NR. 23 – JANUAR 2011

MATHE-LMU.DE

FÖRDERVEREIN MATHEMATIK IN WIRTSCHAFT, UNIVERSITÄT UND SCHULE AN DER LUDWIG-MAXIMILIANS-UNIVERSITÄT MÜNCHEN E.V.

LMU LUDWIG-MAXIMILIANS-UNIVERSITÄT MÜNCHEN

ÜBERFLIEGER GESUCHT!

Ihr seid in der Jahrgangsstufe 13?
Dann haben wir eine gute Idee, was ihr mit euren abgeschlossenen Facharbeiten noch tun könnt:

Beteiligt euch mit euren Arbeiten an einem besonderen Wettbewerb!

DR. HANS RIEGEL-STIFTUNG

Dr. Hans Riegel-Fachpreise für Mathematik, Biologie, Chemie, Physik und Geographie

Teilnahmeberechtigt sind alle Schülerinnen und Schüler der 13. Jahrgangsstufe der Gymnasien in München und Umland (S-Bahn-Bereich).
Teilnahmebedingungen sowie das Formblatt »Bewerbung für die Dr. Hans Riegel-Fachpreise« findet ihr unter:

www.physik.uni-muenchen.de/DrHansRiegelFachpreis

Liebe Leserinnen und Leser, Liebes Vereinsmitglied,

um neue Studierende für unsere Mathematik-Studiengänge zu gewinnen, bemüht sich das Mathematische Institut um ein vielfältiges Angebot für Schülerinnen und Schüler. Aktuell können wir auf das Programm „Mathematik am Samstag“ hinweisen, in dessen Rahmen in nächster Zeit wieder Mitarbeiter des Instituts über interessante mathematische Probleme in allgemeinverständlicher Form vortragen werden. Mit dem „Mobilen MatheLabor“ und dem Programm „Call a MatheProf“ bietet das Institut an, direkt an Schulen zu gehen.

Im letzten Jahr wurde ein neues Projekt ins Leben gerufen: ein Wettbewerb für Mathematik-Facharbeiten von Schülern aus Oberbayern. Die drei besten Arbeiten wurden mit Geldpreisen der Dr. Hans Riegel-Stiftung ausgezeichnet. Auf Seite 24 finden Sie einen ausführlichen Bericht über diesen Wettbewerb und die erste Preisverleihung.

Darüber hinaus wurde im letzten Jahr ein Schulportal neu gestaltet. Dort können sich Schülerinnen, Schüler und Lehrer u. a. über aktuelle Veranstaltungen des Mathematischen Instituts informieren. Die Internet-Adresse und eine genauere Beschreibung des Portals finden Sie auf der Seite 9.

Vitali Wachtel

an dieser Stelle werden Sie vermutlich, wie seit einigen Ausgaben gewohnt, wieder ein paar Zeilen über die umfangreichen Aktivitäten von Mitgliedern unseres Fördervereins etwa bei Öffentlichkeitsveranstaltungen des Mathematischen Instituts erwarten. Leider habe ich diesmal die traurige Pflicht, Sie über den tragischen Unfalltod eines unserer langjährigen Vereinsmitglieder in Kenntnis zu setzen.

Herr Studienrat Winfried Roppel, ein überaus engagierter und äußerst beliebter Mathematik- und Physiklehrer am Ignaz-Günther-Gymnasium Rosenheim und darüber hinaus sehr erfolgreicher Lehrbeauftragter an der Hochschule Rosenheim, ist am 30. August 2010 in seinem Italienurlaub bei einer Klettertour nördlich des Gardasees tödlich verunglückt.

Zahlreiche Beileidsbekundungen, auch von vielen Schülerinnen und Schülern und deren Eltern, in einem lokalen Internetportal zeugen von der großen Betroffenheit, die diese schreckliche Nachricht ausgelöst hat. Auch der Förderverein Mathematik trauert um Winfried Roppel und wird seinem langjährigen treuen Mitglied stets ein ehrendes Andenken bewahren.

Ihr Erwin Schörner

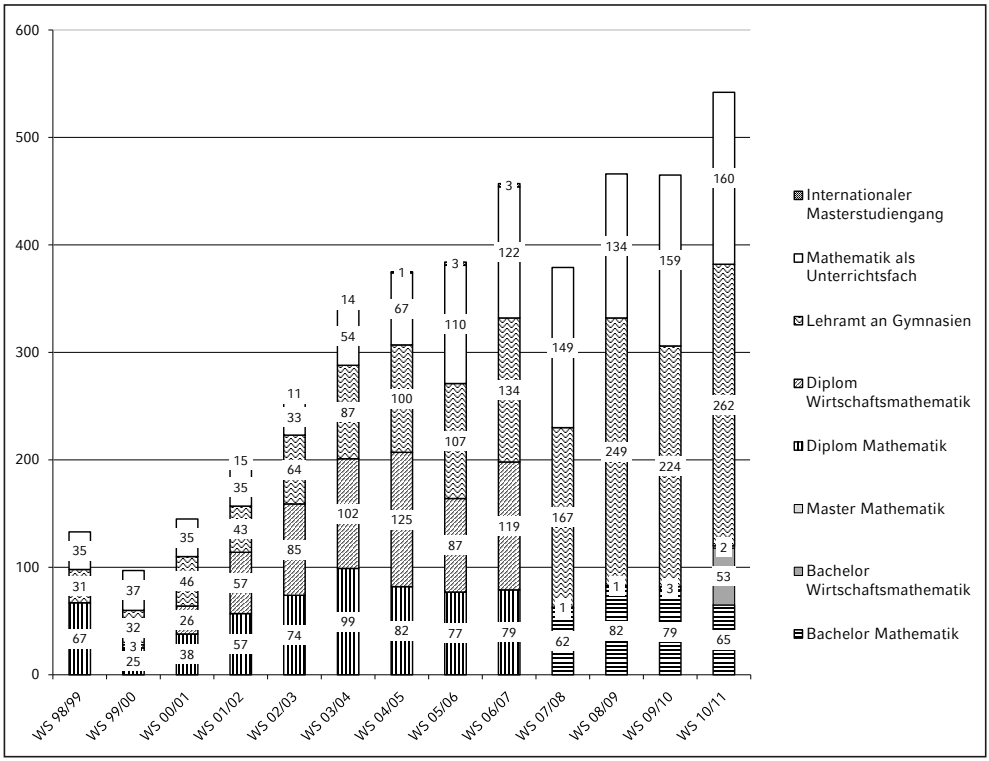
Impressum	**mathe-lmu.de**
Herausgeber	Förderverein Mathematik in Wirtschaft, Universität und Schule an der Ludwig-Maximilians-Universität München e.V., Mathematisches Institut, Universität München, Theresienstr. 39, 80333 München fmwus@mathematik.uni-muenchen.de Konto: 1267532, Bankleitzahl 700 500 00, Bayerische Landesbank
ViSdP	Vitali Wachtel, Mathematisches Institut, Universität München, Theresienstr. 39 80333 München, Tel. 2180-4488 wachtel@mathematik.uni-muenchen.de
Redaktion	Katharina Belaga, Bernhard Emmer, Daniel Rost, Erwin Schörner, Heinrich Steinlein, Vitali Wachtel
Auflage	5000
Layout	Gerhard Koehler, München, kws@kws-koehler.de
Druck	Siller Offsetdruck, Künzelsau

Die Redaktion bedankt sich bei den Firmen, die mit ihren Anzeigen die Herausgabe dieser Zeitung ermöglichten. Wir bitten die Leser um freundliche Beachtung der Anzeigen.

Berichte aus dem Mathematischen Institut

Studienangebot und Einschreibung Zum Wintersemester 2010/11 konnte das Studienangebot des Mathematischen Instituts erheblich erweitert werden: Neben den bereits seit drei Jahren mit großem Erfolg laufenden Bachelorstudiengang Mathematik trat nunmehr offiziell der neu konzipierte und auf die besonderen Anforderungen in der Finanz- und Versicherungswirtschaft zugeschnittene Bachelorstudiengang Wirtschaftsmathematik; darüber hinaus starteten die beiden Masterstudiengänge Mathematik und Wirtschaftsmathematik. Ferner wurde der Prozess der Modularisierung der Lehramtsstudiengänge bei allen Schularten erfolgreich abgeschlossen.

Besonders erfreulich ist auch zu Beginn dieses Studienjahres wieder der Blick auf das Diagramm über die Neueinschreibungen in einen mathematischen Studiengang der LMU München: Die Zahl der Immatrikulationen übertrifft mit insgesamt 542 Studienanfängerinnen und Studienanfängern das bereits sehr hohe Niveau der Vorjahre um rund 20%. Im kommenden Jahr ist, auch bedingt durch den doppelten Abiturjahrgang in Bayern und die Aussetzung der Wehrpflicht, mit einem weiteren deutlichen Anstieg der Studierendenzahlen zu rechnen; das Mathematische Institut bereitet sich bereits seit längerem auf diese Herausforderung vor, um weiterhin gute Studienbedingungen anbieten zu können.



Die durch die Neufassung der Lehramtsprüfungsordnung I vorgeschriebene Modularisierung auch der Lehramtsstudiengänge wurde an der LMU München zum Wintersemester 2010/11 umgesetzt; dabei übernahm das Mathematische Institut bereits im Vorjahr durch die Umsetzung eines innovativen Konzepts für das vertiefte Studium der Mathematik für ein Lehramt an Gymnasien sowie die Beteiligung am Bachelorstudiengang „Prävention, Integration und Rehabilitation bei Hörschädigung", der auch zum Ersten Staatsexamen im Lehramt für Sonderpädagogik führt, eine Vorreiterrolle. Bei der Modularisierung des Unterrichtsfachs Mathematik für ein Lehramt an Grund-, Haupt- und Realschulen wurde vom Mathematischen Institut das seit langem erfolgreiche Konzept eigener, speziell auf die Bedürfnisse dieser Studierendengruppe zugeschnittener Lehrveranstaltungen weiterverfolgt.

Erstmals wurde im letzten Jahr ein Brückenkurs „0. Semester" Mathematik angeboten; in den beiden ersten Oktoberwochen und damit unmittelbar vor Beginn der eigentlichen Vorlesungszeit des Wintersemesters 2010/11 bereiteten Herr Prof. Pickl, Herr Prof. Rost und Herr Dr. Schörner zusammen mit einem engagierten Team die Erstsemester in den verschiedenen mathematischen Studiengängen mit interessanten Fragestellungen, die vormittags in Vorlesungen und nachmittags in Übungen und Tutorien behandelt wurden, auf die universitäre Mathematik vor und erleichterten so den rund 250 Teilnehmerinnen und Teilnehmern den Start ins Mathematikstudium.

Aktuelle Informationen, speziell für Schülerinnen und Schüler sowie Lehrerinnen und Lehrer, sind seit September 2010 in Internet auf dem neu konzipierten Schulportal zu finden, das sehr kompetent und engagiert von Frau Marianne Kardinal betreut wird; einen ausführlichen Artikel hierzu finden Sie auf Seite 9.

Personalien Wie bereits in der letzten Ausgabe berichtet, wurde Herr Prof. Derenthal (Freiburg) auf eine W2-Professur für Algebraische Geometrie berufen; darüber hinaus hat Herr Prof. Diening (Freiburg) den Ruf auf eine W2-Professur für Numerik angenommen, und Herr Prof. Pickl (ETH Zürich) ist auf einer neu geschaffenen W2-Professur für Stochastik (Schwerpunkt Lehramt Gymnasium) tätig. Die drei neuen Kollegen werden auf den Seiten 6 und 7 vorgestellt.

