Diskrete Mathematik für Studierende der Informatik
WiSe 2023/2024
E. Viada
Probeklausur LOESUNGEN

Matrikel-Nr.	

- Die Bearbeitungszeit beträgt **90 Minuten**.
- 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	Σ
										/103

Name: _____

Note: _____

Aufgabe 1 (22 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 / falsch neben die Antwortmöglichkeiten.

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

- ○ $|A \cup B| = |A| + |B|$
- ○ $|A \cup B| > |A \cap B|$
- ⊗ $|A \cup B| + |A \cap B| = |A| + |B|$

b) (2P.) Sei $\mathbb{Z}$ die Menge der ganzen Zahlen, $\mathbb{N}$ die Menge der natürlichen Zahlen (mit 0) und B eine beliebige endliche Menge. Dann gilt:

- ○ $|\mathbb{Z} \cup B| > |\mathbb{Z}|$
- ⊗ $|\mathbb{Z} \cup B| = |\mathbb{Z}|$
- ⊗ $|\mathbb{N}| = |\mathbb{Z}|$

c) (2P.) Die folgenden Aussagen sind Tautologien (also immer wahr):

- ⊗ $A \vee B \quad \leftrightarrow \quad \neg(\neg A \wedge \neg B)$
- ○ $A \vee B \quad \leftrightarrow \quad \neg(\neg A \vee \neg B)$
- ⊗ $\neg(A \vee B) \quad \leftrightarrow \quad \neg A \wedge \neg B$

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

- ○ $\varphi(p) = p$
- ○ $7^{p-1} \equiv 1 \mod p$
- ⊗ $7^p \equiv 7 \mod p$

e) (2P.) Seien $N = p \cdot q$ und e die Kodierungsschlüssel und d der Dekodierungsschlüssel im RSA-Verfahren. Dann kann eine kodierte Nachricht mit folgender Kenntnis effizient entschlüsselt werden:

- ⊗ N, e und p
- ⊗ N, e und $\varphi(q)$
- ⊗ N, e und $\varphi(N)$

f) (2P.) Gegeben sei der logische Ausdruck $\forall x \in A \exists y \in B\colon |x - y| = 1$.
Welche Ausdrücke sind Negationen hiervon?

- ○ $\forall x \notin A \;\; \nexists y \in B\colon |x - y| \neq 1$
- ○ $\exists y \in B \; \forall x \in A\colon |x - y| \neq 1$
- ⊗ $\exists x \in A \; \forall y \in B\colon |x - y| \neq 1$

g) (4P.) Die Relation $R = \{(a, b) \in \mathbb{Z} \times \mathbb{Z} \mid |a - b| < 1\}$ ist:

- ⊗ reflexiv
- ⊗ symmetrisch
- ⊗ transitiv
- ⊗ eine Äquivalenzrelation

Aufgabe 2 (5+5 Punkte)**.**

a) Gegeben sei die Funktion $f\colon \mathbb{N} \to \mathbb{N}$ mit $f(n) = n^2$. Bestimmen Sie, ob f injektiv, surjektiv und/oder bijektiv ist. (Hierbei ist $0 \in \mathbb{N}$.) Begründen Sie Ihre Antwort kurz.

b) Gegeben sei die Funktion $f\colon \mathbb{R} \to \mathbb{R}_{\geq 0}$ mit $f(x) = x^2$. Bestimmen Sie, ob f injektiv, surjektiv und/oder bijektiv ist. Begründen Sie Ihre Antwort kurz.

Lösung.

a) Die Funktion f ist injektiv denn ist $f(n) = f(m)$, dann gilt

$$n^2 = f(n) = f(m) = m^2 \qquad \overset{\sqrt{\ }}{\Rightarrow} \qquad n = m,$$

da $n, m \in \mathbb{N}$ und damit $n, m \geq 0$ gilt.

Die Funktion ist nicht surjektiv, da zum Beispiel $2 \in \mathbb{N}$ nicht im Bild liegt, $f(n) = n^2 \neq 2$ für alle $n \in \mathbb{N}$.

Also ist die Funktion auch nicht bijektiv.

b) Als Funktion $\mathbb{R} \to \mathbb{R}_{\geq 0}$ ist f nicht injektiv, da $f(-1) = 1 = f(1)$.

Die Funktion ist surjektiv, da für jedes $r \in \mathbb{R}_{\geq 0}$ ist $\sqrt{r} \in \mathbb{R}_{\geq 0}$ und $f(\sqrt{r}) = r$.

Die Funktion ist demnach nicht bijektiv.

