TECHNISCHE UNIVERSITÄT BERLIN
Fakultät II – Institut für Mathematik
Ekkehard Köhler

Diskrete MAFI
SoSe 2003

4. Übungsblatt zur Vorlesung
Diskrete und strukturelle Mathematik für Informatiker

Abgabe am 16. Juni *vor* der Vorlesung

Aufgabe 1: **6 Punkte**

Auf dem Kirchentag sind 800 Busse à 36 Pfadfindern eingetroffen. Einige sind wohl verloren gegangen. Sie können leicht schätzen, dass weniger als 5% der Pfadfinder vermisst werden.
Zwei Organisatoren machen sich ans Werk, die Schäfchen zu zählen. Der eine bittet die Pfadfinder sich in Gruppen zu siebt bzw. zu zweit zusammenzufinden. Anschließend zählt er, wieviele sich nicht mehr zu einer vollen Gruppe zusammenfinden konnten. Beim Gruppieren zu Siebenergruppen waren es 5, bei der Paarbildung ging es gerade auf.
Der zweite zählt zunächst 246 Pfadfinder ab, die sich am Pariser Platz in einer Reihe zwischen Brandenburger Tor und Heiligenschein aufstellen. Dann stellen sich die übrigen in immer neuen Reihen davor, so dass vor jedem Pfadfinder der vorhergehenden Reihe genau ein Pfadfinder in der neuen Reihe steht - und umgekehrt. Um die letzte Reihe auch noch aufzufüllen, fehlen 208 Pfadfinder. Danach läßt auch der zweite Organisator Gruppen, diesmal à 6 Pfadfindern, bilden. Dabei bleiben zwei verstörte Pfadis übrig.
Welcher der Organisatoren hat eine sinnvolle Methode gewählt, um die Zahl der vermissten Pfadfinder zu bestimmen?
Bestimmen Sie diese Zahl!

Aufgabe 2: **3+1 Punkte**

a) Wir nehmen an, dass jeder Monat genau 30 Tage hat. Wie sicher ist es, dass es jedes Jahr mindestens einen „Freitag den 13." gibt?

b) Wenn nun jeder Monat genau 28 Tage hätte, welche Fälle würden dann bezüglich der Häufigkeit eines „Freitag des 13." auftreten?

Aufgabe 3: **4 Punkte**

Eine Primzahl der Form $2^n - 1$ mit $n \in \mathbb{N}$ nennt man eine *Mersenne-Primzahl*. Zeige, dass $2^n - 1$ nur dann eine Primzahl sein kann, wenn n eine Primzahl ist. Ist für jede Primzahl n die Zahl $2^n - 1$ eine Primzahl?

Aufgabe 4: **2+2+2 Punkte**

Ihnen geht eine mit dem RSA-Algorithmus verschlüsselte Nachricht zu:

MAPLK .

Ihnen ist der geheime Schlüssel $d = 5$ sowie die öffentliche Zahl $m = 26$ bekannt. Die Nachricht wurde buchstabenweise verschlüsselt, die Buchstaben $A, B, \ldots, Z$ sind dabei den Zahlen $0, 1, \ldots, 25$ zugeordnet worden.

a) Erklären Sie, wie eine Nachricht entschlüsselt wird.

b) Entschlüsseln Sie die erhaltene Nachricht.

c) Bestimmen Sie zu $d = 5$ einen öffentlichen Schlüssel e.

Aufgabe 5: **4 Punkte**

a) Ein geheimes Nachrichtensystem soll aufgebaut werden. Benutzen Sie dazu den RSA-Algorithmus mit den Primzahlen $p = 89$ und $q = 127$. Vergeben Sie öffentliche und geheime Schlüssel und erklären Sie einem potentiellen Benutzer knapp, klar und präzise, wie eine Botschaft zu ver-, bzw. entschlüsseln ist.

b) Ein noch viel geheimeres System arbeitet modulo $m = 47053$. Der öffentlich bekannte Schlüssel eines Benutzers ist $e = 227$. Spione haben herausgefunden, dass m durch 223 teilbar ist. Nun fehlt nur noch etwas mathematisches Geschick, um den geheimen Schlüssel zu knacken. (*Tipp:* $8 \cdot 46620 + 1$ ist durch 227 teilbar.)