Darüber hinaus wurden vom Mathematischen Institut die Berufungsverfahren für die derzeit vakanten Professuren mit großem Nachdruck weiter vorangetrieben, so dass den erfolgreichen Besetzungen und Wiederbesetzungen dieser Stellen mit großer Zuversicht entgegengeblickt werden kann. Darunter befinden sich neben der für alle Lehramtsstudiengänge zentralen W3-Professur für Didaktik der Mathematik und Informatik (Nachfolge Reiss) und der neuen W2-Professur für Didaktik der Mathematik (Schwerpunkt Grundschule) insgesamt vier W2-Professuren für Mathematik bzw. für Angewandte Mathematik und eine W2-Stiftungsprofessur für Quantitative Financial Mathematics sowie eine W1-Juniorprofessur für Mathematik im Rahmen des Elitemasterstudiengangs „Theoretische und Mathematische Physik" und eine W1-Professur für stochastische Methoden der Finanz- und Versicherungswissenschaften.

Veranstaltungen Auch 2010 fand in der letzten Woche der bayerischen Sommerferien das überaus erfolgreiche Probestudium „LMU-Mathe-Sommer“ statt; Herr Dr. Thomas Richthammer, unterstützt von Frau Marianne Kardinal, Frau Nicole Langwieder, Herrn Peter Werthmüller und zahlreichen weiteren Mitarbeiterinnen und Mitarbeitern, bot heuer unter dem Motto „Heiratsvermittlung, kürzeste Wege und das Haus vom Nikolaus“ interessierten Oberstufenschülerinnen und Oberstufenschülern eine Einführung in die Graphentheorie. Rund 120 Teilnehmerinnen und Teilnehmer nutzten die Gelegenheit, sich ein authentisches Bild vom Mathematikstudium an der LMU zu machen.

Die Verabschiedung der Studierenden, die im vergangenen akademischen Jahr einen Abschluss in Mathematik oder Wirtschaftsmathematik erworben haben, erfolgt seit dem vergangenen Jahr in einer eigenen Veranstaltung, um unseren Ehemaligen einen feierlichen Rahmen zur Würdigung ihrer akademischen Leistungen zu bieten. Die Absolventenfeier für den Abschlussjahrgang 2009/10 des Mathematischen Instituts findet am 22. Januar 2011 in Zusammenarbeit mit dem Förderverein Mathematik und mit großzügiger Unterstützung durch den Verein zur Förderung der Versicherungswissenschaft statt.

Die Reihe „Mathematik am Samstag“, die sich seit mehr als zehn Jahren an alle Interessierten, vor allem aber an Schülerinnen und Schüler der gymnasialen Oberstufe richtet, wird auch in diesem Frühjahr mit drei interessanten Vorträgen fortgesetzt; das genaue Programm, Termine und Veranstaltungsort (im Uni-Hauptgebäude) findet man auf Seite 8.

Neu am Institut

Prof. Ulrich Derenthal

Seit Juli 2010 ist Ulrich Derenthal Professor für Mathematik am Lehrstuhl für Algebraische Geometrie der LMU. Ab 1999 studierte er Mathematik an der Universität Göttingen und an der University of California, Berkeley. Nach dem Diplom (2004) bei Ulrich Stuhler und der Promotion zum Thema „Geometry of universal torsors“ (2006) bei Yuri Tschinkel in Göttingen ging er an die Universität Zürich, zunächst als Postdoc bei Andrew Kresch und ab 2008 als Lecturer. Nach Forschungsaufenthalten bei János Kollár an der Princeton University und am Mathematical Sciences Research Institute (MSRI) in Berkeley war er seit 2009 Juniorprofessor für Arithmetische Geometrie an der Albert-Ludwigs-Universität Freiburg.

Die Forschung von Ulrich Derenthal steht vor dem Hintergrund der alten Frage der Zahlentheorie, was die rationalen Lösungen von Polynomgleichungen in mehreren Variablen mit rationalen Koeffizienten sind. Im Sinne der Arithmetischen Geometrie lässt sich das als die Frage nach rationalen Punkten auf algebraischen Varietäten formulieren.

Insbesondere interessiert er sich für Varietäten mit unendlich vielen rationalen Punkten. Die Verteilung dieser Punkte wird von einer Vermutung von Yuri Manin präzise vorhergesagt. Mit Methoden der Algebraischen Geometrie und der Analytischen Zahlentheorie ließ sich die Manin-Vermutung bereits für einige singuläre kubische Flächen beweisen.

Derzeit hält Ulrich Derenthal die Bachelor-Vorlesung Lineare Algebra. Er organisiert zwei Zahlentheorie-Seminare und zusammen mit Andreas Rosenschon das Oberseminar „Algebraische Geometrie“.

Neu am Institut

Prof. Lars Diening

Im September 2010 trat Lars Diening eine Professur am Lehrstuhl für Analysis, Mathematische Physik und Numerik an. Er studierte 1992 bis 1997 Mathematik an der Universität Münster und ging anschließend ein Jahr an die Michigan State University in den USA. Nach dem Beginn der Promotion in Bonn wechselte er mit seinem Betreuer Prof. Růžižka an die Universität Freiburg, wo er 2002 promovierte, 2007 habilitierte und 2010 Professor wurde.

Seine Schwerpunkte liegen im Bereich der Analysis, der numerischen Analysis und der Funktionenräume mit variablen Exponenten. Viele seiner Arbeiten sind motiviert durch das Studium verallgemeinerter Newton'scher Fluide und artverwandter nicht-linearer Minimierungsprobleme. Verallgemeinerte Newton'sche Fluide zeichnen sich dadurch aus, dass der Reibungsterm nicht wie bei Wasser oder Luft linear, sondern nicht-linear vom Geschwindigkeitsgradienten abhängt. In diesem Zusammenhang beschäftigt sich Lars Diening mit Fragen der Existenz, der Regularität, der numerischen Analyse freier Randwertprobleme.

Lars Diening beschäftigt sich auch mit den ungewöhnlichen elektrorheologischen Fluiden. Hierbei handelt es sich um spezielle Materialien, deren Zähigkeit von außen durch Anlegen eines elektrischen Feldes verändert werden kann, und zwar von flüssig bis nahezu fest. Hiermit kann man z. B. intelligente Stoßdämpfer bauen. Anfang 2011 erscheint ein Buch von Lars Diening, welches sich mit den zugehörigen Funktionenräumen mit variablen Exponenten beschäftigt.

Seine derzeitige Vorlesung Numerik wird er im Sommersemester fortsetzen.

Neu am Institut

Prof. Peter Pickl

Im September 2010 trat Peter Pickl, geboren 1975 in München, eine im Forschungsgebiet Stochastik angesiedelte Professur für Angewandte Mathematik an.

Herr Pickl studierte von November 1996 bis Ende 2000 Physik an der LMU. Nach Diplom (2000) und Promotion (2005) in Mathematik unter der Betreuung von Prof. Dr. Detlef Dürr, wirkte er für ein Jahr als Postdoc an der Universität Tübingen. Nach einem knapp zweijährigen Aufenthalt in Wien – zunächst als Stipendiat am Erwin Schrödinger Institut, später als wissenschaftlicher Mitarbeiter an der Universität Wien – war er, ebenfalls für zwei Jahre, Postdoc an der ETH in Zürich. Eine der Aufgaben von Herrn Pickl wird die Mitgestaltung des neu geschaffenen Studiengangs „Mathematik im Gymnasialen Lehramt", sowie die Ausbildung im fachlichen Teil dieses Studiums sein.

Der Forschungsschwerpunkt von Herrn Pickl liegt in der Mathematischen Physik. Er lieferte Beiträge zur mathematischen Streutheorie, QED und der numerischen Lösung der Schrödingergleichung. Momentan beschäftigt er sich hauptsächlich mit der Beschreibung quantenmechanischer und klassischer Vielteilchensysteme. Dabei betrachtet man ein System vieler wechselwirkender Teilchen, die anfänglich unabhängig verteilt sind. Es wird untersucht, ob die Unabhängigkeit näherungsweise auch für spätere Zeiten erhalten bleibt. Durch die Behandlung dieser Themen ist Herr Pickl Experte auf den Gebieten der Analysis und Stochastik.

Herr Pickl hält seit Oktober 2010 den viersemestrigen Zyklus der mathematischen Grundausbildung im gymnasialen Lehramt.

Mathematik am Samstag

Samstag, den 26.02.2011, 14.15 – 15.30

Herr Andreas Fackler	**Wie groß ist die Unendlichkeit?**
Wie viele Zahlen gibt es eigentlich? Erst seitdem Georg Cantor gegen Ende des 19. Jahrhunderts die Mengenlehre begründete, lässt sich diese Frage überhaupt mathematisch behandeln. Seine Theorie erlaubt es uns, unendlich weit zu zählen und Größen unendlich großer Mengen zu untersuchen. Und trotzdem ist die Sache mit der Zahl der Zahlen nicht so einfach.	

Samstag, den 19.03.2011, 14.15 – 15.30

Prof. Dr. Daniel Rost	**Mit 2 Euro an die Börse**
Soll man auf fallende Aktienkurse wetten und z. B. Optionsscheine erwerben? Und was wäre dafür ein „fairer Preis“? Anhand eines ganz einfachen Marktmodells spielen wir Börse und arbeiten uns zum Nobelpreis vor.	

Samstag, den 02.04.2011, 14.15 – 15.30

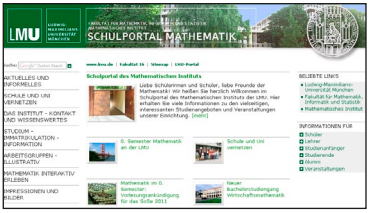
Prof. Dr. Peter Pickl	**Inkommensurabilität und Goldener Schnitt**
Zwei Strecken x,y heißen kommensurabel, wenn man ein gemeinsames Maß, d. h. eine geeignete dritte Strecke z finden kann, so dass x und y ganzzahlige Vielfache dieser Strecke z sind. Es stellt sich die Frage, ob man für jedes denkbare Paar von Strecken in der Ebene ein solches gemeinsames Maß finden kann. Im Vortrag wird anhand eines Beispiels gezeigt, dass dem nicht so ist: Zwei Strecken, deren Teilverhältnis der sogenannte Goldene Schnitt ist, sind inkommensurabel. Die Bedeutung dieser Erkenntnis soll anschließend erläutert werden.	

Alle Vorträge finden im Hörsaal A 125 im Universitätshauptgebäude, Geschwister-Scholl-Platz 1 statt (im 1. Stock südlich vom Audimax).

Herzlich Willkommen im Schulportal des Mathematischen Instituts

http://www.schulportal.mathematik.uni-muenchen.de

Im neu eröffneten **Schulportal des Mathematischen Instituts der LMU** werden Schülerinnen, Schüler und Lehrer über die vielseitigen Studienangebote und Veranstaltungen des Departments informiert.

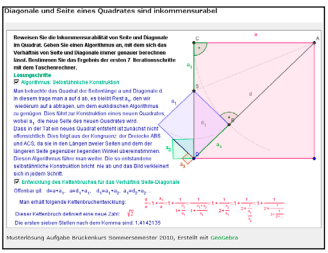


Ob Fragen zur Immatrikulation oder Wissenswertes über unsere Institutsgeschichte, die Website will bei allen Freunden der Mathematik das Interesse am Fach fördern und einen vielleicht geplanten Studienanfang erleichtern.

