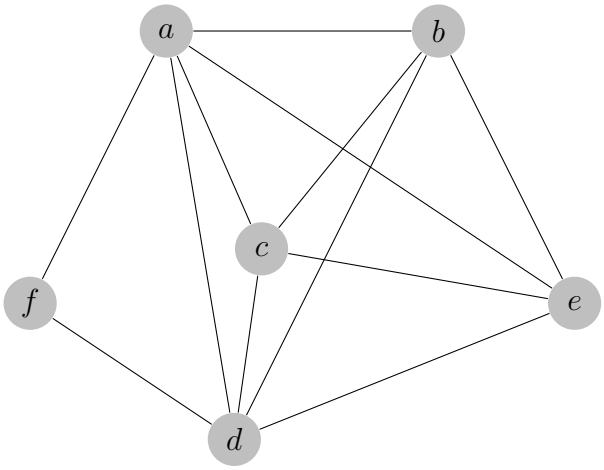
(a) Wie viele Relationen $R \subseteq M \times M$ gibt es über einer Menge M mit 100 Elementen?

(b) In einem Kartenspiel gibt es 100 verschiedene Karten, von denen 10 gezogen werden. Wie viele Möglichkeiten gibt es dafür?

(c) In der Mensa gibt es zehn Arten von Beilagen (wobei wir davon ausgehen, dass jede Beilage unbegrenzt vorhanden ist). Wie viele Möglichkeiten gibt es, drei Beilagen auszuwählen?

(d) Nach der Klausur verlassen alle 120 Studenten nacheinander den Raum. Wie viele Möglichkeiten gibt es hierfür?

Aufgabe 7. (11 Punkte) Gegeben sei folgender Graph G:



(a) Ist G planar? Wenn ja, geben Sie eine planare Zeichnung des Graphen an! Wenn nein, begründen Sie Ihre Antwort.

(b) Geben Sie die Matchingzahl $\mu(G)$ und ein dazugehöriges Matching an. Ist das Matching perfekt?

(c) Geben Sie die Knotenüberdeckungszahl $\gamma(G)$ und die Färbungszahl $\chi(G)$ an.

(d) Ist G bipartit? Wenn ja, geben Sie die beiden Partitionen an! Wenn nein, begründen Sie Ihre Antwort.

(e) Hat G einen Eulerweg bzw. Eulerkreis? Begründen Sie Ihre Antwort.

Aufgabe 8. (10 Punkte) Gegeben die Gruppe $G = (\mathbb{Z}_3 \times \mathbb{Z}_2, \oplus)$, wobei $\oplus$ komponentenweise definiert ist.

(a) Handelt es sich um eine Abelsche Gruppe?

(b) Wie viele Elemente hat G?

(c) Geben Sie das neutrale Element der Gruppe an.

(d) Geben Sie das inverse Element zu $(2, 1)$ an.

(e) Gibt es eine Untergruppe mit fünf Elementen? Begründen Sie Ihre Antwort.

(f) Geben Sie eine Untergruppe von G mit zwei Elementen an.

(g) Die Menge $U = \{(z, 0) \mid z \in \mathbb{Z}_3\}$ ist eine Untergruppe von G. Geben Sie die Linksnebenklassen von U an. Ist U ein Normalteiler? Begründen Sie Ihre Antwort.

Aufgabe 9. (4 Punkte) Berechnen Sie 5^{76} mod 7. Geben Sie Ihren Lösungsweg an.

Aufgabe 10. (5 Punkte) Berechnen Sie mit Hilfe des Euklidischen Algorithmus $\mathrm{ggT}(110, 405)$ sowie Zahlen x und y mit $\mathrm{ggT}(110, 405) = x \cdot 110 + y \cdot 405$.

Aufgabe 11. (10 Punkte) Gegeben seien die Polynome $p(x) = x^4 + x^2 - 2x + 1$ und $q(x) = x^2 - 1$ mit Koeffizienten aus $\mathbb{Q}$.

Berechnen Sie $p(x)$ div $q(x)$, $p(x)$ mod $q(x)$ und $\mathrm{ggT}(p(x), q(x))$.

Aufgabe 12. (9 Punkte) Gegeben sind die öffentlichen Schlüssel $n = 21$ und $k = 7$ für eine RSA-Kodierung.

(a) Kodieren Sie die Nachricht 5.

(b) Bestimmen Sie die privaten Schlüssel $\varphi(n)$, l und dekodieren Sie die Nachricht 2.

Aufgabe 13. (10 Punkte) Bestimmen Sie $x \in \mathbb{Z}_{42}$ mit

$$1 \equiv x \bmod 2$$

$$1 \equiv x \bmod 3$$

$$5 \equiv x \bmod 7$$

Aufgabe 14. (9 Punkte)

(a) Geben Sie die Elemente von $\mathbb{Z}_8^*$ und die Multiplikationstabelle von $(\mathbb{Z}_8^*, \cdot_8)$ an.

(b) Geben Sie einen Isomorphismus von $(\mathbb{Z}_8^*, \cdot_8)$ zu $(\mathbb{Z}_2, +_2) \times (\mathbb{Z}_2, +_2)$ an. Begründen Sie, dass es sich um einen Isomorphismus handelt.

(c) Ist $(\mathbb{Z}_8^*, \cdot_8)$ isomorph zu $(\mathbb{Z}_4, +_4)$? Begründen Sie Ihre Antwort.