Universität Kassel
Fachbereich 10/16

06.03.2013

# 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 **30** Punkte erreicht werden.

| Aufgabe 1 | Aufgabe 2 | Aufgabe 3 | Aufgabe 4 | Aufgabe 5 |
|---|---|---|---|---|
| | | | | |

| Punkte: | **Note:** |
|---|---|
| | |

**Aufgabe 1. (6 Punkte)**

a) Wir betrachten auf $\mathbb{R}$ die durch

$$xSy :\Longleftrightarrow |x-y| \leq 2$$

gegebene Relation $S \subset \mathbb{R} \times \mathbb{R}$. Entscheiden Sie, ob $S$ reflexiv ist, ob $S$ transitiv ist und ob $S$ symmetrisch ist. Begründen Sie in den drei Fällen Ihre Entscheidung stichhaltig!

b) Auf der Menge $M := \{1, 2, 3, 4, 5\}$ betrachten wir die Relation

$$T := \{(1,1), (2,2), (3,3), (4,4), (5,5), (1,2), (2,1), (4,5), (5,4)\}.$$

Die Relation $T$ ist eine Äquivalenzrelation. Dies braucht nicht geprüft werden. Für jedes $x \in M$ gebe man die Äquivalenzklasse $[x] = \{y \in M : xTy\}$ explizit an. Geben Sie ferner die Faktormenge $M/T$ explizit an. (Achten Sie auch auf das richtige Setzen der Mengenklammern.)

c) Für $x, y \in \mathbb{Z}$ setzen wir

$$x \otimes y := x \cdot y - x - y + 2.$$

Man entscheide mit stichhaltiger Begründung, ob die Verknüpfung $\otimes : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ kommutativ ist und ob $\otimes$ assoziativ ist. (Hier stehen $+$, $-$ bzw. $\cdot$ für die gewöhnliche Addition, Subtraktion bzw. Multiplikation in $\mathbb{Z}$.)

**Aufgabe 2. (4 Punkte)** Wir bezeichnen mit $\varphi$ die Eulersche $\varphi$-Funktion.

a) Berechnen Sie $\varphi(990)$.

b) Bestimmen Sie (einschließlich einer stichhaltingen Begründung) *alle* Zahlen $n \geq 1$, die $\varphi(n) = 10$ erfüllen. (Hinweis: Zeigen Sie zunächst, dass eine solche Zahl von der Form $n = 2^e \cdot 3^f \cdot 11^g$ sein muß.)

**Aufgabe 3. (6 Punkte)**

a) Berechnen Sie den größten gemeinsamen Teiler $g = ggT(31, 101)$. Berechnen Sie ferner $u, v \in \mathbb{Z}$ mit $g = 31u + 101v$.

b) Entscheiden Sie, ob $[31]_{101}$ eine Einheit in $\mathbb{Z}/101$ ist und bestimmen Sie gegebenenfalls das zu $[31]_{101}$ inverse Element.

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

$$x \equiv 94 \bmod 101 \quad \text{und} \quad x \equiv 4 \bmod 31$$

erfüllt.

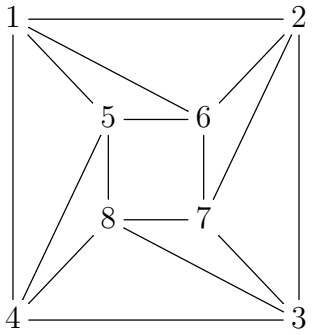
*In allen Teilaufgaben soll der Rechenweg in verständlicher Weise angegeben werden.*

**Aufgabe 4. (4 Punkte)** Wir betrachten die folgende Mini-Version von RSA: Alice hat zwei Primzahlen $p \neq q$ gewählt, $N = pq$ berechnet und $N = 55$ öffentlich gemacht. Der öffentliche Verschlüsselungsexponent von Alice ist $e = 3$.

a) Was ist die RSA-Verschlüsselung der Nachricht $m = [2]_{55} \in \mathbb{Z}/55$ an Alice?

b) Der RSA-Modul $N$ ist zu klein, um Sicherheit zu bieten. Berechnen Sie $p$, $q$, $\varphi(N)$ und den geheimen Entschlüsselungsexponenten $d$ von Alice.