Darüber hinaus gewährt der ständig aktualisierte **News-Ticker** einen Einblick in neueste Ereignisse und Erkenntnisse aus der internationalen, mathematischen Welt.
In verständlicher Art und Weise werden die mathematischen Disziplinen der am Institut vertretenen wissenschaftlichen Arbeitsgruppen dargestellt.

In **Mathematik interaktiv erleben** findet man eine ständig wachsende Linksammlung mathematischer Seiten.

Unter **Schule und Uni vernetzen** wird der regelmäßige kommunikative Austausch des Instituts mit interessierten Schülerinnen, Schülern und Lehrern vorgestellt. Zum einen sind das **Probestudium, Brückenkurse** und **Mathematik am Samstag** für die Zielgruppe Schülerinnen und Schüler und zum anderen **Call am MatheProf**, **Mobiles Mathelabor** für Lehrerinnen, Lehrer und Schulen und natürlich der **Förderverein Mathematik** für alle.



Mit **Applets** zu Problemstellungen verschiedener Vorlesungen werden mathematische Denkmethoden und schwierige Beweisideen schulgerecht visualisiert.

Marianne Kardinal

Zur Emeritierung von Prof. Dr. Helmut Schwichtenberg

Zum Ende des Sommersemesters 2010 ist Herr Prof. Dr. Helmut Schwichtenberg in den Ruhestand getreten.

Helmut Schwichtenberg wurde am 5. April 1942 in Sagan (Niederschlesien) geboren. Nach dem Abitur studierte er ab 1961 an der Freien Universität Berlin, von wo er 1964 nach Münster wechselte. Er promovierte 1968 bei Dieter Rödding und wurde danach in Münster Assistent. 1974 habilitierte er sich in Münster und wurde noch im gleichen Jahr als Wissenschaftlicher Rat und Professor nach Heidelberg berufen.

1978 wurde er Nachfolger von Kurt Schütte auf dem Lehrstuhl für Mathematische Logik an der Ludwig-Maximilians-Universität München. Dort wirkte er in den folgenden 32 Jahren überaus erfolgreich und mit nie nachlassender Energie in Forschung, Lehre, akademischer Selbstverwaltung und Wissenschaftsorganisation. Bald entwickelte er sich zu einer der tragenden Säulen des Mathematischen Instituts und blieb dies bis zu seiner Emeritierung. Er war mehrfach Geschäftsführender Vorstand des Instituts und für zwei Amtszeiten (1985-87 und 2001-03) Dekan der Fakultät für Mathematik (Informatik und Statistik).

Von 1997 bis 2006 war er Sprecher des von ihm zusammen mit Kollegen aus der Informatik unserer Universität und der Technischen Universität München initiierten Graduiertenkollegs *Logik in der Informatik*. Der große Erfolg dieses Graduiertenkollegs ist zweifelsohne in erster Linie Helmut Schwichtenberg zu verdanken.

Davon abgesehen engagierte er sich in zahlreichen anderen Belangen für unser Institut. Er war Mitglied vieler wichtiger Kommissionen (u. a. der Kommissionen für den Aufbau der Bachelor- und Masterstudiengänge, der Kommission für die neue Departmentsordnung und der Lehrkommission) und Mitbegründer des Fördervereins „Mathematik in Wirtschaft, Universität und Schule“ und der bis heute sehr erfolgreichen Veranstaltung „Mathematik am Samstag“. In allen Gremien, denen er angehörte, verstand er es, seine stets sehr dezidierte Meinung wohlbegründet und hartnäckig zu vertreten. Meinungsverschiedenheiten und Differenzen jeglicher Art versuchte er stets in äußerst kollegialer Weise durch persönliche Gespräche mit den Beteiligten zu überwinden.

Schwichtenbergs wissenschaftliche Reputation wurde u. a. anerkannt durch die Wahl in die Bayerische Akademie der Wissenschaften im Jahr 1986 und die Berufung in den sehr einflussreichen Wissenschaftlichen Beirat des Mathematischen Forschungsinstituts Oberwolfach, dem er von 2001 bis 2008 angehörte.

Von 1982 bis 2008 gehörte er zu den Organisatoren der regelmäßig stattfindenden Oberwolfach-Tagungen zur Mathematischen Logik und war von 1989 bis 2007 Mitorganisator der internationalen Sommerschulen Marktoberdorf zum Thema „Anwendun-

gen der Logik in der Informatik". Von 1983 bis 1989 gehörte er zum Editorial Board der Annals of Pure and Applied Logic und seit 1985 ist er Mitherausgeber des Archive for Mathematical Logic.

Die wissenschaftlichen Arbeitsgebiete von Helmut Schwichtenberg sind die Beweistheorie und die Theorie der berechenbaren Funktionen, wobei sich der Schwerpunkt seiner Forschungen und seines Interesses im Lauf der Jahre immer mehr in Richtung zu Anwendungen dieser Gebiete in der Informatik verschoben hat. Seine ersten Publikationen befassten sich mit der Klassifikation der rekursiven Funktionen, insbesondere der Untersuchung verschiedener subrekursiver Hierarchien, deren wichtigste heute als Schwichtenberg-Wainer Hierarchie bekannt ist.

Während eines Gastaufenthalts an der Carnegie Mellon University in Pittsburgh (USA) im Jahre 1987/88 kam er mit der funktionalen Programmiersprache Scheme in Berührung. Er entdeckte Scheme als ein ideales Werkzeug zur Verwirklichung des Kreiselschen „unwinding" Programms, das die Analyse und Nutzung des rechnerischen Gehaltes von Beweisen zum Gegenstand hat. Dabei geht es um Folgendes: Jeder konstruktive Beweis einer Aussage der Gestalt „für alle x gibt es ein y, so dass $A(x,y)$" enthält implizit einen Algorithmus f, der angesetzt auf die Eingabe x ein Ergebnis $f(x)$ mit $A(x,f(x))$ liefert. Liegt der Beweis in formalisierter Form vor, so lässt sich dieser Algorithmus automatisch aus dem Beweis extrahieren (Programmextraktion). Da die Korrektheit eines Beweises maschinell überprüfbar ist, eröffnet sich so – zumindest im Prinzip – die Möglichkeit, automatisch korrekte Software zu produzieren.

Wieder zurück in München begann Schwichtenberg mit der Scheme-Implementierung des MINLOG Systems, welches neben Werkzeugen zur interaktiven Beweisentwicklung und automatischen Programmextraktion inzwischen noch eine Reihe anderer Komponenten besitzt. Mit seinem bis heute andauernden MINLOG Projekt und vielen wissenschaftlichen Publikationen leistete Helmut Schwichtenberg bedeutende Beiträge zur Logik und deren Anwendungen in der Informatik, insbesondere zu den Gebieten automatische Beweissuche, Beweissysteme mit beschränkter Komplexität, effiziente Normalisierung, Programmextraktion und konstruktive Mathematik.

Neben seinen eigenen Forschungen war und ist ihm die Förderung des wissenschaftlichen Nachwuchses ein besonderes Anliegen. Er hat jede sich bietende Möglichkeit ergriffen, um (unter erheblichem Aufwand an Zeit und Energie) Drittmittel-Projekte zu beantragen, aus denen er viele seiner über 20 Doktoranden und andere wissenschaftliche Mitarbeiter finanzieren konnte. Abgesehen von dem schon erwähnten Graduiertenkolleg hat er auf diesem Wege in den letzten 13 Jahren Mittel im Umfang von über 2 Millionen Euro eingeworben.

Mit großem Einsatz nahm er auch seine Tätigkeit als Vertrauensdozent der Studienstiftung des Deutschen Volkes sowie als Vertreter unserer Fakultät im Beirat für das Auslands- und Ausländerstudium der LMU wahr.

An seinem Lehrstuhl schuf er ein wissenschaftlich breites und anregendes Arbeitsumfeld, das viele hervorragende Studenten und hochkarätige Wissenschaftler aus allen Teilen der Welt anzog und ganz entscheidend zu dem hohen internationalen Renommee der Logik-Gruppe unseres Instituts beitrug.

W. Buchholz

Bericht über ein Praktikum bei der Unternehmensberatung d-fine

Praktikum

Als Studentin der Wirtschaftsmathematik ist es für mich von jeher von großem Interesse, die Anwendungsbereiche der Mathematik und dadurch auch die Tätigkeitsfelder von Mathematikern in verschiedenen Unternehmen kennen zu lernen.

Die Art und Weise, wie in Unternehmensberatungen gearbeitet wird, empfand ich dabei generell als recht ansprechend, vor allem wegen der vielfältigen, projektorientierten Aufgaben. So entschloss ich mich für ein Praktikum bei der Unternehmensberatung d-fine, zu welchem ich im Sommer 2010 antrat. d-fine ist mit seinen ungefähr 270 Beratern überwiegend in Deutschland tätig und auf strategische, quantitative und technische Fragestellungen im Risikomanagement spezialisiert. So berät d-fine vor allem Finanzdienstleistungsunternehmen, das heißt Banken, Versicherungen und Asset Manager, und das zum Beispiel bei der Entwicklung einer Risikostrategie oder der Einführung neuer Methoden zur Quantifizierung und Steuerung von Risiken und Erträgen. Nachdem die Berater dabei zumeist vor Herausforderungen stark quantitativer Natur stehen, ist es nicht verwunderlich, dass die Mehrheit der Mitarbeiter einstmals Mathematik oder Physik studierte.

Im Rahmen meines Praktikums bei d-fine wurde ich auf einem Kundenprojekt bei einem international tätigen Asset Manager eingesetzt. Dessen Bewertungsmethoden für die im eigenen Portfolio gehaltenen Finanzinstrumente sollten dabei auf den neuesten Stand der Technik gebracht und zudem aufsichtsrechtlichen Anforderungen angepasst werden. Einen Teil der Portfoliobewertung unter Risikogesichtspunkten machen dabei Schätzungen über Höhe oder Wahrscheinlichkeit eines möglichen Verlusts des Gesamtportfolios unter bestimmten Umständen aus. Hierzu zählen zum Beispiel das Konzept des Value-at-Risk, aber auch die Ergebnisse sogenannter „Stresstests“.

Als Projektmitarbeiterin wurde mir ebendiese Teilaufgabe zur „Parametrisierung historischer Stresstests“ zugewiesen: Ich sollte anhand historischer Kursverläufe verschiedener Finanzinstrumente die Auswirkungen einer Reihe bereits eingetretener Stressszenarien, so zum Beispiel die Auswirkungen der Terroranschläge des 11. September 2001, auf die Wertentwicklung dieser Finanzinstrumente quantifizieren. Das bedeutete letztlich, die durchschnittlichen relativen bzw. absoluten Veränderungen über einen passenden szenarienspezifischen Stresszeitraum zu berechnen und deren maximale bzw. minimale Werte ausfindig zu machen. Diese extremen „Shifts“ sollten auf das aktuelle Portfolio des Asset Managers angewendet werden, um schließlich eine Aussage darüber machen zu können, in welcher Größenordnung sich der Verlust bewegen könnte, träte zum aktuellen Zeitpunkt ein ähnliches Stressszenario ein.

Berechnet werden sollten diese extremen durchschnittlichen Veränderungen mittels

Praktikum

eines von mir zu programmierenden VBA-Tools (Microsoft-Office-Programmierung), das schließlich an unseren Kunden für zukünftige Berechnungen übergehen sollte. Dabei wurde mir zunächst eine grobe Idee von den Anforderungen an das Programm gegeben, das es ermöglichen sollte, teils bis in die 1970er Jahre zurückreichende Zeitreihen auf extreme Ausschläge hin zu untersuchen.

