

Prüfungsklausur zur Vorlesung Diskrete und strukturelle Mathematik für Informatiker

19. Juli 2006

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 zu den *multiple-choice*-Aufgaben, **müssen begründet werden**. Sätze und Ergebnisse aus Vorlesung und Übungszetteln dürfen Sie selbstverständlich benutzen, sollten Sie aber entsprechend benennen.

Alle Blätter sind mit *Namen und Matrikelnummer* zu versehen. Abzugeben sind die Lösungen in *Reinschrift* mit allen *Nebenrechnungen* auf DIN A4-Blättern, sowie Aufgabenblatt und Deckblatt. Fangen Sie für jede Aufgabe bitte ein neues Blatt an.

Mit *Bleistift* oder *in rot* geschriebene Klausurteile können nicht gewertet werden.

Die Bearbeitungszeit für die Klausur beträgt 90 Minuten; die Klausur zählt als bestanden, wenn mindestens 15 Punkte erreicht wurden.

Es sind keinerlei Hilfsmittel erlaubt, insbesondere keine elektronischen Geräte und keine Aufzeichnungen aus Vorlesungen und Tutorien.

Viel Erfolg!

Aufgabe	Punkte	von	Korr.
1		12	
2		6	
3		6	
4		6	
Summe		30	

Note:

Aufgabe 1:**12 Punkte**

Auf jede richtig angekreuzte Frage gibt es in dieser Aufgabe 1 Punkt, für jede falsch angekreuzte Frage -1 Punkt. Ist die Summe der Punktzahlen dieser Aufgabe negativ, wird sie mit 0 Punkten bewertet.

Jeder Baum hat mehr Knoten als Kanten.	<input type="checkbox"/>	<input type="checkbox"/>
Ist ein Polynom über \mathbb{Q} reduzibel, dann auch über \mathbb{Z} .	<input type="checkbox"/>	<input type="checkbox"/>
Die chromatische Zahl eines Graphen ist höchstens so groß wie seine Kantenzahl.	<input type="checkbox"/>	<input type="checkbox"/>
Bezeichne φ die Eulersche φ -Funktion. Für $m < n$ gilt $\varphi(m) < \varphi(n)$.	<input type="checkbox"/>	<input type="checkbox"/>
Jeder Graph mit 100 Knoten und 294 Kanten ist planar.	<input type="checkbox"/>	<input type="checkbox"/>
Bei der RSA-Codierung muss der Sender einer Nachricht nicht wissen, wie seine Nachricht entschlüsselt wird.	<input type="checkbox"/>	<input type="checkbox"/>
Der geheime Schlüssel im RSA-Algorithmus muss eine Primzahlpotenz sein.	<input type="checkbox"/>	<input type="checkbox"/>
Für 2 verschiedene Primzahlen $p_1, p_2 \geq 100$ existiert eine Zahl $x < p_1 p_2$ mit $x \equiv 83 \pmod{p_1}$ und $x \equiv 27 \pmod{p_2}$.	<input type="checkbox"/>	<input type="checkbox"/>
$c = (010101)$ und $c' = (101010)$ sind Codeworte in einem Code, der 3 Fehler korrigiert.	<input type="checkbox"/>	<input type="checkbox"/>
Ein Code, bei dem in jedem Codewort die Anzahl der Einsen durch 3 teilbar ist, ist linear.	<input type="checkbox"/>	<input type="checkbox"/>
$\mathbb{Z}_9[x]/(x^8 - 8x^6 - x^5 + x^4 + 3x^3)$ ist ein Körper.	<input type="checkbox"/>	<input type="checkbox"/>
In jedem Baum ist nm ungerade (n : Knotenzahl, m : Kantenzahl).	<input type="checkbox"/>	<input type="checkbox"/>

Aufgabe 2:**6 Punkte**

- (a) Zeige, dass $K = \{x + y\sqrt{-3} \mid x, y \in \mathbb{Q}\}$ mit der induzierten Addition und Multiplikation von \mathbb{C} ein Unterkörper von \mathbb{C} ist.
- (b) Zerlege das Polynom $x^4 - 2x^2 - 15$ in irreduzible Teiler über \mathbb{Q} , \mathbb{R} , \mathbb{C} und dem Körper K aus Teil (a).
- (c) Finde die Inversen von x und $2x + 1$ bezüglich der Multiplikation in $\mathbb{Z}_3[x]/(x^2 + 1)$.
-

Aufgabe 3:**6 Punkte**

- (a) Sei $G = (V, E)$ ein zusammenhängender Graph und $e \in E$ eine Kante. Zeige: Der Teilgraph $G' = (V, E \setminus \{e\})$ ist genau dann zusammenhängend, wenn es einen Kreis in G gibt, der die Kante e enthält.

- (b) Zeige, dass ein zusammenhängender planarer Graph mit 50 Knoten, in dem jeder Kreis mindestens Länge 5 hat, höchstens 80 Kanten hat.
-

Aufgabe 4:**6 Punkte**

- (a) Zeige, dass folgendes System von Äquivalenzen eine Lösung hat oder beweise das Gegenteil:

$$\begin{aligned}x &\equiv 1 \pmod{3} \\x &\equiv 0 \pmod{7} \\x &\equiv 3 \pmod{11}\end{aligned}$$

- (b) Gib eine Lösung des Systems

$$\begin{aligned}x &\equiv 2 \pmod{6} \\x &\equiv 0 \pmod{14} \\x &\equiv 6 \pmod{22}\end{aligned}$$

- an. (Hinweis: vergleiche das System mit dem aus Teil a).

- (c) Die zweite Zeile des Systems aus Teil (b) soll durch eine Äquivalenz der Form

$$x \equiv y \pmod{14}$$

ersetzt werden. Für welche $y < 14$ hat das System dann eine Lösung, für welche nicht?