**Aufgabe 5. (10 Punkte)** Wir betrachten den in der Skizze dargestellten endlichen, einfachen Graphen $\Gamma = (V, E)$:




a) Entscheiden Sie, ob $\Gamma$ hamiltonsch ist, und geben Sie gegebenenfalls einen Hamiltonkreis in $\Gamma$ explizit an.

b) Entscheiden Sie, ob $\Gamma$ eulersch ist, und geben Sie gegebenenfalls eine Euler-Tour in $\Gamma$ explizit an.

c) Was ist die chromatische Zahl $\chi = \chi(\Gamma)$ von diesem Graphen? Beweisen Sie die Antwort, die Sie geben, in dem Sie

- eine Knotenfärbung von $\Gamma$ mit $\chi$ Farben explizit angeben und
- stichhaltig begründen, warum es für $\Gamma$ keine Knotenfärbung mit weniger als $\chi$ Farben gibt.

d) Wir betrachten nun den Graph $\Gamma' = (V, E \cup \{\{5,7\},\{6,8\},\{2,5\}\})$, der aus $\Gamma$ durch Hinzufügen der drei Kanten $\{5,7\}$, $\{6,8\}$ und $\{2,5\}$ entsteht. Entscheiden Sie, ob $\Gamma'$ plättbar ist, und geben Sie eine stichhaltige Begründung für die Aussage, die Sie treffen.

e) Geben Sie die Aussage des Satzes von Ore über die Existenz von Hamilton-Kreisen wieder.

# Lösungsskizze

**Aufgabe 1.**

a) *Behauptung:* $S$ ist reflexiv.
*Beweis.* Es gilt $|x - x| = 0 \leq 2$ und daher $xSx$ für alle $x \in \mathbb{R}$.

*Behauptung:* $S$ ist nicht transitiv. *Beweis.* Es gilt $0S2$ (denn $|0 - 2| = 2 \leq 2$) und $2S4$ (denn $|2 - 4| = 2 \leq 2$) aber nicht $0S4$ (da $|0 - 4| = 4 > 2$).

*Behauptung:* $S$ ist symmetrisch. *Beweis.* Wenn $xSy$ gilt, dann folgt $|x-y| \leq 2$, und da $|y - x| = |-(x - y)| = |x - y|$ gilt erzwingt das $|y - x| \leq 2$ und daher $ySx$.

b) Es gilt $[1] = \{1, 2\}, [2] = \{1, 2\}, [3] = \{3\}, [4] = \{4, 5\}$, und $[5] = \{4, 5\}$. Ferner gilt

$$M/T = \{\{1, 2\}, \{3\}, \{4, 5\}\}.$$

c) Es gilt

$$y \otimes x = yx - y - x + 2 = xy - x - y + 2 = x \otimes y$$

für alle $x, y \in \mathbb{Z}$. Daher ist $\otimes$ kommutativ.

Ferner gilt

$$\begin{aligned} x \otimes (y \otimes z) &= x \otimes (yz - y - z + 2) = \\ &= x(yz - y - z + 2) - x - (yz - y - z + 2) + 2 = \\ &= xyz - xy - xz - yz + x + y + z \end{aligned}$$

und

$$\begin{aligned} (x \otimes y) \otimes z &= (xy - x - y + 2) \otimes z = \\ &= (xy - x - y + 2)z - (xy - x - y + 2) - z + 2 = \\ &= xyz - xz - yz - xy + x + y + z = \\ &= xyz - xy - xz - yz + x + y + z \end{aligned}$$

für alle $x, y, z \in \mathbb{Z}$. Daher ist $\otimes$ assoziativ.