Zunächst einmal ging es darum, sich die nötigen VBA-Fertigkeiten anzueignen. Nachdem ich zu Beginn meiner Arbeit noch keinerlei Erfahrung mit der Programmierung von VBA hatte, konnte ich Schritt für Schritt, auch anhand der Hilfe der Kollegen, die nötigen Kenntnisse erwerben. Über die Zeit meines Praktikums hinweg wuchsen durch die Ergebnisse aus fortwährenden Gesprächen mit meinen Betreuern und dem Kunden die Anforderungen an das Tool und so auch dessen Umfang. Zeitgleich stand ich vor der Herausforderung, Zeitreihendaten zu beschaffen, die möglichst weit zurückreichen, um besonders frühe Ereignisse parametrisieren zu können. Mittels verschiedener Informationsdienste, wie z.B. Bloomberg, versuchte ich mir die nötigen Daten zu verschaffen und bekam nebenbei einen Einblick in die Entstehung unserer Finanzmärkte und in das Aufkommen heute gängiger Finanzprodukte.

Gegen Ende meines Praktikums hatte ich schließlich die nötigen Daten gesammelt, das Tool erfüllte die Anforderungen und wir konnten unsere damit errechneten Parameter für die ausgewählten Szenarien in einem Dokument zusammenfassen. Dieses Parameterdokument und das Tool stellten somit einen weiteren Bestandteil der neuen Portfoliobewertungsmethoden des Kunden dar.

Die Arbeitsatmosphäre, die ich während der Projektarbeit und auch bei den Schulungen am Anfang erleben konnte, war durchweg kollegial und offen. Arbeitsweise und Art, Probleme zu diskutieren und lösen, erinnerte dabei stark an den mathematischen Hintergrund der meisten Kollegen. Viele meiner Kollegen befanden sich in ihren ersten Berufsjahren und dies zumeist nach abgeschlossener Promotion. Meine Erfahrung mit den Arbeitszeiten in der Beratung ist, dass diese projektabhängig teils recht ausgedehnt sein können. So sind Arbeitstage mit mehr als zehnstündiger Anwesenheit beim Kunden auch eher Regel denn Seltenheit.

Letztlich kann ich sagen, dass mir die Arbeit während meines Praktikums viel Spaß machte. Es war herausfordernd, ein eigenes Teilprojekt übernehmen zu dürfen und bei dessen Bearbeitung viele Entscheidungen eigenständig treffen zu können. Außerdem motivierte mich zu sehen, wie so manches aus der Finanzmathematik bekannte Bewertungsmodell auch im Rahmen unseres Projekts zur Anwendung kam.

Carolin Bernhofer

Roboter regieren die Welt!

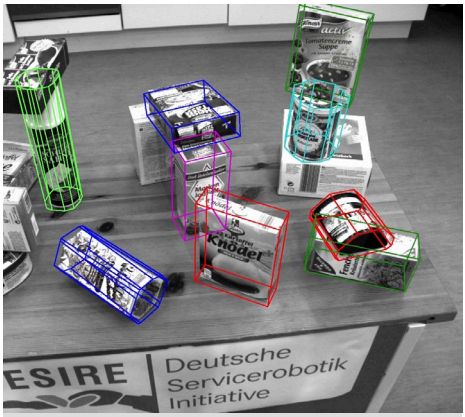
Der Roboter des DESIRE Projekts betrachtet ein komplexes Küchenszenario.

Praktikum

So ein Quatsch, die sind ja viel zu dumm. Das war wohl die erste Lektion, die ich gelernt habe, als ich meine Diplomarbeit im Bereich Robotik bei Siemens begonnen habe.
Die Diplomarbeit bei Siemens zu schreiben bedeutet, dass ich neun Monate in den „Legobau" nach Neuperlach Süd raus fahre und dort meinen Arbeitsplatz bei zwei weiteren Robotikern im Büro habe. Die Arbeitszeiten kommen mir sehr gelegen: Ich darf kommen und gehen, wann ich will.
Dennoch muss ich natürlich fleißig arbeiten, denn wöchentlich gibt es das sogenannte Diplomanden-Seminar. Da stellen mein Mitstreiter, ein Diplomand von der TU Hamburg-Harburg und ich unsere Fortschritte vor. Allerdings ist das keine Präsentation, die einem Magenschmerzen bereiten muss, sondern ein lockeres Zusammentreffen einer kleinen Gruppe aus der Robotik-Abteilung, in der wir einfach erzählen, was wir die letzte Woche so getrieben haben. Dann werden Verbesserungsvorschläge diskutiert, Fragen beantwortet und Anregungen gegeben. Wenn man sich erst mal ans Vortragen gewöhnt hat, eine gute Möglichkeit also um nachzuvollziehen, wo in der Diplomarbeit man sich gerade befindet.
Was mir außerdem gut gefällt, ist die Rundumbetreuung. In der Abteilung sitzen etwa 15 Leute, die sich mehr oder weniger mit dem gleichen Thema auseinandersetzen wie ich, der Objekterkennung bei Robotern. Das heißt, man hat ein echt kompetentes Team von Leuten vor Ort, die sich immer bemühen, mir alle Fragen so gut sie können zu beantworten.
Mathematiker sind unter den Robotikern eher selten anzutreffen. Man findet vielmehr ein buntes Gemisch aus Informatikern, Physikern, Ingenieuren und Elektrotechnikern. Aber genau das bietet die Möglichkeit Einblicke in andere Bereiche und Sichtweisen zu erlangen. Bei so einem komplexen Gebiet, wie der Robotik, müssen sowieso alle eng zusammenarbeiten, um überhaupt Ergebnisse zu erzielen. So intensive Teamarbeit habe ich an der Uni noch nicht erlebt.
Und was ist es jetzt eigentlich, was ich die ganze Zeit dort treibe?
Stell dir vor, du hättest einen Roboter, der

Praktikum

den Auftrag hat, eine bestimmte Schachtel vom Tisch zu holen. Der Roboter weiß, wo der Tisch ist und sieht auch, dass da was drauf ist, jetzt muss er nur noch genau genug erkennen, wo und wie die Schachtel sich auf dem Tisch befindet, um sie greifen zu können.



Den erkannten Objekten wird ein Rahmen zugeordnet, wie und wo der Roboter sie im Raum vermutet.

Also schaut der Roboter durch seine Kameras und macht Messungen mit dem 3D-Sensor, wie zum Beispiel einem Laserscanner. Dann berechnet, oder besser schätzt, er die Lage vom Zielobjekt im sechsdimensionalen Raum. Drei Dimensionen werden für die Translation benötigt – Wo ist die Schachtel? – und drei weitere beschreiben die Rotation – Wie ist die Orientierung des Objekts?

Als Parametrisierung der Pose verwenden wir duale Quaternionen. Die eignen sich gut, weil mit ihnen Rotation und Translation in einem Zug behandelt werden können, sie wenige Parameter haben und flüssige Bewegungen erzeugen. Andere Möglichkeiten wären beispielsweise Rodrigues Vektoren, Euler Winkel oder die Matrixdarstellung.

Leider sind die Messungen, die der Roboter macht, mit vielen Unsicherheiten behaftet, so dass die Objektpose nicht direkt berechnet werden kann. Jedes Gelenk im Roboterkörper ist ein klein bisschen ungenau eingestellt, und die Kamerajustierung ist sicherlich auch nicht perfekt. Es ist produktionsbedingt nicht möglich, alles 100%-ig einzustellen. Außerdem verstellt sich mit jedem Stoß beim Transport wieder irgend etwas. Also behilft man sich bei der Abschätzung der Objektpose mit Wahrscheinlichkeitstheorie. Position und Orientierung werden durch mehrere Gaußkerne modelliert. Zu Anfang sind diese Gaußglocken noch recht breit und flach, doch nach mehr und mehr Messungen (vielleicht von verschiedenen Seiten oder mit anderen Sensoren oder bei hellerem Licht) werden die Verteilungen immer besser gepeakt. Irgendwann ist dann eine Schwelle überschritten, und der Roboter erkennt die Flasche genau genug, um sie greifen zu können, und macht dabei nur noch mit Wahrscheinlichkeit von einem kleinen $\varepsilon>0$ einen Fehler.

Meine Roboter brauchen leider ziemlich lang, um irgendwas zu erkennen. Ein zugeworfenes Objekt aus der Luft zu fangen ist darum bei Weitem noch nicht möglich. Dafür ist immer wieder beeindruckend, wie präzise so ein Roboter bei spezifischen Aufgaben arbeiten kann.

Muriel Lang

Von der Mathematik zur Klimaforschung

Eine ungewöhnliche Karriere

Es war eine schöne Überraschung, nach vielen Jahren eine E-Mail von Heinrich Steinlein zu bekommen, bei dem ich vor Jahr und Tag die Einführung in die Analysis hörte. Es stimmt in der Tat, dass meine Karriere in der Wissenschaft ungewöhnlich verlief – in vieler Hinsicht – und mich zu Themen und an Orte brachte, von denen ich während meines Studiums nur träumte. Der Leitfaden in dieser sehr merkwürdigen Karriere war, immer das zu tun, was mich am meisten reizte und interessierte. Und wenn es einen Ratschlag gibt, den ich Studierenden geben würde, ist es genau das: Auch wenn es nicht das karrieremäßig Logischste ist, es lohnt sich, das zu tun, was einen am meisten interessiert.

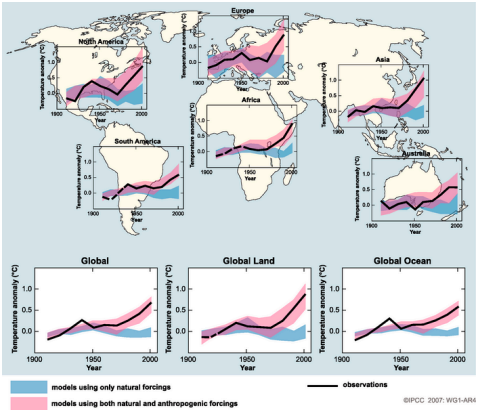
Als ich nach dem Abitur 1980 nach München zum Studium kam, war ich ratlos, wohin ich wollte, und meine Interessen waren breit gestreut. Ich begann zunächst, Vor- und Frühgeschichte zu studieren. Geschichte hatte mich schon immer interessiert, ebenso wie Biologie, Physik (aber da fühlte ich mich, von einem Neusprachlichen Gymnasium kommend, etwas unsicher), und Mathematik machte mir Spaß, aber schien mir doch etwas zu merkwürdig. Allerdings fühlte ich mich mit meinem Studienfach nicht ganz wohl, und nach der Weihnachtspause im ersten Semester war ich auf der Suche nach einem geeigneteren Fach. Nach etwas Herumhören traf ich einen Schulfreund, der an der TU Mathematik studierte – und ich hörte mir eine Vorlesung an, und fand, das sei ja doch deutlich interessanter als in der Schule. Und so fand ich mich plötzlich in den Semesterferien dabei, das erste Semester nachzulernen, um ins 2. Semester in der Mathematik einsteigen zu können. Das wollte ich unbedingt, schon um den Stimmen in meiner Familie, die mir dringend von der Vor- und Frühgeschichte abgeraten hatten, auf keinen Fall recht zu geben. Und tatsächlich machte mir die Mathematik Spaß, und ich kam gut damit klar. Die Experimentalphysik war dagegen immer wieder eine Herausforderung, vor allem wenn es um Elektronen und magnetische Felder ging ..., aber machte mir auch viel Spaß, besonders die Thermodynamik. Während des Studiums fand ich partielle Differentialgleichungen am interessantesten. Ich fand es faszinierend, wie physikalische Prozesse sich durch wenige Zeilen von Gleichungen mit Randbedingungen beschreiben lassen und wie man wiederum Gesetzmäßigkeiten und Eigenschaften dieser Prozesse aus den Gleichungen herauslesen und ableiten konnte. Andererseits fand ich auch Numerische Mathematik interessant, und sie schien mir anwendbar und nützlich. Und so fand ich mich einerseits in einer langen Reihe von Spezialvorlesungen von Professor Wienholtz wieder, die mir unvergesslich sind. Und andererseits bei Prof. Sachs in der Numerik. In dessen Vorlesung wurden eines schönen Tages Bilder aus der numerischen Strömungsmechanik gezeigt. Das sah nun unglaublich interessant aus, und ich konnte ihn nach einigem Überreden überzeugen, mir ein Diplomarbeitsthema und später ein Dissertationsthema in diesem Bereich zu geben. Das Thema wurde vom Sprachverarbeitungslabor der Firma Siemens gefördert, die hofften, mit Hilfe eines Modells der Strömung und Schallausbreitung im Sprachtrakt ihre Sprachsynthese verbessern zu können. Und so trat ich den Spagat an zwischen der Mathematik und ihrer Anwendung, was nicht immer ganz trivial war. Als Entspannung war da das Bergsteigen und Skitourengehen wunderbar, mit Studienfreun-