Zusatzaufgabe: **6 Punkte**
Ein Kodierer ist zu faul sich zwei Schlüssel zu merken. Er möchte daher zum Kodieren von Nachrichten, die aus Abfolgen von Steuerbefehlen, „RECHTS“ , „LINKS“ , „HOCH“ , „RUNTER“ , „VORWÄRTS“ und „RÜCKWÄRTS“ , bestehen, einen RSA-Code benutzen, bei dem beide Schlüssel 7 sind.

1. Realisieren Sie einen solchen Code mit möglichst kleinen Primzahlen.
2. Was wird passieren, wenn mit diesem Code wie in Aufgabe 3 Buchstaben kodiert und wieder dekodiert werden. Wählen Sie etwa das Wort „GUT “als Beispiel.

5. Übungsblatt zur Vorlesung
Diskrete und strukturelle Mathematik für Informatiker

Abgabe am 23. Juni *vor* der Vorlesung

Definition (zu Aufgabe 1):
Eine *Gruppe* ist ein Tupel $(G, \circ)$ aus einer Menge $G \neq \emptyset$ und einer Verknüpfung

$$\begin{aligned} \circ : G \times G &\longrightarrow G \\ (a, b) &\longmapsto a \circ b \end{aligned}$$

mit folgenden Eigenschaften (Gruppenaxiomen):

G1: $(a \circ b) \circ c = a \circ (b \circ c)$ für alle $a, b, c \in G$ (*Assoziativität*).

G2: Es gibt ein *neutrales Element* $e \in G$ mit $e \circ a = a$ für alle $a \in G$.

G3: Zu jedem $a \in G$ gibt es ein *inverses Element* $a' \in G$ mit $a' \circ a = e$.

Weiterhin heißt eine Gruppe $(G, \circ)$ *abelsch* oder *kommutativ*, falls $a \circ b = b \circ a$ für alle $a, b \in G$ (*Kommutativität*).
Beispiele für Gruppen sind $(\mathbb{Z}, +)$, $(\mathbb{Q} \setminus \{0\}, \cdot)$ oder $(\{A \in \mathbb{R}^{2\times 2} \mid \det A \neq 0\}, \cdot)$. Allgemeiner ist für jeden Ring $(R, +, \cdot)$ das Tupel $(R, +)$ eine abelsche Gruppe und für jeden Körper $(K, +, \cdot)$ ist $(K \setminus \{0\}, \cdot)$ eine abelsche Gruppe.

Aufgabe 1: **4 Punkte**
Es sei $(G, \circ)$ eine Gruppe. Man beweise:

a) $a \circ e = e \circ a = a$ für alle $a \in G$.

b) $a \circ a' = a' \circ a = e$ für alle $a \in G$.

c) Sind $a, b \in G$ mit $a \circ b = e$, so ist $a' = b$ und $b' = a$.

d) Zu $a, c \in G$ gibt es genau ein $b \in G$ mit $a \circ b = c$.

Wichtig: Geben Sie bei jedem Schritt bzw. bei jeder Umformung das verwendete Gruppenaxiom an.

Aufgabe 2: **8 Punkte**

Auf der Menge $\{\nabla, \triangle, \square, \lozenge\}$ sind die zwei Verknüpfungen $\bowtie$ und $\oslash$ durch folgende Tabellen gegeben:

$\bowtie$	∇	$\square$	$\triangle$	$\lozenge$
$\triangle$	$\triangle$	$\triangle$	$\triangle$	$\triangle$
∇	$\triangle$	∇	$\triangle$	∇
$\lozenge$	∇	$\lozenge$	$\triangle$	$\square$
$\square$	∇	$\square$	$\triangle$	$\lozenge$

