Universität Kassel
Fachbereich 10/16
Dr. Sebastian Petersen 08.03.2012

Klausur: Diskrete Strukturen II

Name:	Vorname:	Matrikelnummer:	Versuch:

Unterschrift:

Bitte fangen Sie für jede Aufgabe ein neues Blatt an. Beschreiben Sie nur die Vorderseite der Blätter.

Es können maximal 37 Punkte erreicht werden.

Aufgabe 1	Aufgabe 2	Aufgabe 3	Aufgabe 4	Aufgabe 5	Aufgabe 6

Punkte:	**Note:**

Aufgabe 1. (8 Punkte)

a) Ergänzen Sie die folgende Definition: "Eine Relation R auf einer Menge X heißt *partielle Ordnung*, wenn ..."

b) Wann wird eine Relation R auf einer Menge X *transitiv* genannt?

c) Wir betrachten die durch

$$xSy :\Longleftrightarrow\ |x| = |y+1|$$

gegebene Relation S auf $\mathbb{R}$. Entscheiden Sie (mit stichhaltiger Begründung), ob S reflexiv ist und ob S symmetrisch ist. Ist S eine Äquivalenzrelation?

d) Sei $X = \{0, 1\}$. Geben Sie Verknüpfungen $\bullet : X \times X \to X$ und $\cap : X \times X \to X$ derart an, daß $\bullet$ assoziativ und $\cap$ *nicht* assoziativ ist, indem Sie die folgenden Verknüpfungstafeln entsprechend ausfüllen:

$\bullet$	0	1
0		
1		

$\cap$	0	1
0		
1		

Bei dieser Aufgabe 1d) brauchen Sie keine Begründung geben.

Aufgabe 2. (8 Punkte)

a) Für die folgenden Elemente von $\mathbb{Z}/550$ entscheide man jeweils, ob eine Einheit in $\mathbb{Z}/550$ vorliegt: $[3]_{550}$, $[5]_{550}$, $[7]_{550}$ und $[11]_{550}$. Begründen Sie Ihre Antwort!

b) Wie viele Elemente enthält die Einheitengruppe $((\mathbb{Z}/550\mathbb{Z})^\times, \cdot\,)$ insgesamt? Begründen Sie Ihre Antwort, z.B. indem Sie die Rechnung in nachvollziehbarer Weise einschließlich aller Rechenschritte angeben. (Hinweis: Denken Sie an die Sätze zur Eulerschen φ-Funktion.)

c) Berechnen Sie das (multiplikative) Inverse zu $[3]_{13}$ in $\mathbb{F}_{13} = \mathbb{Z}/13$, falls es existiert. Begründen Sie Ihre Antwort.

d) Was besagt der kleine Satz von Fermat?

Aufgabe 3. (4 Punkte)

a) Berechnen Sie ein $x \in \mathbb{Z}$, das

$$x \equiv 5 \bmod 8 \text{ und } x \equiv 7 \bmod 9$$

erfüllt.

b) Entscheiden Sie, ob es ein $x \in \mathbb{Z}$ mit

$$x \equiv 5 \bmod 6 \text{ und } x \equiv 4 \bmod 10$$

gibt und geben Sie einen stichhaltigen Beweis für die Aussage, die Sie treffen.

Aufgabe 4. (2 Punkte) Wir betrachten die folgende Mini-Version von RSA: Alice hat zwei Primzahlen $p \neq q$ gewählt, $N = pq$ berechnet und $N = 77$ öffentlich gemacht. Der öffentliche Verschlüsselungsexponent von Alice ist $e = 7$. Was ist die RSA-Verschlüsselung der Nachricht $m = [2]_{77} \in \mathbb{Z}/77$ an Alice?

Aufgabe 5. (7 Punkte) Sei $\Gamma := (V, E)$ ein einfacher endlicher zusammenhängender Graph und $W := (v_0, \cdots, v_\ell)$ eine endliche Folge in der Knotenmenge V.

a) Wann wird W ein *Hamilton-Kreis* in Γ genannt?

b) Geben Sie eine notwendige und hinreichende Bedingung an die Knotengrade $\deg(v)$ ($v \in V$) an, unter der Γ eulersch ist.

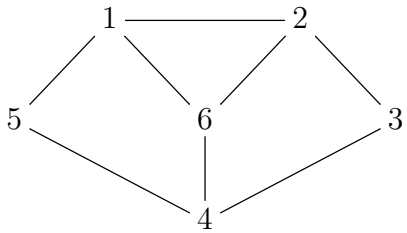
c) In dem vollständigen Graphen $K_5 = (V_5, E_5)$ gebe man einen Hamilton-Kreis $H = (u_0, \cdots, u_5)$ und eine Euler-Tour $T = (t_0, \cdots, t_{10})$ explizit an. (Zur Erinnerung: $V_5 = \{1, 2, 3, 4, 5\}$ und $E_5 = \{\{u, v\} : u, v \in V_5 \text{ und } u \neq v\}$.)

