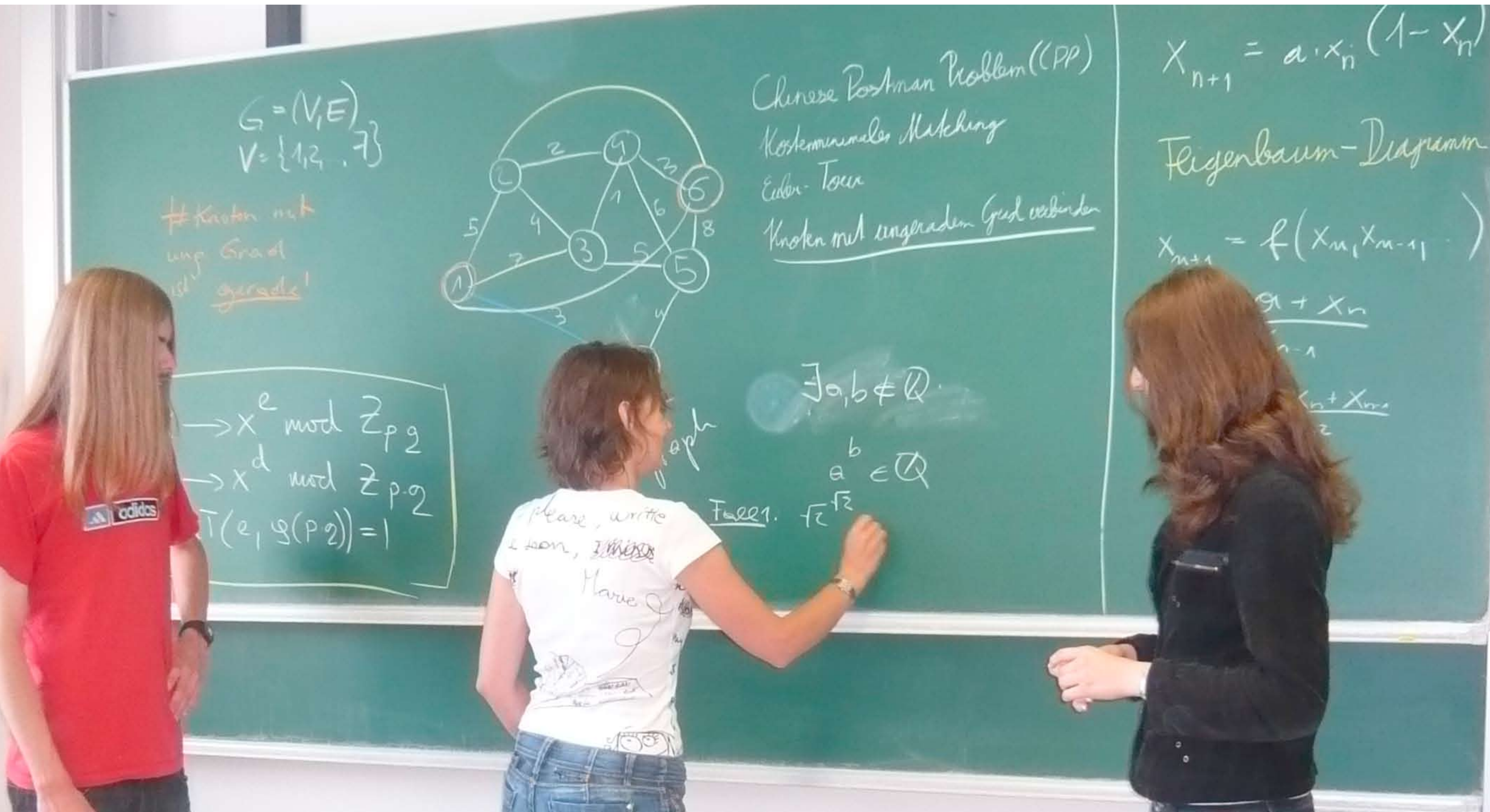


>>it-Ferialpraktikum

7. Juli-5. August 2008

Projekt: Kryptologie, Kombinatorische Optimierung, Dynamische Systeme



Projektbeschreibung bzw. Aufgaben der IT-PraktikantInnen innerhalb dieses Projektes

3 Bereiche - 2 PraktikantInnen - 1 Monat

Durch das vom FFG geförderte Projekt „Forschung macht Schule“ absolvierten zwei mathematikbegeisterte SchülerInnen ein Praktikum am Institut für Mathematik der Alpen-Adria-Universität. Sie arbeiteten an Projekten in den drei Schwerpunktbereichen Kryptologie, Kombinatorische Optimierung und Dynamische Systeme.

Kryptologie

In vielen modernen kryptographischen Verfahren werden Daten durch die Elemente eines endlichen Körpers $GF(q)$ oder eines Restklassenringes $Z/(p,q)$ der ganzen Zahlen Z modulo dem Produkt zweier Primzahlen p und q quellenkodiert und dann mittels einer Potenzpermutation „ x geht über in x^e “ verschlüsselt. Es gilt nun die Anzahl der Fixpunkte der als Chiffrierfunktion verwendeten Potenzpermutation, die Zyklenlänge der verwendeten Permutationen und die Struktur der Gruppe aller möglichen Potenzpermutationen zu untersuchen.

Kombinatorische Optimierung

In der Kombinatorischen Optimierung beschäftigten sich die PraktikantInnen mit dem Briefträgerproblem und in diesem Zusammenhang auch mit dem Dijkstra-Algorithmus, Euler-Touren und kostenminimalen Matchings. Ein Ausschnitt aus der Klagenfurter Innenstadt wurde ausgewählt, um das Briefträgerproblem darauf anzuwenden. Die geschickte Auswahl des Stadtteils war eine der Herausforderungen, um das Finden der optimalen Lösung durch einen Laien möglichst schwierig - aber möglich - zu machen.

Dynamische Systeme

Viele Ergebnisse in der Theorie diskreter und kontinuierlicher dynamischer Systeme basieren auf Computerexperimenten. Dies gilt unter anderem bei der Analyse von Systemen betreffend Existenz und Anzahl von periodischen Lösungen, in der Bifurkationstheorie (Analyse von Systemen in Abhängigkeit von Parametern) und insbesondere bei Untersuchungen von chaotischen Phänomenen. Bereits für - auf den ersten Blick - sehr einfache Systeme gibt es keine oder nur ansatzweise Lösungen zu den angeführten Fragestellungen. Die FerialpraktikantInnen bekamen anhand von einfachen Beispielen einen Einblick in diese aktuellen und faszinierenden Forschungsbereiche. Sie führten Computerexperimente zu folgenden offenen Fragestellungen durch:

- * periodische Lösungen von Differenzgleichungen mit rationalen Funktionen;
- * Anzahl und Lage von Grenzzyklen der Systeme $x'=P(x,y)$, $y'=Q(x,y)$ mit quadratischen Polynomen P und Q

Praktikumsgeber

Alpen-Adria-Universität
Institut für Mathematik
Universitätsstraße 65-67
9020 Klagenfurt
<http://www.uni-klu.ac.at/tewi/tema/math/>

BetreuerInnen

Univ.-Prof. Dr. Winfried Müller
(Winfried.Mueller@uni-klu.ac.at)
Ao. Univ.-Prof. Dr. Christine Nowak
(Christine.Nowak@uni-klu.ac.at)
Dr. Angelika Wiegele (Angelika.Wiegele@uni-klu.ac.at)

PraktikantInnen

Manuel Grumet, 6. Klasse, BG Tanzenberg
Miriam Hraßnigg, 7. Klasse, BRG Klagenfurt-Viktring