TECHNISCHE UNIVERSITÄT BERLIN
Fakultät II – Institut für Mathematik
Ekkehard Köhler

Prüfungsklausur „Diskrete und strukturelle Mathematik für Informatiker"

Name: ....

Vorname: ....

Matr.-Nr.: ....

☐ Informatik ☐ Sonstige: ....

*Mit dem Aushang des Klausurergebnisses nur mit der Matrikelnummer am Anschlagbrett im Flur **MA 6-1** bin ich einverstanden.*

Alle Antworten, mit Ausnahme der *multiple-choice*-Aufgaben, müssen genau begründet werden. Dabei dürfen Ergebnisse aus dem Skript und von den Übungsblättern (mit genauer Quellenangabe) benutzt werden.
Alle Blätter sind mit *Namen und Matrikelnummer* zu versehen. Abzugeben sind die Lösungen in *Reinschrift* mit allen *Nebenrechnungen* auf DIN A4-Blättern, sowie diesen Aufgabenblättern als Deckblättern. Bitte jeweils ein neues Blatt für eine neue Aufgabe.
Mit *Bleistift* oder *in rot* geschriebene Klausurteile können nicht gewertet werden.
Die Bearbeitungszeit für die Klausur beträgt 90 Minuten.
Einzige erlaubte Hilfsmittel sind das Vorlesungsskript und die Übungsblätter. Nicht erlaubt sind insbesondere elektronische Rechenhilfen aller Art.

Aufgabe	Punkte	von
1		5
2		5
3		4
4		5
5		4
Summe		23

Note: ....

....
(Unterschrift des Korrektors)

Aufgabe 1: **2+3 Punkte**

a) Welche der folgenden Aussagen ist wahr, welche falsch? Kreuzen Sie die entsprechenden Kästchen deutlich an, wie es bei der ersten, offensichtlich falschen Aussage vorgeführt ist. Beachten Sie, daß fehlerhaftes Ankreuzen zu Punktabzug führt, Sie jedoch keinesfalls weniger als 0 Punkte auf den *multiple-choice*-Teil erhalten.

W	F
	X

Jeder Graph ist zusammenhängend.

W	F

Jeder Graph mit geradem Knotengrad an jedem Knoten besitzt eine geschlossene Eulerkantenfolge.

W	F

Sei $G = \{V, E\}$ ein Graph mit 7 Knoten $V = \{v_i | 1 \leq i \leq 7\}$ mit den folgenden Knotengraden: $d(v_1) = d(v_2) = 2, d(v_3) = 3, d(v_4) = d(v_5) = d(v_6) = 4$ und $d(v_7) = 5$. Daraus folgt: G ist kein Baum.

b) Sei $G = (V, E)$ ein ebener und zusammenhängender Graph. Zeigen Sie, daß G keine drei spannenden Bäume mit paarweise disjunkten Kantenmengen enthält.

Aufgabe 2: **5 Punkte**

Das Programm $China^{rs}$ besitzt drei Prozesse, die nach Laufzeiten von 7, 10 bzw. 5 Zeiteinheiten auf eine gemeinsame Datenressource zugreifen.

a) Können Sie durch geschickte Wahl ganzzahliger Startzeiten erreichen, daß niemals alle drei gleichzeitig zugreifen? (Wenn ja, wie, wenn nein, weshalb nicht!)

b) Angenommen, Sie haben keinen Einfluß auf die Startzeiten. Stattdessen können Sie jedem Prozess eine feste, ganzzahlige, nicht negative Wartezeit zuweisen, die seine Laufzeit verlängert. Machen Sie einen begründeten Vorschlag für die Wahl der Wartezeiten, um zu garantieren, daß gemeinsame Zugriffe aller drei Prozesse mindestens 380 Zeiteinheiten auseinanderliegen. Dabei soll die Summe der Wartezeiten der drei Prozesse möglichst klein sein.

c) Rechnen Sie nun mit den von Ihnen in b) gewählten Zeiten (ansonsten nehmen Sie 9, 5 und 13 als Laufzeiten). Die beiden kürzesten Prozesse greifen gerade gemeinsam zu. Der dritte Prozess hat 3 Zeiteinheiten früher zugegriffen. Wann werden das nächste Mal alle drei zugreifen?

Aufgabe 3: **4 Punkte**

Gegeben sei der RSA-Code mit öffentlicher Zahl $m = 185$ und öffentlichem Schlüssel $e = 149$.

a) Bestimmen Sie, $\varphi(m)$, den Wert der Eulerschen Funktion bei m.

b) Verschlüsseln Sie $x = 14$.

Aufgabe 4: **2+3 Punkte**

a) Welche der folgenden Aussagen ist wahr, welche falsch? Kreuzen Sie die entsprechenden Kästchen deutlich an.
Beachten Sie, daß fehlerhaftes Ankreuzen zu Punktabzug führt, Sie jedoch keinesfalls weniger als 0 Punkte auf den *multiple-choice*-Teil erhalten.

W	F

Jeder Körper ist ein Ring mit 1.

W	F

In jedem kommutativen Ring R mit 1 gilt: $\forall k, l \in R \setminus \{0\} : k \cdot l \in R \setminus \{0\}$.

b) Sei R ein Ring, U und V Unterringe von R. Zeigen Sie daß $U \cap V \neq \emptyset$, und $U \cap V$ ebenfalls ein Unterring von R ist.

Aufgabe 5: **4 Punkte**

Es sei $f \in \mathbb{Z}_3[x]$ mit $f(x) = x^3 + 2x^2 + 1$.

a) $\mathbb{Z}_3(f)$ ist ein Körper. Beweisen Sie dies.

b) Wieviele Elemente hat $\mathbb{Z}_3(f)$?

c) Bestimmen Sie ein $g \in \mathbb{Z}_3(f)$, so daß für das entsprechende Element in $\mathbb{Z}_3[x]$ gilt:

$$x^3 + 1 \equiv g \mod f.$$
