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

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. Es ist jeweils mindestens eine der Aussagen wahr. Begründungen sind hier nicht gefordert.
Sollten Sie ihre Antwort ändern wollen, schreiben Sie bitte deutlich wahr / fasch 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
- ⊗ $R \subset \mathbb{Z} \times \mathbb{Z}$

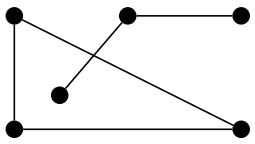
c) (2P.) Sei $p \geq 3$ eine Primzahl. Dann gilt:

- ⊗ $\varphi(p)$ 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?

Lösung.
Da $0 \cdot 0 = 0 \not> 0$ ist, ist $(0, 0) \notin R$ und somit ist R nicht reflexiv.

Da aus $(a, b) \in R$ folgt, dass $ba = ab > 0$ ist, ist auch $(b, a) \in R$ und somit ist R symmetrisch.

Wenn $(a, b) \in R$ und $(b, c) \in R$, dann ist $ab > 0$, das heißt $a \neq 0, b \neq 0$ und a und b haben das selbe Vorzeichen, also $a > 0, b > 0$ oder $a < 0, b < 0$. Ebenso $b > 0, c > 0$ oder $b < 0, c < 0$. Damit muss also gelten, dass $a \neq 0$ und $c \neq 0$ und entweder $a < 0, b < 0, c < 0$ oder $a > 0, b > 0, c > 0$. In beiden Fällen ist $ac > 0$ und somit $(a, c) \in R$. Also ist R transitiv.

Da R nicht reflexiv ist, handelt es sich bei R um keine 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.

Lösung.

a) Die Funktion ist nicht injektiv, da $f(-1) = 1 = f(1)$.

Die Funktion ist nicht surjektiv, da $f(x) = |x| \neq -1$ für alle $x \in \mathbb{R}$, also -1 nicht im Bild liegt.

Insbesondere ist die Funktion nicht bijektiv.

b) Als Funktion $\mathbb{N} \to \mathbb{N}$ ist f injektiv, da $f(n) = |n| = n$ und somit aus $n = f(n) = f(m) = m$ auch $n = m$ folgt.

Ebenso ist f surjektiv, da für jedes $n \in \mathbb{N}$ im Bild gilt, dass $f(n) = n$.

Somit ist f hier bijektiv.

□

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

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

Lösung.
Wir benutzen eine Wahrheitstabelle:

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

Wir sehen nun, dass $\neg(\neg A \wedge (A \vee B)) \vee B$ immer wahr ist, also eine Tautologie.

□

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 $0 \in \mathbb{N}$.)

Lösung.
Induktionsanfang: Für $n = 0$ gilt:

$$7^0 - 2^0 = 1 - 1 = 0$$

und 47 teilt 0, also ist die Aussage für $n = 0$ wahr.

Induktionsvoraussetung: Wir nehmen an, für ein $n \in \mathbb{N}$ gilt $7^{2n} - 2^n$ ist durch 47 teilbar.

Induktionsschritt: Dann folgt für $n + 1$, dass

$$\begin{aligned} 7^{2(n+1)} - 2^{n+1} &= 7^2 \cdot 7^{2n} - 2 \cdot 2^n = 49 \cdot 7^{2n} - 2 \cdot 2^n \\ &= 47 \cdot 7^{2n} + 2 \cdot 7^{2n} - 2 \cdot 2^n = \underbrace{47 \cdot 7^{2n}}_{\text{teilbar durch } 47} + 2 \cdot \underbrace{(7^{2n} - 2^n)}_{\text{teilbar nach } \mathbf{IV}} \end{aligned}$$

Insbesondere ist also auch $7^{2(n+1)} - 2^{n+1}$ durch 47 teilbar, wie zu zeigen war.
Damit ist die Induktion vollständig und die Aussage gezeigt. □

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.

Lösung.

a) Für den ersten Stapel können 13 aus den 52 Karten gewählt werden, hierfür gibt es $\binom{52}{13}$ Möglichkeiten.

Für den zweiten Stapel können dann 13 aus den verbleibenden $52 - 13 = 39$ Karten gewählt werden, hierfür gibt es $\binom{39}{13}$ Möglichkeiten.

Für Stapel drei dann $\binom{26}{13}$ und für den letzten Stapel bleiben nur die letzten Karten übrig.

Es gibt daher insgesamt $\binom{52}{13}\binom{39}{13}\binom{26}{13}$ Möglichkeiten, die Karten auf viel Stapel aufzuteilen.

b) Wir brauchen eine 2, hierfür gibt es 4 Möglichkeiten. Ebenso für die Karten mit 3,4,5,6.

Ohne auf die Reihenfolge zu achten, gibt es also 4^5 mögliche Kombinationen aus Karten, die wir am Ende auf der Hand haben können.

Für jede dieser Kombination gibt es zudem 5! mögliche Reihenfolgen, in denen wir diese 5 Karten ziehen können.

Daher gibt es insgesamt $5! \cdot 4^5$ Möglichkeiten, eine solche Straße zu ziehen.

□

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 $21x + 161y = \mathrm{ggT}(21, 161)$.