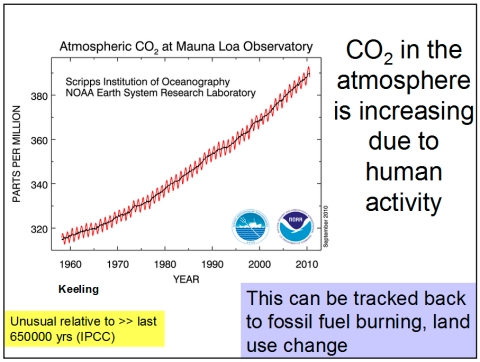
Der Franz-Josef-Gletscher auf der Südinsel Neuseelands

den aus der Mathematik. Wir liehen uns Karten vom Alpenverein aus und erkundeten die Gletscher in Sommer und Winter. Die Karten waren oft mehrere Jahre alt, und wir fanden die Gletscher meistens weiter oben als in der Karte eingezeichnet und wunderten uns. In der populärwissenschaftlichen Literatur tauchten damals die ersten Artikel zur Klimaänderung und zum nuklearen Winter auf, was mich sehr interessierte.

Nach meiner Dissertation war die große und schwierige Frage: was nun? Ich bewarb mich in der Industrie, z. B. Unternehmensberatung, Rentenrücklagenberechnung, Versicherungen. Allerdings hatte ich auch davon gehört, dass es in Hamburg ein Institut gäbe, an dem Klimamodelle entwickelt würden. Das Thema schien mir eine faszinierende und komplizierte Anwendung numerischer Strömungsmechanik zu sein, und so bewarb ich mich ins Blaue hinein, und nicht ganz im Ernst. Ich war sehr erstaunt, als ich einen Anruf von Hans von Storch bekam mit der Frage, ob ich denn eine akademische Karriere im Sinne hätte? Da war ich mir ja gar nicht sicher, aber zum Vorstellungsgespräch ließ ich mich doch gern einladen. Nach schlafloser Nacht (in der ich mir immer wieder sagte, das sei doch das Verrückteste, was man machen könnte) fuhr ich nach Hamburg und stellte mich bei Klaus Hasselmann und Hans von Storch am Max-Planck-Institut für Meteorologie vor. Ich war von der Atmosphäre am Institut, den spannenden Fragen, den tollen internationalen Kontakten und Reisen und den imponierenden Kollegen so eingenommen, dass ich zusagte. Und damit eine befristete Stelle weit von München besser bezahlten Dauerstellen in der Industrie vorzog. Und das, obgleich klar war, dass die Modellierthemen besetzt waren und ich mit Modell- und Beobachtungsvergleichen beschäftigt sein würde. Ein Thema, an dem ich nun, 20 Jahre später, immer noch sitze, und das immer noch seine Reize hat: Die Beobachtungen sind die „ground truth“, das einzige, was uns sagen kann, ob das Modell denn etwas taugt. Andererseits

Obersulzbachkees am Großvenediger. Vor wenigen Jahren bedeckte der Gletscher noch die ganze Seefläche. (Bild: Martin Steinlein)





Links: Vergleich der beobachteten Änderung (über 10 Jahre gemittelt) der Oberflächentemperatur über Kontinenten (schwarze Linie, Änderung relativ zur Mitteltemperatur 1900-1950) zum 5-95% Range von Modellsimulationen des 20.Jahrhunderts, die mit natürlichen und anthropogenen Strahlungsantrieb (rot) und nur mit natürlichen Änderungen (blau) angetrieben wurden; Figur aus dem IPCC Bericht, WG I, siehe www.ipcc.ch.

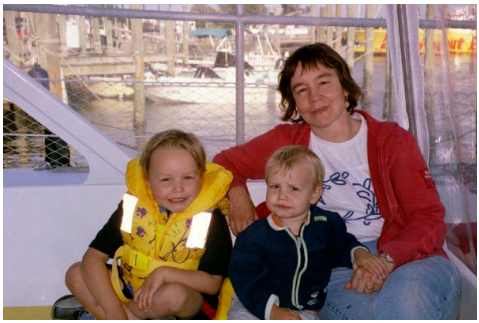
Rechts: Die Änderung in der atmosphärischen Kohlendioxid-Konzentration; Daten vom Mauna Loa Observatory, Keeling.

sind die Beobachtungen auch von Unsicherheiten umgeben, Messfehler, Punkte in Raum und Zeit, die sich mit dem Modell nicht so einfach vergleichen lassen. Dazu kommt, dass Klima von vielen Variablen in 4 Dimensionen beschrieben wird und man in diesem Sumpf von Daten leicht ersticken kann. Klaus Hasselmanns Fingerprint Methode zeigte, wie man in diesem Datenwald nach dem Signal der Anthropogenen Klimaänderung suchen könnte. Man wählt einen Fingerprint in Raum und Zeit aus der Modellvorhersage und projiziert die Beobachtungen darauf. Wenn man eine geeignete Metrik wählt, ist das Verhältnis dieses Klimasignals zum Klimarauschen (der Variabilität, die das Klimasystem ständig durch Chaos erzeugt) optimal, und damit die Chance erhöht, das Signal der Klimaänderung zu finden. Damit beschäftigte ich mich in meinen fünf wunderbaren Jahren am MPI. Wir fanden das Klimasignal und zeigten, dass das geographische Muster der 30- und 50-jährigen Trends in der Oberflächentemperatur der Erde das Muster der Klimaänderung zeigt, das aus Modellläufen erwartet wird. Und dass ein derzeitiges Muster in dieser Stärke weder mit natürlicher Variabilität noch mit Änderungen der Sonneneinstrahlung erklärt werden kann. Nebenher arbeitete ich mit den Modellierern, z. B. Ulrich Cubasch (der nun Professor an der FU Berlin ist), an der Auswertung und Publikation der Modellläufe. Klaus Hasselmann und Hans von Storch waren in der Zeit wunderbare Mentoren. Ich glaube, es ist kein Zufall, dass vor allem Hans, der auch Mathematiker ist, und ich uns wissenschaftlich hervorragend verstanden. Klaus lehrte mich das Publizieren (Schreiben war ja nicht ganz meine Stärke) und war mir ein großes Vorbild. Seine wissenschaftlichen Ideen, zum Beispiel zur Ursache der langfristigen Klimavariabilität in der Interaktion des langsam reagierenden Ozeans mit kurzfristiger Wettervariabilität der Atmosphäre haben mich meine Karriere hindurch beeinflusst.

Nach 5 Jahren dann wieder die Frage: was nun? Ich hatte mittlerweile während eines zweimonatigen Aufenthalts in Texas einen Amerikaner kennengelernt, und von daher waren die USA mein nächstes Ziel. Es war wirklich ein großes Glück, ein Feodor Lynen-Stipendium der Alexander von Humboldt-Stiftung an Land zu ziehen, mit dem ich für 2 Jahre nach Seattle

zur University of Washington gehen konnte, um mehr über Klimadynamik zu lernen. Damit hat sich für mich die Klimavariabilität von „Rauschen" zu einem interessanten Forschungsthema entwickelt, und ich lernte mehr und mehr über die Atmosphäre, das Klimasystem und die Beobachtungen.

Eine persönliche Herausforderung in den nächsten Jahren war für mich, Wissenschaft und Ehe und Familie irgendwie zu vereinbaren. Es war nicht leicht. Mein Mann war bei Texas A&M Projektwissenschaftler und später Professor, und nachdem das mit der Fernehe (Seattle ist sehr weit von Texas) und dem Kinderwunsch sich nicht unter einen Hut bringen ließ, ging ich nach Texas auf eine Projektstelle und dann später gemeinsam mit meinem Mann an die Duke University in North Carolina. In den USA kann man an einer Universität so lange als Projektwissenschaftler(in) arbeiten, wie man Mittel an Land ziehen kann. Dieser Lebensstil ist einerseits sehr frei, man kann sich die Forschungsthemen, Projektpartner und Schwerpunkte frei wählen, aber natürlich hängt immer das Damoklesschwert über einem, dass alle Projekte irgendwann zu Ende sind und neue eingeworben werden müssen. Gottlob gelang mir dies über 10 Jahre immer wieder. Ich war in dieser Zeit immer wieder frustriert und wünschte mir mehr Dauerperspektive. Heute sehe ich, dass diese Flexibilität mir auch sehr geholfen hat. In der Zeit habe ich zwei Kinder bekommen, und war auf 50%, dann auf 75% und 80% Teilzeit. Und so habe ich in diesen 10 Jahren meine Forschungsthemen verfolgt und mich um meine Kinder gekümmert, ohne Lehre und mit Komiteearbeit nur in Bereichen, die mich auch interessierten. Ein Komitee, das mich interessierte, war das Intergovernmental Panel on Climate Change (IPCC), ein Komitee der UN und der World Meteorological Organization, das alle paar Jahre einen umfangreichen Bericht zur Klimaänderung verfasst. Ich habe an den letzten 3 Berichten mitgeschrieben, im letzten als Hauptautorin des Kapitels zu den Ursachen des Klimawandels im Teil 1 des Berichts (The Physical Science Basis). Die präzise und objektive Beschreibung der wissenschaftlichen Erkenntnisse und ihrer Unsicherheiten für diesen Bericht hat viel Spaß gemacht. Ich war auch im Team, das die Kurzzusammenfassung für Politiker entworfen hat. Es war interessant, aus einem wissenschaftlichen Bericht von vielen Hundert Seiten die wesentlichsten und robustesten Ergebnisse für diese Kurzzusammenfassung herauszuarbeiten.



