Universität Duisburg-Essen
Fachbereich Mathematik
Prof. Dr. Günter Törner
Dipl.-Math. Verena Gondek

SS 2009

Übungen zu Algebra und Diskrete Mathematik I

Blatt 5

Aufgabe 17 (6 Punkte)

Beweisen Sie folgende Behauptung: In jeder Gruppe von mindestens zwei Personen gibt es zwei, die die gleiche Anzahl von Bekannten innerhalb dieser Gruppe haben. Dabei wird als Bekannte einer Person nicht die Person selbst mitgerechnet.

Aufgabe 18 (6 Punkte)

Betrachten Sie folgende Situation: In einer Menge von Städten sei jedes Paar von Städten durch genau eine von drei möglichen Verkehrsarten (Bus, Bahn, Flugzeug) verbunden. Dabei seien folgende Bedingungen erfüllt:

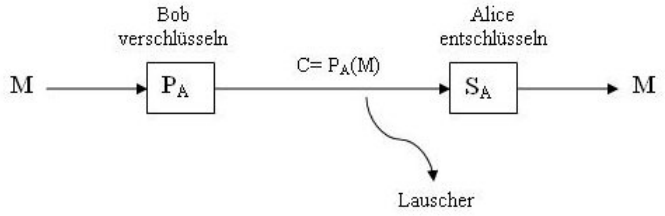
1. Alle drei Möglichkeiten treten im Städtenetz mindestens einmal auf.
2. Keine Stadt ist durch alle drei Transportarten eingebunden.
3. Keine drei Städte sind paarweise durch die gleiche Transportart verbunden.

Bestimmen Sie die maximale Anzahl von Städten, die man so verbinden kann, dass alle Bedingungen erfüllt sind.

Aufgabe 19 (6 Punkte)

In einem Verschlüsselungssystem mit *öffentlichem Schlüssel* besitzt jeder Teilnehmer einen öffentlichen und einen geheimen Schlüssel (public/private key, bzw. $P(\cdot)/S(\cdot)$). Diese beiden Schlüssel jedes Teilnehmers werden durch zueinander inverse Funktionen definiert. Für jede Nachricht M gilt also $P(S(M) = M = S(P(M))$.

Angenommen Teilnehmer Bob (B) will eine Nachricht M an Alice (A) versenden. Dazu verschlüsselt er die Nachricht mit dem öffentlichen Schlüssel von Alice: $C = P_A(M)$. Diese wiederum kann die erhaltene Nachricht C mit ihrem privaten Schlüssel entschlüsseln: $M = S_A(C)$. Diesen Vorgang verschaulicht die nachfolgende Grafik:



Bei der sogenannten *RSA-Verschlüsselung* erzeugt jeder Teilnehmer seinen öffentlichen und geheimen Schlüssel mit der folgenden Prozedur:

1. Er wählt zufällig zwei möglichst große verschiedene Primzahlen p und q.
2. Er berechnet $n := p \cdot q$.
3. Er wählt eine kleine ungerade ganze Zahl e, die teilerfremd zu $\phi(n)$ ist.
4. Er berechnet d als multiplikative Inverse von e modulo $\phi(n)$, d.h. $d \cdot e = 1 \bmod \phi(n)$.
5. Er veröffentlicht das Paar $P = (e, n)$ als seinen öffentlichen RSA-Schlüssel.
6. Er behält das Paar $S = (d, n)$ als geheimen RSA-Schlüssel für sich.

Man chiffriert eine Nachricht M mit dem öffentlichen Schlüssel mit Hilfe der Transformation:

$$P(M) = M^e (mod\ n) \tag{1}$$

Genauso kann man eine chiffrierte Nachricht C mit dem geheimen Schlüssel entschlüsseln:

$$S(C) = C^d (mod\ n) \tag{2}$$

Beweisen Sie, dass dieses Verfahren für Nachrichten $M \in \mathbb{Z} := \{0, \ldots n-1\}$ funktioniert, also dass die auf diese Weise definierten Funktionen invers zueinander sind.

Hinweis: Verwenden Sie (ohne Beweis) den sogenannten kleinen Satz von Fermat: Ist p eine Primzahl und $m \in \mathbb{N}$, dann gilt: $m^p = m \bmod p$.

Aufgabe 20 (6 Punkte)

Es seien $n \in \mathbb{N}$ und $a \in \mathbb{C}$. Zeigen Sie:

1. $\sum_{k=0}^{n} \binom{a}{k} x^k y^{n-k} = \sum_{k=0}^{n} \binom{n-a}{k} (-x)^k (x+y)^{n-k}$.
2. $\sum_{k=0}^{n} \binom{2n+1}{k} 2^{n-k} = \sum_{k=0}^{n} \binom{n+k}{k} 3^{n-k}$.

Hinweis: Verwenden Sie für Teil 1 die Polynommethode.

Abgabe: Bis Montag, den 25. Mai 2009, 10:30 im Postkasten LE 4.Etage.