Diskrete Mathematik für Studierende der Informatik
WiSe 2021/2022
E. Viada / T. Höpfner
Probeklausur

Matrikel-Nr.	

- Die Bearbeitungszeit beträgt **80 Minuten**[1].
- Erlaubte Hilfsmittel sind nur Schreibwerkzeuge (kein Bleistift, nur schwarz oder blau). Insbesondere keine Taschenrechner und beschriftete Zettel!
- Grundlegende Rechenschritte und Begründungen sind jeweils anzugeben. Unzureichende Begründungen können zu Punktabzug führen.
- Nicht links oben in die Ecke schreiben und rechts einen kleinen Rand (2 cm) lassen.
- Keine Schmierblätter mit abgeben (Können nicht bewertet werden).

DIESEN ABSCHNITT BITTE NICHT AUSFÜLLEN!

1	2	3	4	5	6	7	8	9	10	11	Σ
											/102

Name: _____

Note: _____

[1] Die Probeklausur ist von der Länge her etwas kürzer als die tatsächlichen Klausuren. Dort wird der Multiple-Choice Teil etwas länger sein (ca. 20% der Punkte).

Aufgabe 1 (12 Punkte)**.** Markieren Sie für jede Teilaufgabe alle Aussage die wahr sind:

⊗ Diese Aussage ist wahr. ○ Diese Aussage ist falsch.

Sie erhalten nur dann Punkte auf eine Teilaufgabe, wenn Sie genau alle wahren Aussagen ankreuzen. Begründungen sind hier nicht gefordert.
Sollten Sie ihre Antwort ändern wollen, schreiben Sie bitte deutlich wahr / falsch neben die Antwortmöglichkeiten.

a) (2P.) Seien A und B zwei disjunkte Mengen. Dann gilt:

- ○ $A \setminus B$ und $B \setminus A$ sind disjunkt
- ○ Das Komplement von A und das Komplement von B sind disjunkt
- ○ $B \setminus A \subset B$

b) (2P.) Sei $n \in \mathbb{N}_+$ und R die Relation auf $\mathbb{Z}$, gegeben durch $(a, b) \in R$ genau dann, wenn $n | b - a$.

- ○ R ist eine Äquivalenzrelation
- ○ Die Äquivalenzklassen von R sind paarweise disjunkt
- ○ $R \subset \mathbb{Z} \times \mathbb{Z}$

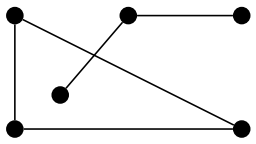
c) (2P.) Sei $p \geq 3$ eine Primzahl. Dann gilt:

- ○ $\varphi(p)$ ist gerade
- ○ $7^p \equiv 1 \mod p$
- ○ $2x \equiv n \mod p$ besitzt genau dann eine Lösung $x \in \mathbb{Z}/p\mathbb{Z}$, wenn $n \in \mathbb{Z}$ gerade ist

d) (2P.) Für jeden beliebigen Körper $(K, +, \cdot)$ gilt:

- ○ $(K, +)$ ist eine Gruppe
- ○ $(K, \cdot)$ ist eine Gruppe
- ○ $(K, +, \cdot)$ ist ein Ring

e) (2P.) Gegeben sei der Graph G aus der Abbildung rechts.



- ○ G ist zusammenhängend
- ○ G ist planar
- ○ G ist eulersch

f) (2P.) Sei p eine Primzahl. Dann gilt für jedes $0 \leq k \leq p - 1$ so, dass $[k] \in (\mathbb{Z}/p\mathbb{Z})^*$:

- ○ $k^2 \not\equiv 1 \mod p$
- ○ Die Ordnung von $[k]$ teilt $\varphi(p)$
- ○ $[k]$ erzeugt $(\mathbb{Z}/p\mathbb{Z})^*$

Aufgabe 2 (5 Punkte)**.** Gegeben sei die Relation

$$R = \{(a, b) \in \mathbb{Z} \times \mathbb{Z} \mid a \cdot b > 0\}.$$

Prüfen Sie, ob diese Relation reflexiv, symmetrisch und/oder transitiv ist. Handelt es sich bei R um eine Äquivalenzrelation?

Aufgabe 3 (5+5 Punkte)**.**

a) Gegeben sei die Funktion $f\colon \mathbb{R} \to \mathbb{R}$ mit $f(x) = |x|$. Bestimmen Sie, ob f injektiv, surjektiv und/oder bijektiv ist. Begründen Sie Ihre Antwort kurz.

b) Gegeben sei die Funktion $f\colon \mathbb{N} \to \mathbb{N}$ mit $f(n) = |n|$. Bestimmen Sie, ob f injektiv, surjektiv und/oder bijektiv ist. (Hierbei ist $0 \in \mathbb{N}$.) Begründen Sie Ihre Antwort kurz.

Aufgabe 4 (5 Punkte)**.** Zeigen Sie, dass die folgende logische Aussage eine Tautologie (also immer wahr) ist:

$$\neg(\neg A \wedge (A \vee B)) \vee B$$

Aufgabe 5 (10 Punkte)**.** Zeigen Sie mithilfe der vollständigen Induktion für alle $n \in \mathbb{N}$, dass $7^{2n} - 2^n$ durch 47 teilbar ist. (Hier ist $0 \in \mathbb{N}$.)