Aufgabe 6. (8 Punkte) Sei $\Gamma = (V, E)$ ein einfacher, *plättbarer*, zusammenhängender, endlicher Graph.

a) Sei $v(\Gamma) = |V|$, $e(\Gamma) = |E|$ und $g(\Gamma)$ die Anzahl der Gebiete, in die der geplättet gezeichnete Graph Γ die Ebene zerlegt. Welchen Wert hat dann die Größe $c(\Gamma) := v(\Gamma) - e(\Gamma) + g(\Gamma)$?

b) Geben Sie eine möglichst kleine obere Schranke an die chromatische Zahl $\chi(\Gamma)$ an.

c) Wir betrachten nun den in der Skizze dargestellten Graphen G:



Geben Sie eine Knotenfärbung mit möglichst wenig Farben explizit an.

d) Wir betrachten den vollständigen Graphen $K_6 = (V_6, E_6)$ mit Knotenmenge $V_6 = \{1, 2, \cdots, 6\}$. Sei $H := (V_6, E_6 \setminus \{\{1, 2\}, \{2, 3\}\})$ der Graph, der aus K_6 durch das Entfernen der beiden Kanten $\{1, 2\}$ und $\{2, 3\}$ entsteht. Entscheiden Sie, ob H plättbar ist, und beweisen Sie die Aussage, die Sie treffen.

Diskrete Mathematik II
Lösungsskizze zu der Klausur von 08.03.2012

Aufgabe 1.

a) Siehe Skript.

b) Siehe Skript

c) Wir betrachten die durch

$$xSy :\Longleftrightarrow\ |x| = |y+1|$$

gegebene Relation S auf $\mathbb{R}$.

Behauptung. S ist nicht reflexiv. *Beweis.* Z.B. gilt nicht $0S0$, da $|0| \neq |0+1|$.

Behauptung. S ist nicht symmetrisch. *Beweis.* Es gilt $1S0$, weil $|1| = |0+1|$. Die Aussage $0S1$ ist aber falsch, weil $|0| \neq |1+1|$.

S ist keine Äquivalenzrelation, sonst müßte S reflexiv (und symmetrisch) sein.

d) Sei $X = \{0,1\}$. Definiere Verknüpfungen $\bullet : X \times X \to X$ und $\cap : X \times X \to X$ folgendermaßen.

$\bullet$	0	1
0	0	0
1	0	1

$\cap$	0	1
0	1	1
1	0	0

Dann ist $\bullet$ assoziativ (da es i.w. die Multiplikation des Körpers $\mathbb{F}_2$ ist). Ferner ist $\cap$ nicht assoziativ. (Begründung: $0 \cap (0 \cap 0) = 0 \cap 1 = 1$ aber $(0 \cap 0) \cap 0 = 1 \cap 0 = 0$).
(Nach den Begründungen war hier nicht gefragt - ich gebe sie nur der Vollständigkeit halber an.)

Aufgabe 2.

a) Allgemein gilt für $N \geq 2$ und $x \in \mathbb{Z}$: Genau dann ist $[x]_N$ eine Einheit in $\mathbb{Z}/N$, wenn x zu N teilerfremd ist. Man hat die PFZ $550 = 2 \cdot 5^2 \cdot 11$.

Daher gilt: $[3]_{550}$ und $[7]_{550}$ sind Einheit in $\mathbb{Z}/550$. Ferner gilt: $[5]_{550}$ und $[11]_{550}$ sind Nicht-Einheiten in $\mathbb{Z}/550$.

b) Wie viele Elemente enthält die Einheitengruppe $((\mathbb{Z}/550\mathbb{Z})^\times, \cdot)$ insgesamt? Es gilt nach Definition der φ-Funktion und einem Satz der Vorlesung:

$$|(\mathbb{Z}/550\mathbb{Z})^\times| = \varphi(550) = \varphi(2 \cdot 5^2 \cdot 11) = (2-1) \cdot 5(5-1) \cdot (11-1) = 200.$$

c) Das (multiplikative) Inverse zu $[3]_{13}$ in $\mathbb{F}_{13} = \mathbb{Z}/13$ ist $[3]^{-1} = [9]$. Begründung: $3 \cdot 9 = 27 = 1(13)$.

d) Der kleine Satz von Fermat besagt: Sei $N \geq 2$ eine natürliche Zahl und $x \in \mathbb{Z}$. Wenn x zu N teilerfremd ist, dann gilt $x^{\varphi(N)} = 1 \bmod N$.