**Aufgabe 2.**

a) $\varphi(990) = \varphi(2 \cdot 3^2 \cdot 5 \cdot 11) = (2 - 1) \cdot 3 \cdot (3 - 1) \cdot (5 - 1) \cdot (11 - 1) = 240$.

b) *Behauptung.* Wenn $\varphi(n) = 10$ gilt, dann gibt es Zahlen $e, f, g \geq 0$ mit $n = 2^e 3^f 11^g$.
*Beweis.* Gelte $\varphi(n) = 10$ und sei $p$ ein Primteiler von $n$. Dann ist $\varphi(n) = 10$ durch $p-1$ teilbar nach der Formel aus der Vorlesung, die schon in a) benutzt wurde. Es kann also nicht $p \geq 12$ gelten, denn sonst wäre $p - 1 > 10$. Daher ist $p \leq 11$. Wäre $p = 5$ müßte 10 durch 4 teilbar sein, was nicht der Fall ist. Wäre $p = 7$, so müßte 10 durch 6 teilbar sein, was ebenfalls nicht der Fall ist. Also muß $p \in \{2, 3, 5\}$ gelten. Die Zahl $n$ ist hat also höchstens 2, 3 oder 5 also Primteiler und ist daher von der in der Behauptung geschilderten Gestalt. $\square$

*Überlegung.* Seien nun $e, f, g \geq 0$ Zahlen mit $\varphi(2^e 3^f 11^g) = 10$. Sei $n = 2^e 3^f 11^g$. Wäre $g \geq 2$ so würde folgen, dass 10 durch $\varphi(11^g) = 11^{g-1} \cdot 10$ also insbesondere durch 110 teilbar wäre, was nicht der Fall ist. Also folgt $g \in \{0, 1\}$. Es kann andererseits nicht $g = 0$ gelten, da sonst $\varphi(n) = \varphi(2^e 3^f)$ nicht durch 5 teilbar wäre und somit nicht gleich 10 sein könnte. Dies erzwingt $\boxed{g = 1}$ und $\varphi(2^e 3^f) = 1$.

Aus $\varphi(2^e 3^f) = 1$ folgt $\varphi(2^e) = 1$ und $\varphi(3^f) = 1$ und letzteres erzwingt $\boxed{f = 0}$, da sonst $\varphi(3^f) = 3^{f-1} \cdot 2$ zu groß. Aus $\varphi(2^e) = 1$ folgt schließlich $\boxed{e \in \{0, 1\}}$. Insgesamt folgt $n \in \{11, 22\}$. Man sieht leicht, dass umgekehrt auch wirklich $\varphi(11) = 10$ und $\varphi(22) = 10$ gilt. □

*Antwort.* Genau dann gilt $\varphi(n) = 10$, wenn $n = 11$ oder $n = 22$ gilt.

**Aufgabe 3.**

a) Es gilt

$$\begin{aligned} 101/31 &= 3 \text{ Rest } 8 \\ 31/8 &= 3 \text{ Rest } 7 \\ 8/7 &= 1 \text{ Rest } 1 \end{aligned}$$

und daher

$$\mathrm{ggT}(101, 31) = \mathrm{ggT}(31, 8) = \mathrm{ggT}(8, 7) = \mathrm{ggT}(7, 1) = 1.$$

Durch Rückwärtseinsetzen erhält man

$$\begin{aligned} 1 &= 8 - 7 = 8 - (31 - 3 \cdot 8) = -31 + 4 \cdot 8 = \\ &= -31 + 4 \cdot (101 - 3 \cdot 31) = 4 \cdot 101 - 13 \cdot 31. \end{aligned}$$

b) Da $\mathrm{ggT}(31, 101) = 1$ gilt, muss $[31]$ eine Einheit in $\mathbb{Z}/101$ sein. Ferner gilt (vgl. Teil a))

$$1 = 4 \cdot 101 - 13 \cdot 31 = -13 \cdot 31 \bmod 101$$

und daher $[31]^{-1} = [-13] = [88]$.

c) Nach a) gilt $1 = 4 \cdot 101 - 13 \cdot 31$. Daher erfüllt

$$x = 4 \cdot 101 \cdot 4 - 13 \cdot 31 \cdot 94 = -36266$$

die beiden Kongruenzen.