□

Aufgabe 3 (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) Wie viele Kombinationen aus 5 Karten gibt es, bei denen 3 Karten die Farbe Herz und 2 Karten die Farbe Kreuz haben: $\heartsuit, \heartsuit, \heartsuit, \clubsuit, \clubsuit$?

b) Wie viele Möglichkeiten gibt es, die 4 Asse (A) und 4 Könige (K) anzuordnen, wenn es nur auf die Zahl und nicht auf die Farbe ankommt?
(Eine Möglichkeit wäre also z.B. AKKAAKKA.)

Lösung.

a) Es gibt $\binom{13}{3}$ Möglichkeiten drei von den 13 Herz-Karten zu wählen, und $\binom{13}{2}$ Möglichkeiten die Kreuz-Karten zu wählen. Damit ergeben sich insgesamt $\binom{13}{3}\binom{13}{2}$ Möglichkeiten.

b) Mann hat verschieden Wege es zu lösen. Einer Seite diese sind die Anagramme von AKKAAKKA und somit $\frac{8!}{4!4!}$ Andereseite, wir müssen die 8 Karten auf 8 Plätze aufteilen. Wir wählen 4 der 8 Plätze aus, um dort Asse hinzulegen. Hierfür gibt es $\binom{8}{4}$ Möglichkeiten. Da es uns nicht auf die Farbe ankommt, gibt es nun genau eine Möglichkeit die vier Asse auf diese Plätze zu legen und die Könige auf die verbleibenden Plätze. Damit ergeben sich insgesamt $\binom{8}{4}$ Möglichkeiten.

   Klar die zwei Lösungen ergeben das selbe resultat

□

Aufgabe 4 (5 Punkte)**.**

a) Berechnen Sie $\mathrm{ggT}(28, 92)$ mithilfe des euklidischen Algorithmus.

b) Bestimmen Sie $x, y \in \mathbb{Z}$, sodass $28x + 92y = \mathrm{ggT}(28, 92)$.

Lösung. a)

$$\begin{aligned} 92 &= 3 \cdot 28 + 8 \\ 28 &= 3 \cdot 8 + 4 \\ 8 &= 2 \cdot 4 + 0 \end{aligned}$$

Also ist $\mathrm{ggT}(28, 92) = 4$.

b) Durch Rückeinsetzen:

$$\begin{aligned} 4 &= 28 - 3 \cdot 8 \\ &= 28 - 3 \cdot (92 - 3 \cdot 28) \\ &= 10 \cdot 28 - 3 \cdot 92 \end{aligned}$$

also ist $x = 10$ und $y = -3$ eine Lösung.

□

Aufgabe 5 (5 Punkte)**.** Berechnen Sie $\varphi(84)$, $\varphi(7^2)$ und $\varphi(7^2 \cdot 84)$.
Geben Sie die Antworten in der Primfaktorzerlegung an.

Lösung.
In Primfaktoren zerlegt ist

$$84 = 2 \cdot 42 = 2^2 \cdot 21 = 2^2 \cdot 3 \cdot 7.$$

Damit ist nach der Formel für φ:

$$\begin{aligned}
\varphi(84) &= \varphi(2^2 \cdot 3 \cdot 7) = 2 \cdot 2 \cdot 6 = 2^3 \cdot 3, \\
\varphi(7^2) &= 7 \cdot 6 = 2 \cdot 3 \cdot 7, \\
\varphi(7^2 \cdot 84) &= \varphi(2^2 \cdot 3 \cdot 7^3) = 2 \cdot 2 \cdot 7^2 \cdot 6 = 2^3 \cdot 3 \cdot 7^2.
\end{aligned}$$

□

Aufgabe 6 (5 Punkte)**.** Bestimmen Sie $81^{76} \mod 7$.

Lösung. Es ist $\varphi(7) = 6$ und daher

$$\begin{aligned}
81^{76} &= (77 + 4)^{76} \equiv 4^{76} \\
&= 4^{72+4} = 4^{6 \cdot 12} \cdot 4^4 \equiv 1 \cdot 4^4 \\
&= 16^2 \equiv 2^2 = 4 \mod 7.
\end{aligned}$$

□

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

a) Begründen Sie, warum die Kongruenz $11x \equiv 22 \mod 33$ die selben Lösungen hat, wie die Kongruenz $x \equiv 2 \mod 3$.

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

$$11x \equiv 22 \mod 33, \qquad x \equiv 3 \mod 5 \qquad \text{und} \qquad 4x \equiv 3 \mod 7$$

Lösung.

a) Die Kongruenz $11x \equiv 22 \mod 33$ ist erfüllt genau dann, wenn es ein $y \in \mathbb{Z}$ gibt, sodass

$$11x + 33y = 22.$$

Mit Teilen durch 11 ist dies äquivalent dazu, dass es ein $y \in \mathbb{Z}$ gibt, sodass

$$x + 3y = 2,$$

also $x \equiv 2 \mod 3$.

b) Zunächst ersetzen wir die erste Kongruenz durch $x \equiv 2 \mod 3$, siehe a).