2007 wollte ich nun wirklich eine Dauerstelle, und so ging ich auf Bewerbungstour. Die University of Edinburgh machte mir ein Angebot, auf das ich nach einigem Nachdenken einging. Ganz nach Deutschland zurück wäre meinem amerikanischen Ehemann schwer gefallen, aber es war nett, wieder in Europa zu sein. Die Anpassung an Schottland ist meinen Jungs nicht leicht gefallen, aber ich denke, es hat sich gelohnt. Edinburgh hat mich sehr gut behandelt, nach 2 Jahren wurde ich zum Professor befördert. Die Triangulierung von Forschung, Lehre und Familie ist mir immer noch eine Herausforderung. Verbringe ich genug Zeit mit meinen Jungs? Ist meine Lehre gut genug,

lernen die Studierenden Nützliches? Bekommt meine Forschungsgruppe genug Anstöße von mir? Es wird nicht langweilig, und oft wünsche ich mir, der Tag hätte 48 Stunden!
In der Klimaforschung, die ein sehr junger Wissenschaftszweig ist, sind neben Meteorologen und Ozeanographen viele Mathematiker und Statistiker tätig, auch Physiker und Chemiker. Es ist nicht nur die mathematische Denkweise, die gebraucht wird. Auch viele Techniken sind mathematisch orientiert, und logisches und statistisches Denken sind notwendig. In den letzten Jahren schließt sich für mich der Kreis zur Vor- und Frühgeschichte: Meine Forschung beschäftigt sich zunehmend mit der Rekon-struktion und Interpretation des Klimas der Vergangenheit, z. B. im Holozän, und beantwortet zum Beispiel die Frage, womit sich die kalten Winter im späten 17. und frühen 19. Jahrhundert erklären lassen, und wieweit man aus dem Klima der letzten Eiszeit und des letzten Millenniums lernen kann, wie stark das Klimasystem auf Änderungen in der globalen Strahlungsbilanz reagiert. Wenn man das weiß, kann man auch genauer und robuster vorhersagen, wieviel Erwärmung auf ein weiteres Ansteigen der Kohlendioxid-Konzentration folgen wird ...

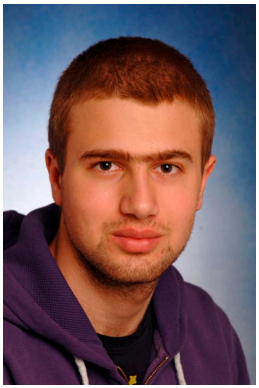
Gabi Hegerl

Praktikum am Mathematischen Institut

In vielen Gymnasien Bayerns steht in der 9., 10. oder 11. Jahrgangsstufe ein meist einwöchiges Betriebspraktikum auf dem Stundenplan. Dessen Zielsetzung ist es, den Schülerinnen und Schülern durch praktische Erfahrungen erste Einblicke in die Berufswelt zu gewähren und eine Entscheidungshilfe für die spätere Studien- und Berufswahl zu geben. Dabei besteht die Möglichkeit, das Praktikum auch an einer staatlichen Einrichtung wie dem Mathematischen Institut der LMU zu absolvieren. Die Praktikantinnen und Praktikanten lernen dabei Struktur und organisatorischen Ablauf im Institut kennen, werden – soweit möglich – in die Arbeitsprozesse mit einbezogen und kommen dabei natürlich auch in Berührung mit der universitären Mathematik.
Der nachstehende Bericht von Herrn Rami Daknama, einem unserer Praktikanten des letzten Jahres, vermittelt einen Eindruck von einem möglichen Verlauf eines solchen Praktikums. Da die Anzahl der Praktikumsplätze, die das Institut im Jahr einrichten kann, naturgemäß beschränkt ist, sollten sich interessierte Schülerinnen und Schüler rechtzeitig am besten per mail (rost@math.lmu.de) mit Herrn Prof. Dr. Daniel Rost in Verbindung setzen.

Praktikumsbericht von Herrn Rami Daknama

Im Zeitraum vom 19. bis 28. Juli 2010 absolvierte ich ein Praktikum am Mathematischen Institut der Ludwig-Maximilians-Universität München. Zu dieser Zeit besuchte ich die 11. Klasse des Wittelsbacher-Gymnasiums München. Im Rahmen des Berufs- und Studienorientierungsangebots unserer Schule hatte jeder Schüler die Möglichkeit, ein achttägiges Praktikum abzuleisten. Da ich mich sehr für Mathematik interessiere und plane, Finanzmathematik zu studieren, bewarb ich mich für ein Praktikum beim Mathematischen



Institut, da ich dort bereits sehr positive Erfahrungen bei einem äußerst informativen und ausführlichen Beratungsgespräch mit Herrn Dr. Schörner bezüglich des Aufbaus und der Möglichkeiten eines Mathematikstudiums gemacht hatte.

Das Praktikum begann am 19. Juli 2010. Nachdem ich um 9.30 Uhr in der Theresienstraße im Mathematischen Institut angekommen bin und Herrn Prof. Dr. Rost kennengelernt habe, mit dem ich zuvor lediglich über E-Mail in Kontakt stand, zeigt dieser mir das Gebäude und erklärt mir die Struktur und den Aufbau des Instituts. Auf einer großen Schautafel sehe ich, welche Lehrstühle es gibt und welcher Professor zu welchem Lehrstuhl gehört. Anschließend erhalte ich einen Plan, auf dem alle Vorlesungen der Woche aufgelistet sind. Ich darf an jeder Vorlesung meiner Wahl teilnehmen. Anschließend treffe ich auch Herrn Dr. Schörner, der mich in den nächsten Tagen zusammen mit Herrn Prof. Dr. Rost betreuen wird.

Gegen Ende des ersten Praktikumstags arbeite ich mich mit Hilfe von Lehrbüchern in die Programmiersprache „HTML“ ein, mit der Homepages erstellt werden können.

In den folgenden Tagen ist es meine Aufgabe, die Homepage des Fördervereins mitzugestalten: Ich lade Bilder der Absolventen des letzten Jahres auf die Homepage hoch, verlinke diese und sortiere sie nach Namen. Dabei lerne ich die Grundprinzipien des Programmierens kennen und sehe die Ergebnisse auch sofort auf der Homepage des Fördervereins des Mathematischen Instituts.

Weitere Aufgaben sind beispielsweise die Auswertung von Vorlesungsumfragen und die Erfassung der Bewerbungen von Studierenden für die begehrten Korrektor- und Tutorplätze. Dabei habe ich die Möglichkeit, mich mit dem in der Mathematik hauptsächlich verwendeten Textverarbeitungsprogramm „LaTeX“ vertraut zu machen, mit dem ich dann die gewünschte Übersichtstabelle erstelle.

Die Vorlesungen, die ich besuche, sind alle sehr interessant. Natürlich fehlt zum genaueren Verständnis noch das Vorwissen; auf jeden Fall ist es sehr spannend, einen Einblick ins „Studentenleben“ zu bekommen. Das Praktikum lässt klar erkennen, wie allgegenwärtig die Mathematik in unserer Welt ist. Besonders interessant finde ich den Teilbereich der Wirtschafts- und Finanzmathematik, von dem ich mir auch mehrere Vorlesungen anhöre.

Insgesamt hat das Praktikum sehr viel Spaß gemacht und einen guten Einblick in das Leben und Arbeiten an einer Universität gegeben. Der Gesamteindruck ist sehr positiv und bestärkt mich darin, an der LMU Wirtschafts- und Finanzmathematik studieren zu wollen. Nach dem Studium an einer Universität zu arbeiten, ist wohl auch eine interessante Möglichkeit.

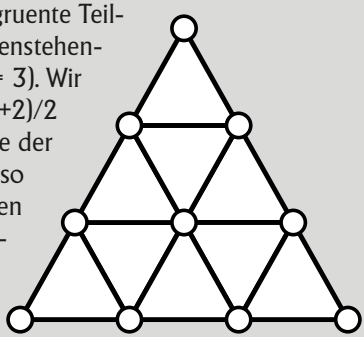
Besonders gefallen hat mir, mit welcher Geduld, Hilfsbereitschaft und Freundlichkeit Herr Prof. Dr. Rost und Herr Dr. Schörner mir stets halfen, mir etwas erklärten oder mir etwas zeigten.

Ein Praktikum am Mathematischen Institut der LMU München zu machen, kann ich jedem empfehlen, der an einem Mathematikstudium interessiert ist oder sich damit näher auseinandersetzen will.

Rami Daknama

Rätselecke

Ein Dreieck werde durch Parallelen zu den Dreiecksseiten in n^2 kongruente Teildreiecke zerlegt (vgl. nebenstehende Skizze für den Fall $n = 3$). Wir wollen jedem der $(n+1)(n+2)/2$ Geradenschnittpunkte eine der Zahlen $1,\ldots,n+1$ zuordnen, so dass auf keiner der $3n$ Geraden die gleiche Zahl mehrfach vergeben wird. Man zeige, dass dies für $n = 2,4,6,\ldots$ stets möglich ist und auch für $n = 5$, nicht jedoch für $n = 3$.



Die Seitenflächen eines Würfels seien in vier gleiche Teilquadrate unterteilt, die wir jeweils in einer der Farben Blau, Gelb oder Rot einfärben wollen. Wir wollen dabei wie folgt vorgehen: Wir geben bei drei Teilquadraten die Farbe vor und färben anschließend sukzessive diejenigen Teilquadrate ein, deren Farbe durch die Vorschrift, dass nie Teilquadrate mit gemeinsamer Kante gleich gefärbt sein dürfen, eindeutig bestimmt ist (vgl. die erste Aufgabe der Rätselecke von Heft 20). Zeige, dass so mit geeigneter Vorgabe maximal weitere 11 Teilquadrate eingefärbt werden können.

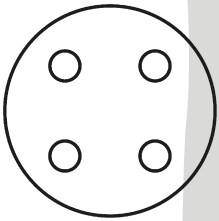
Max hat ein kleinkariertes DIN A4-Blatt (Gitterabstand 0,5 cm) und möchte Orthogonalprojektionen von Würfeln zeichnen, so dass

a) jeder Eckpunkt auf einen Gitterpunkt fällt,
b) alle Seitenflächen als (nichtausgeartete) Parallelogramme erscheinen, aber nicht als Rauten, und
c) vier der Würfelkanten vertikale Linien ergeben.

Gibt es überhaupt solche Würfelprojektionen, und wenn ja, wie viele (wobei wir bei Projektionen, die durch Spiegelungen oder Verschiebung ineinander übergeführt werden können, keinen Unterschied machen)?

Lösungen zu den Rätseln von Ausgabe 22

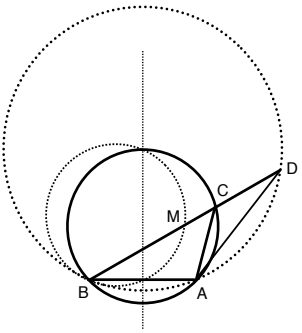
Schloss *Um Schneewittchen in ihrem Kristallsarg zu schützen, haben die sieben Zwerge ein eigenartiges Schloss gebaut: Es hat vier Öffnungen, in die man nicht reinsehen kann; man kann aber in zwei beliebige Öffnungen gleichzeitig beide Hände einführen und den sich in jeder Öffnung befindenden Türgriff horizontal oder vertikal stellen; zieht man die Hände aus den Öffnungen, so dreht sich das Schloss so schnell, bevor es stehen bleibt, dass es dem Beobachter unmöglich wird, die neue Position des Schlosses zu bestimmen. Die Tür öffnet sich, wenn alle Türgriffe entweder horizontal oder vertikal gestellt sind.*
Wird es dem Prinz gelingen, die Tür in einer endlichen Zeit zu öffnen und die Prinzessin zu retten?