Lösung.

a) Nach euklidischem Algorithmus:

$$\begin{aligned} 161 &= 7 \cdot 21 + 14 \\ 21 &= 1 \cdot 14 + 7 \\ 14 &= 2 \cdot 7 + 0 \end{aligned}$$

Also ist $\mathrm{ggT}(21, 161) = 7$.

b) Nun mit Rückwertseinsätzen:

$$\begin{aligned} 7 &= 21 - 14 \\ &= 21 - (161 - 7 \cdot 21) \\ &= 8 \cdot 21 - 161. \end{aligned}$$

Also ist $x = 8$ und $y = -1$ eine mögliche Lösung.

□

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.

Lösung. Wir bestimmen zuerst $[2]_5^{-1}$. Da $2 \cdot 3 = 6 \equiv 1 \mod 5$, ist $[2]_5^{-1} = [3]_5$. Durch multiplizieren der ersten Kongruenz mit 3 ergibt sich

$$2x \equiv 3 \mod 5 \qquad \longleftrightarrow \qquad x \equiv 9 \equiv 4 \mod 5.$$

Da $2 \cdot 4 = 8 \equiv 1 \mod 7$ ist durch multiplizieren mit 4

$$2x \equiv 5 \mod 7 \qquad \longleftrightarrow \qquad x \equiv 20 \equiv -1 \mod 7.$$

Da $3 \cdot (-4) = -12 \equiv 1 \mod 13$, ist durch multiplizieren mit -4

$$3x \equiv 2 \mod 13 \qquad \longleftrightarrow \qquad x \equiv -8 \equiv 5 \mod 13.$$

Äquivalent zur Aufgabenstellung ist also das System

$$x \equiv 4 \mod 5, \qquad x \equiv -1 \mod 7, \qquad x \equiv 5 \mod 13.$$

Nun benutzen wir die Lösungsformel:

$$\begin{aligned}
N &= 5 \cdot 7 \cdot 13 = 35 \cdot 13 = 350 + 105 = 455, \\
N_1 &= 7 \cdot 13 = 70 + 21 = 91, \\
N_2 &= 5 \cdot 13 = 65, \\
N_3 &= 5 \cdot 7 = 35, \\
M_1 &= [N_1]_{n_1}^{-1} = [91]_5^{-1} = [1]_5^{-1} = [1]_5 \\
M_2 &= [65]_7^{-1} = [2]_7^{-1} = [4]_7 \\
M_3 &= [35]_{13}^{-1} = [9]_{13}^{-1}
\end{aligned}$$

Um $M_3 = [9]_{13}^{-1}$ zu bestimmen, sehen wir, dass $3 \cdot 9 = 27 \equiv 1 \mod 13$, also ist $M_3 = [3]_{13}$. Also sind die Lösungen genau gegeben durch

$$\begin{aligned}
x &\equiv 4 \cdot 91 \cdot 1 + (-1) \cdot 65 \cdot 4 + 5 \cdot 35 \cdot 3 \mod 455 \\
&\equiv 364 - 260 + 175 \cdot 3 = 104 + 525 = 629 \equiv 629 - 455 = 174 \mod 455
\end{aligned}$$

sprich $x \equiv 174 \mod 455$. □

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.

Lösung.
Mit Polynomdivision modulo 5 ergibt sich

$$\begin{array}{rl}
([4]x^4 - [2]x^3 + [2]x^2 - [1]x + [1]) : ([2]x^2 + [3]) = [2]x^2 + \ldots \\
-([4]x^4 \qquad\quad + [1]x^2) \\
\hline
(-[2]x^3 + [1]x^2 - [1]x + [1]) : ([2]x^2 + [3]) = [-1]x + \ldots \\
-\quad (-[2]x^3 \qquad\quad - [3]x) \\
\hline
(\ [1]x^2 + [2]x + [1]) : ([2]x^2 + [3]) = [3] + \ldots \\
-\quad (\ [1]x^2 \qquad\quad + [4]) \\
\hline
\qquad\qquad [2]x - [3]
\end{array}$$

Also ist $q(x) = [2]x^2 + [4]x + [3]$ und $r(x) = [2]x + [2]$. □

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.

Lösung.

a) Zum Kodieren berechnen wir $2^{11} \mod 51$:

$$2^2 = 4, \qquad 2^4 = 4^2 = 16, \qquad 2^8 = 16^2 = 256 = 5 \cdot 51 + 1 \equiv 1 \mod 51$$

und daher

$$2^{11} = 2^8 \cdot 2^2 \cdot 2 \equiv 1 \cdot 4 \cdot 2 = 8 \mod 51.$$

Die kodierte Nachricht ist also 8.

b) Es ist $51 = 3 \cdot 17$. Daher ist $\varphi(51) = 2 \cdot 16 = 32$.
Da d das multiplikative Inverse zu e modulo 32 ist und $3 \cdot 11 = 33 \equiv 1 \mod 32$, ist $d = 3$.

c) Zum Dekodieren berechnen wir $4^d = 4^3 \mod 51$:

$$4^3 = 64 \equiv 13 \mod 51.$$

Die dekodierte Nachricht ist 13.

□

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.

Lösung. Wir stellen fest, dass der Induktionsschritt richtig scheint. Der Fehler sollte also irgendwo im Induktionsschritt stecken.
Gehen wir diesen langsam für $n = 1 \to n + 1 = 2$ durch, dann ist der vorletzte Schritt ein Problem. Hier teilen wir durch $n - 1 = 1 - 1 = 0$, was nicht erlaubt ist.
Daher ist der Induktionsschritt für $n = 1$ ungültig und die Induktion daher nicht vollständig. □