Für die dritte Kongruenz berechnent wir $[4]_7^{-1}$, dies ist gegeben durch $[2]_7$, da $2 \cdot 4 = 8 \equiv 1 \mod 7$. Multiplizieren mit 2 in der dritten Kongruenz gibt also

$$4x \equiv 3 \mod 5 \qquad \Leftrightarrow \qquad x \equiv 6 \mod 7.$$

$3, 5, 7$ sind paarweise Coprim. Damit erhalten wir die Kongruenzen

$$x \equiv 2 \mod 3, \qquad x \equiv 3 \mod 5, \qquad x \equiv 6 \mod 7.$$

Wir wenden nun die Lösungsformel an:

$$\begin{aligned}
N &= 3 \cdot 5 \cdot 7 = 105, \\
N_1 &= 5 \cdot 7 = 35, \quad N_2 = 3 \cdot 7 = 21, \quad N_3 = 3 \cdot 5 = 15, \\
M_1 &= [N_1]_{n_1}^{-1} = [35]_3^{-1} = [2]_3^{-1} = [2]_3, \\
M_2 &= [N_2]_{n_2}^{-1} = [21]_5^{-1} = [1]_5^{-1} = [1]_5, \\
M_3 &= [N_3]_{n_3}^{-1} = [15]_7^{-1} = [1]_7^{-1} = [1]_7.
\end{aligned}$$

Also

$$2 \cdot 35 \cdot 2 + 3 \cdot 21 \cdot 1 + 6 \cdot 15 \cdot 1 \equiv 140 + 63 + 90 \equiv 293 \equiv 83 \mod 105$$

und die Lösungen sind gegeben durch $x \equiv 83 \mod 105$.

□

Aufgabe 8 (3+3+4 Punkte)**.** Gegeben sind die öffentlichen Schlüssel $N = 22$ und $e = 7$ für eine RSA-Kodierung.

a) Kodieren Sie die Nachricht 3.

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

c) Dekodieren Sie die Nachricht 4.

Lösung.

a) Zum Kodieren berechnen wir $3^e \mod 22$:

$$3^7 = 3^4 \cdot 3^2 \cdot 3,$$

wobei $3^2 = 9$, $3^4 = 9^2 = 81 \equiv -7 \mod 22$, also

$$3^7 \equiv (-7) \cdot 9 \cdot 3 = -63 \cdot 3 \equiv 3 \cdot 3 = 9 \mod 11.$$

Die kodierte Nachricht ist also 9.

b) Es ist $22 = 2 \cdot 11$, also $\varphi(22) = 1 \cdot 10 = 10$.
Damit ist $d = [e]_{10}^{-1} = [7]_{10}^{-1}$. Da $3 \cdot 7 = 21 \equiv 1 \mod 10$, ist also $d = 3$.

c) Zum Dekodieren ist $4^d = 4^3 = 64 \equiv 20 \mod 22$ zu bestimmen.
Die dekodierte Nachricht ist also 20.

□

Aufgabe 9 (10 Punkte)**.** Zeigen Sie für alle $n \in \mathbb{N}_+$, dass

$$\sum_{k=1}^{n} \frac{1}{4k^2-1} = \frac{n}{2n+1}.$$

Hinweis: Formulieren Sie die Induktionsvorrausetzung für $n-1$ und führen Sie den Induktionsschritt für n.

Lösung.
Induktionsanfang: Für $n = 1$ ist

$$\frac{1}{4 \cdot 1^2 - 1} = \frac{1}{3} \quad \stackrel{!}{=} \quad \frac{1}{3} = \frac{1}{2 \cdot 1 + 1}.$$

Induktionsvorrausetzung: Wir nehmen an, für ein $\mathbb{N} \ni n > 2$ gilt

$$\sum_{k=1}^{n-1} \frac{1}{4k^2-1} = \frac{n-1}{2(n-1)+1} = \frac{n-1}{2n-1}.$$

Induktionsschritt: Dann folgt für n:

$$\begin{aligned}
\sum_{k=1}^{n} \frac{1}{4k^2-1} &= \sum_{k=1}^{n} \frac{1}{4k^2-1} + \frac{1}{4n^2-1} \stackrel{\text{IB}}{=} \frac{n-1}{2n-1} + \frac{1}{4n^2-1} \\
&= \frac{n-1}{2n-1} + \frac{1}{(2n+1)(2n-1)} = \frac{(n-1)(2n+1)+1}{(2n+1)(2n-1)} \\
&= \frac{2n^2-n}{(2n+1)(2n-1)} = \frac{(2n-1)n}{(2n+1)(2n-1)} = \frac{n}{2n+1},
\end{aligned}$$

was gerade zu zeigen war.
Damit ist die Induktion vollständig. □