TECHNISCHE UNIVERSITÄT BERLIN
Fakultät II – Institut für Mathematik
Prof. Stefan Felsner
Andreas Paffenholz

DISKRETE MAFI
Sommersemester 2005
Wiebke Höhn
Raman Sanyal
Xiumei Wang

DISKRETE UND STRUKTURELLE MATHEMATIK FÜR INFORMATIKER
5. ÜBUNGSBLATT

Abgabe am 20. Juni 2005 **vor** der Vorlesung

Zum Erreichen der vollen Punktzahl muss bei jeder Aufgabe der Lösungsweg vollständig angegeben werden.

Hinweise zur Klausur:

Die Klausur findet am 13. Juli 2004 von 14:00 bis 16:00 statt. Der genaue Ort wird noch bekanntgegeben.

Wenn Sie *zu einem Tutorium angemeldet sind, aber nicht an der Klausur teilnehmen möchten*, melden Sie sich bitte **bis zum 4. Juli 2004** per Mail an `paffenholz@math.tu-berlin.de` *ab* (Mail mit dem Subject: `MAFI Klausurabmeldung`) – andernfalls sind Sie automatisch zur Klausur angemeldet.

Wenn Sie *an der Klausur teilnehmen möchten, aber noch nicht zu einem Tutorium angemeldet sind*, melden Sie sich bitte **so bald wie möglich, aber spätestens bis zum 4. Juli 2005**, ebenfalls per Mail, zur Klausur *an*. Subject der Mail: `MAFI Klausuranmeldung`, Inhalt:
`Matrikelnr & Name & Vorname & Geschlecht & Studiengang & Semesterzahl.`

Voraussetzung für die Teilnahme an der Klausur ist das Erreichen von 50% der Punkte aus den Übungsblättern oder die erfolgreiche Bearbeitung der Übungsblätter in einem der vorangegangenen Jahre.
Voraussetzung für die Teilnahme an der Nachklausur ist die Teilnahme an der Klausur, bzw. - im Krankheitsfall - ein ärztliches Attest für den Tag der Klausur.
Zur Klausur zugelassen sind keinerlei Aufzeichnungen aus der Vorlesung und keine elektronischen Geräte, also insbesondere keine Mobiltelefone, Computer und Taschenrechner.

AUFGABE 1. — 3+1 PUNKTE

Sei A eine endliche Menge mit $|A| = n$, $n \geq 1$. Mit $S(A)$ bezeichnen wir die Menge aller bijektiven Abbildungen $\sigma : A \to A$.

(1) Zeigen Sie, dass $S(A)$ mit der Hintereinanderausführung von Abbildungen eine Gruppe bildet.
(2) Für welche n ist die Gruppe kommutativ?

AUFGABE 2. — 3 PUNKTE

Wir betrachten die Menge der Matrizen

$$M := \left\{ \begin{pmatrix} x & y \\ -y & x \end{pmatrix} \mid x, y \in \mathbb{Z} \right\},$$

Zeigen Sie, dass M mit der üblichen Matrizenaddition und -multiplikation ein Ring ist. Hat M eine Eins? Ist M auch ein Körper (Begründung!)?

Aufgabe 3. 3 Punkte

Zwei (endliche) Gruppen G_1 und G_2 heißen *isomorph*, wenn es eine bijektive Abbildung $\varphi : G_1 \to G_2$ gibt, die $\varphi(x_1 \circ x_2) = \varphi(x_1) \circ \varphi(x_2)$ erfüllt für alle $x_1, x_2 \in G_1$.

Geben Sie zwei nichtisomorphe Gruppen mit vier Elementen an (begründen Sie Ihre Antwort!).

Aufgabe 4. 2+3+2 Punkte

Sei G eine Gruppe mit Verknüpfung $\circ$. Eine Untergruppe ist eine Teilmenge $H \subseteq G$ von G mit der Eigenschaft, dass für alle $a, b \in H$ auch $a \circ b$ und a^{-1} in H enthalten sind.

Sei $g \in G$. Die *Rechtsnebenklasse* von H bzgl. g ist die Menge

$$R_g := H \circ g = \{x \in G \mid x = h \circ g \text{ für ein } h \in H\}.$$

Analog definiert man *Linksnebenklassen* durch

$$L_g := g \circ H = \{x \in G \mid x = g \circ h \text{ für ein } h \in H\}.$$

Die Menge der Linksnebenklassen von G wird mit G/H bezeichnet.

(1) Wann gilt $L_g = R_g$ für alle $g \in G$? Geben Sie ein Beispiel für eine Gruppe G mit einer Untergruppe H, so dass Rechts- und Linksnebenklassen in G bzgl. H verschieden sind.

Eine Untergruppe H heißt *Normalteiler* in G, wenn sie $g \circ H = H \circ g$ für alle $g \in G$ erfüllt. Auf der Menge G/H der Linksnebenklassen eines Normalteilers H definieren wir durch

$$(g_1 \circ H) \otimes (g_2 \circ H) := (g_1 \circ g_2) \circ H$$

eine Verknüpfung.

(2) Zeigen Sie, dass G/H mit der Verknüpfung $\otimes$ eine Gruppe bildet. Was ist die Eins in dieser Gruppe? Diese Gruppe heißt *Faktorgruppe* von G nach H.

(3) Sei

$$G := \left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \mid a, b, c \in \mathbb{R},\ a, c \neq 0 \right\} \qquad \text{und} \qquad H := \left\{ \begin{pmatrix} x & 0 \\ 0 & x \end{pmatrix} \mid x \in \mathbb{R} \setminus \{0\} \right\}.$$

Zeigen Sie,

(a) dass H ein Normalteiler von G ist, und

(b) dass die Faktorgruppe G/H isomorph zu einer Untergruppe von G ist. Geben Sie diese an.

Aufgabe 5. 3 Punkte

Ein Benutzer des RSA-Verfahrens wählt sich die beiden Primzahlen $p = 5$ und $q = 11$.

Bestimmen sie für diese Wahl alle möglichen Schlüsselpaare (e, d) von öffentlichem und privatem Schlüssel.