Aufgabe 6 (5+5 Punkte)**.** Gegeben sei ein Kartenspiel mit 52 Karten.
Jede Karte trägt eine der 13 Zahlen $\{2, 3, 4, 5, 6, 7, 8, 9, 10, \mathrm{J}, \mathrm{D}, \mathrm{K}, \mathrm{A}\}$ und eine der 4 Farben $\{\clubsuit, \blacklozenge, \spadesuit, \heartsuit\}$, sodass es jede der $4 \cdot 13 = 52$ Kombinationen genau einmal gibt.

a) Auf wie viele Möglichkeiten lassen sich die 52 Karten auf 4 Stapel mit je 13 Karten aufteilen? Begründen Sie Ihre Antwort.

b) Wie viele Möglichkeiten gibt es, mit 5 mal ziehen eine "Straße" der Form $2, 3, 4, 5, 6$ zu ziehen? Begründen Sie Ihre Antwort.
(Hierbei sind $2\heartsuit, 3\clubsuit, 4\clubsuit, 5\heartsuit, 6\spadesuit$ und $3\clubsuit, 6\spadesuit, 4\clubsuit, 2\heartsuit, 5\heartsuit$ zwei verschiedene Möglichkeiten.)

Binomialkoeffizienten, Fakultäten und Ähnliches können Sie unausgerechnet stehen lassen.

Aufgabe 7 (5+5 Punkte)**.**

a) Berechnen Sie $\mathrm{ggT}(21, 161)$ mithilfe des euklidischen Algorithmus.

b) Bestimmen Sie $x, y \in \mathbb{Z}$, sodass $21x + 161y = \mathrm{ggT}(21, 161)$.

Aufgabe 8 (7+3 Punkte)**.**

a) Bestimmen Sie alle Lösungen für das folgende System von Kongruenzen:

$$2x \equiv 3 \mod 5, \qquad 2x \equiv 5 \mod 7 \qquad \text{und} \qquad 3x \equiv 2 \mod 13$$

b) Gegeben seien k Kongruenzen

$$x \equiv a_i \mod n_i,$$

wobei $i = 1, ..., k$ und n_i paarweise teilerfremde Zahlen sind. Beschreiben Sie mithilfe geeigneter Formeln, wie sich alle x, welche alle Kongruenzen gleichzeitig lösen, finden lassen.

Aufgabe 9 (10 Punkte)**.** Sei $K = \mathbb{Z}/5\mathbb{Z}$. Berechnen Sie $q(x)$ und $r(x)$ in $K[X]$, sodass

$$f(x) = q(x) \cdot g(x) + r(x)$$

wobei $f(x) = [4]x^4 - [2]x^3 + [2]x^2 - x + [1]$ und $g(x) = [2]x^2 + [3]$ aus $K[X]$ sind und $\mathrm{Grad}(g) > \mathrm{Grad}(r)$ gelten soll.

Aufgabe 10 (3+3+4 Punkte)**.** Gegeben sind die öffentlichen Schlüssel $N = 51$ und $e = 11$ für eine RSA-Kodierung.

a) Kodieren Sie die Nachricht 2.

b) Bestimmen Sie die privaten Schlüssel d und $\varphi(N)$.

c) Dekodieren Sie die Nachricht 4.

Aufgabe 11 (10 Punkte)**.** Der folgende Beweis über vollständige Induktion ist falsch. Geben Sie an, wo sich der Fehler befinden und begründen Sie Ihre Aussage.

Wir behaupten, dass die folgende Aussage für alle $n \in \mathbb{N}_+$ gilt:

$$n = \sqrt{1 + (n-1)\sqrt{1 + n\sqrt{1 + (n+1)\sqrt{1 + (n+2)\sqrt{\dots}}}}}$$

(Der rechte Ausdruck ergibt für alle $n \in \mathbb{N}_+$ eine endliche Zahl, das dürfen Sie als wahr hinnehmen.)

Induktionsanfang: Für $n = 1$ ist zu zeigen, dass

$$1 \quad \stackrel{!}{=} \quad \sqrt{1} = \sqrt{1 + 0\sqrt{\dots}}$$

was erfüllt ist.

Induktionsvoraussetzung: Wir nehmen an, dass es ein $n \in \mathbb{N}_+$ gibt, sodass:

$$n = \sqrt{1 + (n-1)\sqrt{1 + n\sqrt{1 + (n+1)\sqrt{1 + (n+2)\sqrt{\dots}}}}}$$

Induktionsschritt: Wir zeigen nun, dass die Aussage dann auch für $n + 1$ gilt.
Nach Induktionsvoraussetzung ist:

$$n = \sqrt{1 + (n-1)\sqrt{1 + n\sqrt{1 + (n+1)\sqrt{1 + (n+2)\sqrt{\dots}}}}}$$

Wir quadrieren beide Seiten, dann erhalten wir:

$$n^2 = 1 + (n-1)\sqrt{1 + n\sqrt{1 + (n+1)\sqrt{1 + (n+2)\sqrt{\dots}}}} \quad \Big| -1$$

$$\longleftrightarrow \quad (n-1)(n+1) = n^2 - 1 = (n-1)\sqrt{1 + n\sqrt{1 + (n+1)\sqrt{1 + (n+2)\sqrt{\dots}}}} \quad \Big| : (n-1)$$

$$\longleftrightarrow \quad n + 1 = \frac{(n-1)(n+1)}{n-1} = \sqrt{1 + n\sqrt{1 + (n+1)\sqrt{1 + (n+2)\sqrt{\dots}}}}$$

Aus der letzten Zeile lesen wir nun die Aussage für $n + 1$ ab, sodass der Induktionsschritt gilt.