8. März 2011 Prof. Dr. W. Bley

UNIVERSITÄT KASSEL

Lösungen zur Klausur WS 2010/11 Diskrete Strukturen II (Informatik)

1	2	3	4	5	6	$\sum$

Name: ....

Matr.-Nr.: ....

Viel Erfolg!

Aufgabe 1 **(4 Punkte)**

Sei $m > 1$ eine natürliche Zahl. Betrachten Sie die beiden folgenden Teilmengen der komplexen Zahlen

$$\begin{aligned} R &= \{a + bi \mid a, b \in \mathbb{Z}\}, \\ I &= \{ma + bi \mid a, b \in \mathbb{Z}\}. \end{aligned}$$

a) Zeigen Sie, daß durch

$$\alpha \sim \beta :\Longleftrightarrow \alpha - \beta \in I$$

eine Äquivalenzrelation auf R definiert wird.

b) Bestimmen Sie explizit die verschiedenen Äquivalenzklassen.

Lösung:

a) Es ist zu zeigen, dass $\sim$ reflexiv, symetrisch und transitiv ist.

Reflexivität: $\alpha \sim \alpha \iff \alpha - \alpha = 0 \in I$. Dies ist richtig, da offensichtlich $0 \in I$.

Symmetrie: $\alpha \sim \beta \iff \alpha - \beta \in I \iff \beta - \alpha \in I \iff \beta \sim \alpha$. Hierbei gilt die zweite Äquivalenz, da mit ξ auch $-\xi$ in I enthalten ist.

Transitivität: $\alpha \sim \beta, \beta \sim \gamma \implies \alpha - \beta, \beta - \gamma \in I$. Da I bezüglich der Addition abgeschlossen ist, folgt $(\alpha - \beta) + (\beta - \gamma) = \alpha - \gamma \in I$. Also ist $\alpha \sim \gamma$.

b) Es gibt m verschiedene Äquivalenzklassen, nämlich

$$s + I = \{s + am + bi \mid a, b \in \mathbb{Z}\}, \quad s = 1, \ldots, m - 1.$$

Aufgabe 2 **(6 Punkte)**

Es sei $G = S_4$ die Gruppe der Permutationen der Menge $\{1, 2, 3, 4\}$.

a) Bestimmen Sie die Anzahl der Elemente von G.

b) Berechnen Sie das Inverse zu $(1\ 2\ 3) \circ (3\ 4)$.

c) Hat G eine Untergruppe der Ordnung 5. Bestimmen Sie explizit eine Untergruppe der Ordnung 6.

d) Es sei U die kleinste Untergruppe von G, die die Permutationen $(1\ 2)$ und $(3\ 4)$ enthält. Es sei V die kleinste Untergruppe, die die Permutation $(1\ 2\ 3\ 4)$ enthält. Sind U und V isomorph?

Lösung:
a) $|S_4| = 4! = 24$.

b) $((1\ 2\ 3) \circ (3\ 4))^{-1} = (3\ 4) \circ (1\ 3\ 2) = (2\ 1\ 4\ 3)$.

c) Für jede Untergruppe H von G gilt nach dem Satz von Lagrange: $|H| \mid |G|$. Also kann es keine Untergruppe der Ordnung 5 geben. Betrachtet man die Menge aller Permutationen, die die 4 fix lassen, so erhält man eine zur S_3 isomorphe Untergruppe. Bekanntlich hat die S_3 genau 6 Elemente.

d) Als Untegruppen müssen sowohl U als auch V bezüglich $\circ$ abgeschlossen sein. Man sieht leicht ein, dass

$$\begin{aligned} U &= \{id, (1\ 2), (3\ 4), (1\ 2) \circ (3\ 4)\}, \\ V &= \{id, (1\ 2\ 3\ 4), (1\ 3) \circ (2\ 4), (1\ 4\ 3\ 2)\}. \end{aligned}$$

Da U kein Element der Ordnung 4 enthält, können die beiden Gruppen nicht isomorph sein.

Aufgabe 3 **(7 Punkte)**

a) Berechnen Sie das multiplikative Inverse von $\overline{13}$ in $\mathbb{Z}/100\mathbb{Z}$.

b) Finden Sie **eine** Lösung $x \in \mathbb{Z}$ der simultanen Kongruenzen

$$\begin{aligned} 13x &\equiv 1 \ (\bmod 100) \\ x &\equiv 2 \ (\bmod 9) \\ x^2 &\equiv 4 \ (\bmod 11) \end{aligned}$$

Lösung:
a) Mit Hilfe des Euklidischen Algorithmus berechnet man $1 = 3 \cdot 100 - 23 \cdot 13$. Also ist

$$\overline{13}^{-1} = \overline{-23} = \overline{77}.$$

b) Es gilt nach Teilaufgabe a)

$$13x \equiv 1(\bmod 100) \iff x \equiv 77(\bmod 100).$$

Die Gleichung $x^2 \equiv 4(\bmod 11)$ hat die beiden Lösungen ± 2 modulo 11. Löst man also die Gleichung $x \equiv 2(\bmod 99)$, so sind die zweite und dritte Kongruenz erfüllt. Man hat also noch die simultanen Kongruenzen

$$\begin{aligned} x &\equiv 77 \ (\bmod 100) \\ x &\equiv 2 \ (\bmod 99) \end{aligned}$$

zu lösen. Anwendung des im Rahmen des Chinesischen Restsatzes erlernten Verfahrens liefert zum Beispiel die Lösung $x = -7423$.