*Anmerkungen:*

- Wegen $-36266 = 1306 \bmod 31 \cdot 101$ erfüllt 1306 die beiden Kongruenzen ebenfalls.
- Statt obigem systematischem Ansatz kann man auch versuchen, eine Lösung zu erraten.

**Aufgabe 4.**

a) Die Verschlüsselung ist $c = [2]_{55}^3 = [8]_{55}$.

b) Durch Faktorisieren von $N$ erhält man $p = 5$, $q = 11$. Es folgt $\varphi(N) = (p-1)(q-1) = 40$. Ferner weiß man, dass $ed = 1 \bmod \varphi(N)$ und daher $3d = 1 \bmod 40$ gelten muss. Man sieht, dass $d = 27$.

**Aufgabe 5.**

a) Zum Beispiel ist $(1, 2, 3, 4, 8, 7, 6, 5, 1)$ ein Hamilton-Kreis in $\Gamma$. Insbesondere ist $\Gamma$ hamiltonsch.

b) Zum Beispiel ist $(1, 5, 6, 2, 1, 6, 7, 2, 3, 7, 8, 3, 4, 8, 5, 4, 1)$ eine Euler-Tour in $\Gamma$. Insbesondere ist $\Gamma$ eulersch[1].

c) Es gilt jedenfalls $\chi(\Gamma) \geq 3$, da $\Gamma$ das Dreieck $\Delta$ mit Knoten $5, 6, 1$ enthält. Nehmen wir an, es gäbe eine Knotenfärbung $f : K \to \{\text{rot}, \text{gelb}, \text{blau}\}$. Die Knoten $5, 6, 1$ müßten dann unterschiedlich gefärbt sein, o.E. $f(1) = \text{rot}$, $f(5) = \text{gelb}$ und $f(6) = \text{blau}$. Da 2 mit 1 und 6 verbunden ist kann $f(2)$ weder rot noch blau sein. Also müßte $f(2) = \text{gelb}$ gelten. Da 7 mit 6 und 2 verbunden ist würde das $f(7) = \text{rot}$ erzwingen. Daraus würde folgen, dass $f(3) = \text{blau}$, weil 3 mit 7 und mit 2 verbunden ist. Nun ist 8 mit dem gelben Knoten 5, dem roten Knoten 7 und dem blauen Knoten 3 verbunden. Widerspruch - man sieht, dass man mit 3 Farben nicht auskommt.

Es gilt also $\chi(\Gamma) \geq 4$. Geben nun eine Knotenfärbung mit 4 Farben explizit an[2]:

| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
|---|---|---|---|---|---|---|---|
| rot | gelb | blau | grün | gelb | blau | grün | rot |

Es muss also $\chi(\Gamma) = 4$ gelten.

d) *Behauptung:* $\Gamma'$ ist nicht plättbar. *Beweis.* $\Gamma'$ hat $v = 8$ Knoten und $e = 19$ Kanten. Wäre $\Gamma'$ plättbar, so müßte nach Vorlesung $e \leq 3v - 6$ gelten was nicht der Fall ist. (Hier ist $3v - 6 = 18$ und $e = 19$ - zu viele Kanten).

e) Siehe Skript.

[1] Dass $\Gamma$ eulersch ist sieht man auch daran, dass alle Knotengrade gerade sind.

[2] Aus dem Vierfarbensatz von Apel und Haken folgt, dass eine solche Färbung existiert, da $\Gamma$ offensichtlich plättbar ist.