

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

Matrikel-Nr.	
--------------	--

- Die Bearbeitungszeit beträgt **70 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		Σ

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. 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):

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

☐ $A \vee B \leftrightarrow \neg(\neg A \vee \neg B)$

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

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

☐ $\varphi(p) = p$

☐ $7^{p-1} \equiv 1 \pmod{p}$

☐ $7^p \equiv 7 \pmod{p}$

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 $\forall x \in A \exists y \in B: |x - y| = 1$. Welche Ausdrücke sind Negationen hiervon?

- ☐ $\forall x \notin A \nexists y \in B: |x - y| \neq 1$
- ☐ $\exists y \in B \forall x \in A: |x - y| \neq 1$
- ☐ $\exists x \in A \forall y \in B: |x - y| \neq 1$

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 $f: \mathbb{N} \rightarrow \mathbb{N}$ 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 $f: \mathbb{R} \rightarrow \mathbb{R}_{\geq 0}$ mit $f(x) = x^2$. Bestimmen Sie, ob f injektiv, surjektiv und/oder bijektiv ist. Begründen Sie Ihre Antwort kurz.

Aufgabe 3 (5+5 Punkte). Gegeben sei ein Kartenspiel mit 52 Karten.

Jede Karte trägt eine der 13 Zahlen $\{2, 3, 4, 5, 6, 7, 8, 9, 10, J, D, K, A\}$ und eine der 4 Farben $\{\clubsuit, \diamondsuit, \spadesuit, \heartsuit\}$, 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 (\heartsuit) und 2 Karten die Farbe Kreuz (\clubsuit) haben: $\heartsuit, \heartsuit, \heartsuit, \clubsuit, \clubsuit$? Begründen Sie Ihre Antwort.
- 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? Begründen Sie Ihre Antwort.
(Eine Möglichkeit wäre also z.B. AKKAAKKA.)

Binomialkoeffizienten, Fakultäten und Ähnliches können Sie unausgerechnet stehen lassen.

Aufgabe 4 (5Punkte).

- a) Berechnen Sie $\text{ggT}(28, 92)$ mithilfe des euklidischen Algorithmus.
- b) Bestimmen Sie $x, y \in \mathbb{Z}$, sodass $28x + 92y = \text{ggT}(28, 92)$.

Aufgabe 5 (6 Punkte). Berechnen Sie $\varphi(84)$, $\varphi(7^2)$ und $\varphi(7^2 \cdot 84)$.
Geben Sie die Antworten in der Primfaktorzerlegung an.

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

Aufgabe 7 (3+7 Punkte).

- a) Begründen Sie, warum die Kongruenz $11x \equiv 22 \pmod{33}$ die selben Lösungen hat, wie die Kongruenz $x \equiv 2 \pmod{3}$.
- b) Bestimmen Sie alle Lösungen für das folgende System von Kongruenzen:

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

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.

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 Induktionsvoraussetzung für $n - 1$ und führen Sie den Induktionsschritt für n .