Aufgabe 4 **(5 Punkte)**

Es sei $p \neq 2$ eine Primzahl.

a) Sei $a \in \mathbb{Z}$ und es gelte $ggT(a, p) = 1$. Zeigen Sie:

$$a^{\frac{p-1}{2}} \equiv \pm 1 (\mod p).$$

b) Es sei $F = \mathbb{Z}/p\mathbb{Z}$ der Körper mit p Elementen. Wieviele Nullstellen hat das Polynom $x^p - x \in F[x]$ in F? Begründen Sie Ihre Antwort!

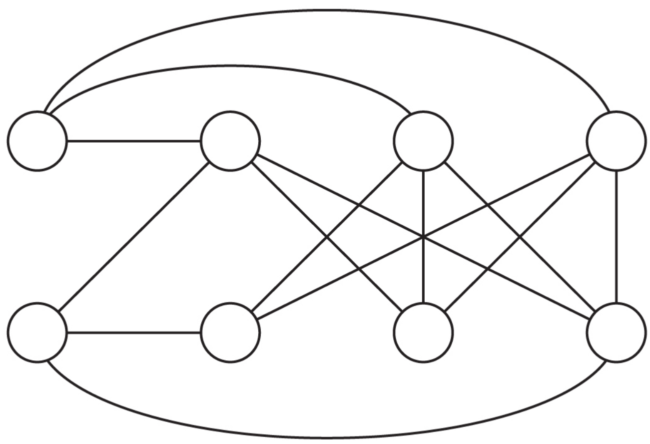
Lösung:
Der kleine Satz von Fermat besagt, dass $a^{p-1} \equiv 1 (\mod p)$ für alle $a \in \mathbb{Z}$ mit $ggT(a, p) = 1$. Wegen $\left(a^{(p-1)/2}\right)^2 \equiv 1 (\mod p)$ ist also $a^{(p-1)/2}$ eine Nullstelle von $x^2 - \bar{1} \in F[x]$, wobei $F = \mathbb{Z}/p\mathbb{Z}$. Dieses Polynom hat jedoch genau die Nullstellen $\overline{\pm 1}$. Hieraus folgt die Behauptung.

b) Wieder folgt aus dem "Kleinen Fermat", dass jedes $a \in F$ Nullstelle von $x^p - x = x(x^{p-1} - 1)$ ist. Also haben wir p Nullstellen.

Aufgabe 5 **(4 Punkte)**

a) Zeigen Sie, daß der vollständige Graph K_4 plättbar ist.

b) Ist der folgende Graph plättbar? Begründen Sie Ihre Antwort!



Lösung:
a) Das ist offensichtlich.

b) Wir numerieren die Knoten von links oben nach rechts unten mit 1 bis 8. Man streiche zunächst den Knoten 1 und und die Kanten $(1,4), (1,3), (5,8)$. Sodann verschmelze man den Knoten 5 und erhält dadurch den GEW-Graph. Also ist der Graph nach dem Satz von Kuratowski nicht plättbar.

Aufgabe 6 **(6 Punkte)**

(a) Bestimmen Sie die chromatische Zahl des Petersen-Graph.

(b) Gibt es einen bipartiten Graph mit 7 Knoten und 13 Kanten?

Begründen Sie Ihre Antworten!

Lösung:
a) Wie man leicht sieht, enthält der Petersen-Graph Kreise der Länge 5. Also ist er nicht bipartit und folglich gilt für die chromatische Zahl $\chi(G) \geq 3$. Andererseits findet man leicht eine Färbung mit drei Farben (etwa mit dem Greedy-Algorithmus). Also gilt: $\chi(G) = 3$.

b) Wie üblich habe der bipartite Graph Knoten $a_1, \ldots, a_n$ und $b_1, \ldots, b_m$. Es gilt also hier $n + m = 7$. Da von den a-Knoten nur Kanten zu den b-Knoten erlaubt sind, gibt es maximal nm verschiedene Kanten. Für das Paar (n, m) gibt es bis auf Symmetrie nur die Möglichkeiten $(1, 6), (2, 5), (3, 4)$. Also kann es höchsten 12 Kanten geben, ein bipartiter Graph mit 13 Kanten existiert also nicht.