$\oslash$	$\square$	$\lozenge$	$\triangle$	∇
$\lozenge$	$\triangle$	∇	$\lozenge$	$\square$
∇	$\lozenge$	$\square$	∇	$\triangle$
$\triangle$	$\square$	$\lozenge$	$\triangle$	∇
$\square$	∇	$\triangle$	$\square$	$\lozenge$

a) Zeigen Sie, dass dadurch ein Ring definiert ist. (Welche Operation muß als Addition gewählt werden?)

b) Bestimmen Sie das neutrale Element der Addition und der Multiplikation, bzw. zeigen Sie, dass die Multiplikation kein neutrales Element besitzt.

c) Sind die Strukturen kommutativ?

d) Gibt es Elemente ungleich dem neutralen Element, deren Produkt das neutrale Element ergibt?

e) Zeigen Sie an den Verknüpfungstabellen, dass es sich nicht um einen Körper handelt.

f) Geben Sie einen abstrakten Grund an, weshalb dies kein Körper ist.

g) Eine von beiden Verknüpfungen definiert eine Gruppe. Suchen Sie eine echte Teilmenge, auf der diese Verknüpfung auch eine Gruppe definiert. Kann man die Menge so einschränken, dass die andere Verknüpfung auf der eingeschränkten Menge eine Gruppe definiert?

h) Vertauscht man in den Tabellen einfach die Zeichen untereinander, so erhält man im Wesentlichen dieselbe Struktur. Kann man die Tabelle der Verknüpfung, die eine Gruppe definiert, auch noch auf eine andere Weise - also nicht durch bloßes Vertauschen der Zeichen - ändern, so dass dabei dennoch eine Gruppe definiert wird?

Aufgabe 3: **4 Punkte**

Sei R ein Ring. Ein Unterring $I \leq R$ heißt ein *Ideal* von R, wenn $\forall r \in R, s \in I : rs, sr \in I$.
Zeigen Sie:

a) In jedem Ring R bilden R und $\{\mathbf{0}\}$ Ideale - wobei „$\mathbf{0}$“ das neutrale Element der Addition im Ring bezeichnet.

b) Sei nun R ein kommutativer Ring mit Eins, für den gilt $\forall a, b \in R\backslash\{0\} : ab \in R\backslash\{0\}$. R hat genau dann zu jedem Element ungleich der Null ein Inverses, wenn R und $\{\mathbf{0}\}$ die einzigen Ideale von R bilden. (Achtung: Ideale von Ringen mit Eins sind im Allgemeinen nicht selbst wieder Ringe mit Eins!) Was haben Sie damit gezeigt?

Aufgabe 4: **6 Punkte**

Es sei

$$X := \left\{ \begin{pmatrix} x & y \\ -y & x \end{pmatrix} \mid x, y \in \mathbb{R} \right\} \subset \mathbb{R}^{2\times 2} \ .$$

Man zeige:

a) $(X, +, \cdot)$ ist ein Unterring von $(\mathbb{R}^{2\times 2}, +, \cdot)$.

b) $(X, +, \cdot)$ ist ein Körper.

(Motivation: $(X, +, \cdot)$ lässt sich mit den komplexen Zahlen identifizieren!)

Zusatzaufgabe: **6 Punkte**

Sei R ein Ring und I ein Ideal von R. Zeigen Sie:

a) Es wird $\forall x, y \in R$ durch $x \sim_I y \ :\Leftrightarrow \ \exists s \in I : x + s = y$ eine Äquivalenzrelation auf R definiert. Sei $R/\sim_I =: R/I$ die Menge der Äquvalenzklassen bezüglich $\sim_I$, mit zwei, wie folgt definierten Verknüpfungen: Seien$X, Y \in R/I, x, y \in R$ mit $x \in X$ und $y \in Y$:

$$X \oplus Y := \{z \in R | z \sim_I x + y\}$$
$$X \odot Y := \{z \in R | z \sim_I x \cdot y\}$$

b) Die beiden Verknüpfungen sind wohldefiniert.

c) R/I ist ein Ring.

d) Sei H das kleinste Ideal von $\mathbb{Z}$, das die 41 enthält. $\mathbb{Z}/H$ ist ein Körper.