Der Prinz kann in maximal fünf Schritten das Schloss öffnen:

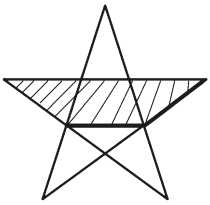
1. Er greift zunächst in zwei diagonal gegenüberliegende Öffnungen. Wenn die Griffe in gleicher Stellung sind, dreht er beide, anderenfalls nur einen. Wenn sich die Tür nicht öffnet, kann er im ersten Fall den nächsten Schritt überspringen, im zweiten Fall
2. greift er wieder in zwei diagonal gegenüberliegende Öffnungen und dreht beide Griffe. Wenn sich die Tür wieder nicht öffnet, weiß er, dass die beiden anderen Griffe in verschiedener Stellung sind.
3. Er greift wieder in diagonal gegenüberliegende Öffnungen und dreht nur einen Griff. Waren die Griffe in unterschiedlicher Stellung und öffnet sich die Tür nicht, so kann er den nächsten Schritt überspringen. In anderen Falle hat er nun zwei nebeneinanderliegende Paare von Griffen in gleicher Stellung.
4. Jetzt greift er in zwei nebeneinanderliegende Öffnungen und dreht beide Griffe. Wenn sich die Tür nicht öffnet, hat er nun zwei Paare diagonal gegenüberliegender Griffe in gleicher Stellung.
5. Mit Drehen der Griffe eines diagonalen Paares öffnet sich die Tür.

Mitte *Wähle auf dem Kreisumfang zwei verschiedene Punkte A und B. Für beliebige Punkte C der Kreislinie sei M die Mitte der gebrochenen Linie ACB. Finde die Menge aller dieser Punkte M.*



Die gesuchte Menge ist eine Figur 8 mit dem Kreuzungspunkt genau in der Mitte zwischen A und B, die sich aus vier Kreisbogenstücken zusammensetzt. Wir beschreiben dies anhand eines dieser Bogenstücke:
Sei BC länger als AC. Verlängere BC um die Länge von AC bis zum Punkt D. Im Dreieck ACD ist $\sphericalangle CAD = \sphericalangle CDA$ und $\sphericalangle CAD + \sphericalangle CDA = \sphericalangle ACB$, d. h. $\sphericalangle CDA = 1/2\ \sphericalangle ACB$. Folglich ändert sich $\sphericalangle CDA$ nicht, wenn sich der Punkt C auf der Kreislinie bewegt, und D bewegt sich dann auf einer Kreislinie, die durch die Punkte A und B geht. Somit liegt der Punkt M auf einer Kreislinie mit halbem Radius, die durch den Punkt B, die Mitte der Strecke AB und den Mittelpunkt des Kreisbogens zwischen A und B, auf dem C liegt, geht.

Stern *Zeige, dass die schraffierte Fläche und die nichtschraffierte Fläche des Sterns gleich groß sind.*



Natürlich genügt es zu zeigen, dass die Fläche des mittleren schraffierten Trapezes gleich der Summe der Flächen der angrenzenden darüber- und darunterliegenden Dreiecke ist. Teilt man dieses Trapez mittels einer Geraden in zwei Dreiecke, so ist das eine kongruent zum darunterliegenden (stumpfwinkligen) Dreieck, das andere bildet mit der angrenzenden Spitze eine Raute, hat also die gleiche Fläche wie alle Sternspitzen.

Die Haribo-Fragen oder wer ist Thomas Gottwald?

Dr. Hans Riegel-Stiftung

Im Oktober letzten Jahres erfuhr ich, dass unser Institut mit etwas Glück die Dr. Hans Riegel-Fachpreise vergeben darf. Natürlich stellten sich mir als voraussichtlichem Mitorganisator sofort mehrere Fragen. Bis zum Abschluss des Projektes kamen noch einige hinzu:

Wer ist Dr. Hans Riegel? Dr. Hans Riegel ist Mitinhaber der Firma Haribo. Nach dem Studium der VWL promovierte er zu seiner Firma

passend über das Thema *„Die Entwicklung der Weltzuckerwirtschaft während und nach dem zweiten Weltkrieg"*.[i] 1987 gründet er die nach ihm benannte Stiftung. Wegen seines sozialen Engagements wurde er 1993 mit dem Verdienstkreuz Erster Klasse ausgezeichnet.[ii] Unsere französischen Freunde haben Dr. Hans Riegel zum Ritter der Ehrenlegion ernannt.[iii]

Was ist das Ziel der Dr. Hans Riegel-Stiftung? Das Ziel der Stiftung ist es, junge Menschen zu ermutigen, zu fördern, zu beflügeln und so junge Talente für die Zukunft stark zu machen.[iv] Das kann natürlich alles und nichts heißen. Aber konkret sollen u. a.

durch die Fachpreise junge Talente im mathematisch-naturwissenschaftlichen Bereich gefördert werden und frühzeitig mit Hochschulen und den entsprechenden Fördermöglichkeiten in Kontakt kommen. Außerdem wird durch diesen Wettbewerb der Austausch zwischen den Bildungsträgern Schule und Universität unterstützt und so eine bessere Begabtenförderung erreicht.[v]

Die für die Universität zentrale Frage ist: **Warum bietet sich die Kooperation der LMU und der Dr. Hans Riegel-Stiftung an?** Seit 2007 können Schüler im Rhein-Sieg-Kreis ihre Facharbeiten an der Uni Bonn einreichen. Diese werden dann von Wissenschaftlern der jeweiligen Institute begutachtet und die besten drei werden von der Stiftung mit Geldpreisen in Höhe von 600, 400, 200 € prämiert. Durch die positiven Erfahrungen ermuntert wollte die Stiftung 2010 im gesamten deutschsprachigen Raum zusammen mit mehreren Universitäten lokal Fachpreise ausloben. Für Oberbayern bot sich natürlich die Münchner Universität an. Insbesondere das Mathematische Institut der LMU versucht seit einiger Zeit mit verschiedenen Angeboten auf Schüler zuzugehen. Die Fachpreise ergänzten diese schon vorhandenen Maßnahmen hervorragend. So gesehen ist die Kooperation nur natürlich.

[i] Quelle: http://www.hans-riegel-stiftung.de/core/deDE/stiftung/gruender/lehrjahre.php

[ii] Quelle: http://www.hans-riegel-stiftung.de/core/deDE/stiftung/gruender/anerkennungauszeichnungen.php

[iii] Quelle: http://de.wikipedia.org/wiki/Hans_Riegel_junior

[iv] Quelle: http://www.hans-riegel-stiftung.de/core/deDE/ziel/index.php

[v] Quelle: http://www.hans-riegel-stiftung.de/core/deDE/fachpreise/wettbewerb.php

Ein Team unseres Instituts bestehend aus Prof. Schottenloher und drei Assistenten (Andreas Fackler, Lukas Moser und mir) übernahm die Organisation des Wettbewerbs. Sehr schnell stellte sich die Frage: **Wie sollen wir den Wettbewerb bloß organisieren?** Routiniert strukturierte Herr Schottenloher die Aufgabenbereiche und sorgte dafür, dass unser Viererteam keine Aufgabe vergaß. Hierbei übernahm er die Ausführung von einigen Aufgaben selbst. Somit schickten wir unzählige Poster und tausende Flyer an alle Gymnasien von Oberbayern. Weiterhin gelang es uns durch persönliche Kontakte eine Vielzahl von engagierten Mathematiklehrern auf den Wettbewerb aufmerksam zu machen.

Trotz unserer aufwändigen Werbemaßnahmen fragten wir uns: **Wird das auch nur einen Schüler interessieren?** Dies wurde relativ schnell eindeutig geklärt, da immer mehr Facharbeiten bei uns ankamen. Die Frage wandelte sich also aus Gründen des Selbstschutzes zu „Wird das nicht zu viele Schüler interessieren"? Am Ende hatten weit über 150 Schüler ihre Facharbeiten in den Bereichen Erdkunde und Mathematik eingereicht. Der Großteil war zu unserer Überraschung aus dem Fach Mathematik. Wir benötigten also tatkräftige Hilfe bei der Begutachtung. Diese fanden wir in den Diplomandinnen Felizitas Weidner und Katharina Jochemko, ohne deren Hilfe wir mehrfach gescheitert wären!

Nach mehreren Runden sorgfältiger Begutachtungen waren immer noch so viele Facharbeiten in der engeren Wahl, dass uns die Frage **„wer gewonnen hat"** (besser gesagt: „wer hat nicht gewonnen") nicht leicht fiel. Aus diesem Grund vergaben wir dann auch noch sieben mit Buchpreisen dotierte vierte Plätze pro Fach. Verdient erhielt Frau **Karin Zacherl** für ihre Arbeit **„Tischtennis – Mathematische Analyse"** den ersten Platz in Mathematik. Lukas Moser hat in seiner Rede bei der Preisverleihung die Arbeit folgendermaßen beschrieben: *„Vor einigen Jahren wurden im Tischtennis die Regeln geändert. Sätze gewinnt man nun nicht mehr mit 21, sondern bereits mit 11 Punkten; dafür muss man aber zum Sieg in einer Partie drei statt wie bisher zwei Sätze gewinnen. Wie wirkt sich diese Änderung jetzt auf die Gewinnchancen beider Spieler aus? Und dauert eine Partie nach den neuen Regeln eigentlich genauso lange wie vorher? Ich verrate die Antwort, zu der Frau Zacherl durch eine methodisch mustergültige mathematische Analyse gelangt: nach den neuen Regeln ist es etwas leichter geworden, gegen einen überlegenen Spieler einen Satz zu gewinnen; die*

Chance auf den Gewinn einer Partie ist aber kaum verändert. Außerdem ist die zu erwartende Dauer einer Partie um etwa 10 Prozent gesunken. Als Zuckerl zeigt Frau Zacherl noch, dass die häufig geäußerte These: „Wer erst einmal 4:0 in Führung liegt, gewinnt den Satz fast sicher!" tatsächlich stimmt, und überprüft (vorbildlicherweise!) ihre theoretischen Resultate anhand von umfangreichem Datenmaterial aus Tischtennis-Vereinsarchiven." Auch die Beurteilung der Arbeit kann ich nicht treffender formulieren als Lukas dies getan hat: *„Die gesamte Arbeit ist ein glänzendes Beispiel dafür, wie man mit Hilfe einer sinnvollen Modellierung und geschickter mathematischer Analyse realistische Fragestellungen umfassend untersuchen und beantworten kann. Die mathematische Argumentation ist souverän und durchsichtig, die Darstellung stets verständlich und konzis. Frau Zacherl zeigt auch, welche komplexen Probleme mit nicht viel mehr als den Mathematikkenntnissen der Oberstufe lösbar sind, wenn man sie so geschickt und sorgfältig anwendet wie sie. Diese ganz eigenständige Forschungsarbeit ist eine beeindruckende Leistung, die Frau Zacherl zur Siegerin des diesjährigen Dr. Hans Riegel-Fachpreises in Mathematik macht. Herzlichen Glückwunsch!"*

Nachdem die Sieger festgelegt waren, war die Organisation einer Preisverleihung der nächste logische Schritt. Als Moderator wurde von der Seite der Stiftung Thomas Gottschalk ins Spiel gebracht. Dazu fragten wir uns natürlich: **Meinen die wirklich *den* Gottschalk?** Sie meinten tatsächlich den eloquenten, extrovertierten, telegenen, schillernden und lockeren (ehemals blonden) Moderator von „Wetten, dass ..?", der auch die Werbefigur der Firma Haribo ist. Zusammengefasst das genaue Gegenteil des Stereotyps eines Mathematikers, bis auf den Hang zu gewagter, unpassender Kleidung. Somit alles, was uns auf der Preisverleihung fehlte. Perfekt. Auch konnten wir mit Herrn Schottenloher auf einen Mathematiker zurückgreifen, der nicht sofort neben Thomas Gottschalk im Hintergrund verschwindet.