Aufgabe 3.

a) Betrachte das System

$$X \equiv 5 \bmod 8\ (K1) \text{ und } X \equiv 7 \bmod 9\ (K2)$$

von Kongruenzen. Die ersten positiven Lösungen von $(K1)$ sind:

$$5, 13, 21, 29, 37, 45, 53, 61, \cdots.$$

Man sieht, daß $x = 61$ auch die Kongruenz $(K2)$ erfüllt.

b) *Behauptung:* Es gibt kein $x \in \mathbb{Z}$ mit

$$x \equiv 5 \bmod 6 \text{ und } x \equiv 4 \bmod 10.$$

Beweis. Nimm an, es gäbe doch ein solches x. Dann würde wegen der ersten Kongruenz x ungerade sein. Die zweite Kongruenz würde aber erzwingen, daß x gerade ist. Widerspruch.

Aufgabe 4. Die Verschlüsselung ist

$$c := m^e = [2^7]_{77} = [128]_{77} = [51]_{77}.$$

Aufgabe 5. Sei $\Gamma := (V, E)$ ein einfacher endlicher zusammenhängender Graph und $W := (v_0, \cdots, v_\ell)$ eine endliche Folge in der Knotenmenge V.

a) Siehe Skriptum.

b) Nach einem zentralen Satz aus Kapitel VIII. der Vorlesung gilt: Genau dann ist Γ eulersch, wenn $\deg(v)$ gerade ist für jeden Knoten $v \in V$.

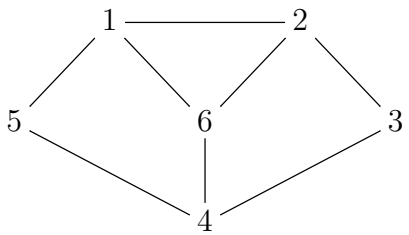
c) $(1, 2, 3, 4, 5, 1)$ ist ein Hamilton-Kreis in K_5. Ferner ist $(1, 2, 3, 4, 5, 3, 1, 4, 2, 5, 1)$ eine Euler-Tour in K_5. (Zur Erinnerung: $V_5 = \{1, 2, 3, 4, 5\}$ und $E_5 = \{\{u, v\} : u, v \in V_5 \text{ und } u \neq v\}$.)

Aufgabe 6. Sei $\Gamma = (V, E)$ ein einfacher, *plättbarer*, zusammenhängender, endlicher Graph.

a) Sei $v(\Gamma) = |V|$, $e(\Gamma) = |E|$ und $g(\Gamma)$ die Anzahl der Gebiete, in die der geplättet gezeichnete Graph Γ die Ebene zerlegt. Nach der eulerschen Polyederformel gilt dann $v(\Gamma) - e(\Gamma) + g(\Gamma) = 2$.

b) Nach dem Vierfarben-Satz von Appel und Haken gilt $\chi(\Gamma) \leq 4$. (Eine kleinere Schranke, die für alle denkbaren Γ funktioniert, gibt es nicht.)

c) Wir betrachten nun den in der Skizze dargestellten Graphen G:



Die Funktion $f : V \to \{rot, blau, gelb\}$, die durch

x	1	2	3	4	5	6
$f(x)$	*blau*	*gelb*	*rot*	*gelb*	*rot*	*rot*

definiert wird, ist eine Kantenfärbung mit 3 Farben. (Mit weniger Farben kommt man nicht aus, da man nach Vorlesung schon für einen Kreis ungerader Länge 3 Farben braucht.)

d) Wir betrachten den vollständigen Graphen $K_6 = (V_6, E_6)$ mit Knotenmenge $V_6 = \{1, 2, \cdots, 6\}$. Sei $H := (V_6, E_6 \setminus \{\{1, 2\}, \{2, 3\}\})$ der Graph, der aus K_6 durch das Entfernen der beiden Kanten $\{1, 2\}$ und $\{2, 3\}$ entsteht.

Behauptung. H ist nicht plättbar. *Beweis.* $v(H) = 6$ und $e(H) = \begin{pmatrix} 6 \\ 2 \end{pmatrix} - 2 = 13$. Wäre H plättbar, so müßte nach einer Folgerung zu der eulerschen Polyederformel (siehe Skript) schon $e(H) \leq 3v(H) - 6$ gelten, was nicht der Fall ist. $\square$