Nur die Preise zu verleihen, war uns einfach zu wenig und wäre unserem schönen

Institut nicht gerecht geworden. **Wie sollte also die Preisverleihung ablaufen?** Wir überlegten uns, dass die Veranstaltung mit populär-wissenschaftlichen Vorträgen anfangen sollte. Danach sollte es ein Buffet im Senatssaal geben und anschließend die Preisverleihung, moderiert von Herrn Gottschalk. Durch die gesamte Veranstaltung sollte Prof. Dr. Schottenloher führen. Diese sollte nicht irgendwo, sondern am besten in der großen Aula stattfinden, beginnend mit einem Grußwort unseres Vizepräsident Prof. Dr. Reinhard Putz. Alles in allem eine nette kleine (etwas größenwahnsinnige) Programmplanung. Dass die Umsetzung klappte, ist mir immer noch unbegreiflich. Wir bekamen trotz der kurzfristigen Anfrage sogar alle nötigen Räume, allerdings erst nachdem uns die zentrale Hörsaalvergabe beinahe einen Kopf kürzer gemacht hatte. Prof. Dr. Frank Schröder sagte zu, einen Geographie-Vortrag über *„Die Glokalisierung auf unseren Tellern“* zu übernehmen. Hierzu sollte ich vielleicht anmerken, dass Glokalisierung kein Rechtschreibfehler, sondern ein Kunstwort bzw. eine Mischung aus Globalisierung und Lokalisierung ist. Für die Mathematik erklärt sich dankenswerterweise Prof. Dr. Francesca Biagini bereit einen Vortrag über *„Money out of nothing? Prinzipien und Grundlagen der Finanzmathematik“* zu halten. Auch erhielten wir wieder tatkräftige Hilfe durch die Studenten Felizitas Weidner, Karolina Vocke und Thomas Schacherer.
Es war also soweit alles wunderbar geplant, aber genau deswegen stellten wir uns die Frage **„Was kann hier alles schiefgehen?“** Wir befürchteten kein Publikum, keine Schüler und somit einen leeren Saal, vor dem Thomas Gottschalk zu Recht nicht auftreten würde. Besonders, da Kaiserwetter prognostiziert war und auch noch am Tag zuvor viele Abifeiern stattfanden. Im Nachhinein betrachtet ist erstaunlich wenig schiefgegangen. Es hatte sich sogar ein beträchtliches Publikum und etwas Presse versammelt. Auf der Veranstaltung ist auch eine kleine Anekdote entstanden, als Herr Gottschalk auf der Bühne als Herr Gottwald angekündigt wurde. Dies nahm Herr „Gottwald“ übrigens mit professionellem Humor und revanchierte sich kurz darauf schlagfertig. Seine Moderation war mustergültig. Zuerst fand er ein paar bemerkenswert ernste Worte zur (mangelnden) Bereitschaft in unserer Gesellschaft sich anzustrengen und

Peter Laffin und Dr. Reinhard Schneider von der Dr. Hans Riegel-Stiftung

durch dringend benötigte Spitzenleistung (auch in der Forschung) zu brillieren. Danach interviewte er gekonnt die Preisträger über Ihre Facharbeiten. Hierbei gelang es ihm eine lockere Atmosphäre zu schaffen, so dass die Preisträger das Publikum vergaßen. Auch in der lokalen Presse wurde die Preisverleihung erwähnt, allerdings wurde hier leider mehr die Geographie in den Vordergrund gestellt. Ein Indiz, dass sich der Ruf der Mathematik trotz aller Anstrengungen (z. B. Jahr der Mathematik) noch nicht genug verbessert hat.

Abschließend stellt sich die Frage **„Wie sieht die Zukunft der Fachpreise aus?“**. Die Organisation wird von einer professionellen Fachkraft des Präsidiums und die Begutachtung wird wohl wieder von Freiwilligen der Institute übernommen. Thomas Gottschalk hat signalisiert, dass er sich gerne wieder für die Forschung und vor allem für seine alte Universität, LMU, Zeit nehmen würde. Zusätzlich werden ab nächstem Jahr auch in der Biologie, der Chemie und der Physik jeweils Preisgelder in Höhe von 600 €, 400 € und 200 € vergeben. Da die Facharbeiten aber ein baldiges Auslaufdatum haben, werden die Auszeichnungen wohl bald für Seminararbeiten vergeben. Insgesamt ist das Projekt „Dr. Hans Riegel-Fachpreise“ also wesentlich besser aufgestellt als zuvor und die Wahrscheinlichkeit ist hoch, dass sich die Dr. Hans Riegel-Fachpreise in Oberbayern zu einem beliebten jährlichen Schülerwettbewerb entwickeln werden. Ein infinitesimal kleiner Wermutstropfen ist, dass die Mathematik in Zukunft nicht mehr die zentrale Rolle spielen wird.

Falls Ihr euch jetzt noch Fragen stellt, einfach kurz auf der Homepage www.math.lmu.de/fachpreise/ vorbeischauen oder mich direkt fragen.

Sebastian Carstens

Disclaimer:
Die Meinung des Autors spiegelt nicht unbedingt die Meinung des Organisationsteams oder des Instituts wider. Auch für die Unbedenklichkeit der angegebenen URLs kann der Autor nicht garantieren.

Kryptographie und Algorithmische Zahlentheorie

Otto Forster

Während früher die Kryptographie hauptsächlich beim Militär und im Diplomatischen Dienst eine Rolle spielte, kommt heute fast jeder direkt oder indirekt mit Kryptographie in Berührung; sei es, dass er vom Bankautomaten Geld abhebt oder über das Internet Waren oder Dienstleistungen kauft. In der modernen Kryptographie spielen verschiedene Probleme der Algorithmischen Zahlentheorie eine Rolle.

Klassische Kryptographie

Die Kryptographie hat eine lange Geschichte. So wird berichtet, dass Caesar seine Nachrichten dadurch verschlüsselte, dass er jeden Buchstaben durch den dritten im Alphabet folgenden ersetzte, also A durch D, B durch E, u.s.w. So würde etwa aus dem Klartext KRYPTOGRAPHIE der Geheimtext

NUBSWRJUDSKLH

Natürlich ist die Entschlüsselung trivial, selbst wenn statt des hier verwendeten Offsets 3 eine andere geheim gehaltene Zahl m benutzt wird. Da es nur 26 verschiedene Möglichkeiten gibt, kann man durch Durchprobieren aller Fälle leicht den Klartext rekonstruieren, was der Leser etwa mit dem Geheimtext

CEHWUDIJKDTXQJWEBTYCCKDT

versuchen kann. Etwas schwieriger wird es, wenn statt dieser sog. Caesar-Substitution eine beliebige Permutation π des Alphabets A,B,...,Z verwendet wird. Hier verwendet man zum Entschlüsseln Statistiken über Buchstaben-Häufigkeiten und Häufigkeiten von Bigrammen. Z.B. ist im Deutschen 'E' mit 17% der häufigste Buchstabe, vor 'N' mit 10%; die häufigsten Bigramme sind 'ER' und 'EN'. (Solche Statistiken helfen natürlich nur bei etwas längeren Geheimtexten, oder wenn für mehrere Verschlüsselungen derselbe Schlüssel π verwendet wird.) Um das unbefugte Entschlüsseln zu erschweren, wurden im Laufe der Zeit komplexere Verfahren entwickelt, bei denen nicht alle Buchstaben des Klartextes derselben Permutation unterworfen werden. Das wohl berühmteste Kryptosystem ist die vom deutschen Militär im zweiten Weltkrieg verwendete ENIGMA. Dies ist eine sog. Rotormaschine. Die Verschlüsselung wird durch Hintereinanderschalten mehrerer Permutationen, die auf drehbaren Scheiben verdrahtet sind, bewirkt. Nach jedem Buchstaben des Klartextes werden die Scheiben wie bei einem Zählwerk um eins weitergedreht, so dass jedes Mal eine neue Permutation entsteht. Zur Kryptoanalyse der ENIGMA siehe den interessanten Aufsatz von *Cornelius Greither:* 'Mathematik und Geheimhaltung' in MATHE-LMU.DE, Nr. 19, Januar 2009, S. 28 – 34.

Es gibt ein Kryptosystem, dessen Sicherheit man mathematisch beweisen kann, das sog. *One-Time-Pad* (Vernam 1918). Es lässt sich so beschreiben: Um einen Klartext $A_1A_2\dots A_n$ der Länge n zu verschlüsseln, benutzt man ein "One-Time-Pad" gleicher Länge, das ist eine zufällige Folge $P_1P_2\dots P_n$ von Buchstaben. Der Geheimtext $C_1C_2\dots C_n$ entsteht durch Addition modulo 26 des One-Time-Pads auf den Klartext, wobei das Alphabet $\{A, B, \dots, Z\}$ mit $\mathbb{Z}/26$ identifiziert wird ($A = 0$, $B = 1$, $C = 2$, $\dots$, $Z = 25$): $C_k := A_k + P_k$. Zum Beispiel:

```
  KRYPTOGRAPHIE
+NCPHIBBADGDCN
--------------
  XTNWBPHRDVKKR
```

Unter der Voraussetzung, dass die Folge

$P_1 \dots P_n$ rein zufällig ist und nur einmal verwendet wird, lässt sich zeigen, dass die Kenntnis des verschlüsselten Textes keinerlei Informationsgewinn über den Klartext bringt (im Sinne der Shannonschen Informationstheorie), d.h. man weiß über den Klartext genauso viel, wie man auch ohne das Vorliegen des verschlüsselten Textes wüsste. Der Nachteil des One-Time-Pads ist natürlich, dass der Schlüssel ebenso lang wie die Nachricht selbst ist und für jede Nachricht ein neuer Schlüssel erforderlich ist. Deshalb ist es für den alltäglichen Gebrauch nicht geeignet. Es soll aber (in einer Variante) für den sog. heißen Draht zwischen Washington und Moskau verwendet worden sein.

Moderne Blockverschlüsselungs-Verfahren

In der klassischen Kryptographie wird der Text als eine Folge von Buchstaben A,. . . ,Z betrachtet, wobei zwischen Groß- und Kleinschreibung nicht unterschieden wird. Leerzeichen, Satz- und Sonderzeichen werden ignoriert, Ziffern werden meist ausgeschrieben. Die Verschlüsselung wirkt auf die einzelnen Buchstaben als Ganzes. In der modernen Kryptographie wird der Text als Folge von Bytes zu je 8 Bits betrachtet, also insgesamt als eine lange Folge von Bits (die die Werte 0 und 1 annehmen können). Bei sog. Blockverschlüsselungs-Verfahren wird der Text in eine Folge von Blöcken fester Bit-Länge unterteilt, die einzeln verschlüsselt werden.

Mehr als zwei Jahrzehnte lang wurde, vor allem im Bankwesen, der von IBM und NSA entwickelte DES (Data Encryption Standard) verwendet, der 1977 in den USA als Standard für nicht-klassifizierte Daten eingeführt worden ist. Hier haben die einzelnen Blöcke eine Länge von 8 Bytes = 64 Bits. Die Schlüssellänge ist 56 Bits (8 Bytes zu 7 Bits, das achte Bit dient als Prüfbit). Dabei kann jedes der 64 Bits des Klartext-Blocks jedes Bit des verschlüsselten Blocks beeinflussen. Ändert man nur ein einziges Bit des Klartext-Blocks, so werden durchschnittlich die Hälfte aller Bits des verschlüsselten Blocks geändert; Analoges gilt, wenn der Schlüssel nur um ein einziges Bit geändert wird. Im Laufe der langen Zeit der Verwendung von DES wurde kein besseres Verfahren zum unbefugten Entschlüsseln gefunden als die "Brute-Force"-Methode, das systematische Durchprobieren aller $2^{56} = 72\,057\,594\,037\,927\,936 \approx 7.2 \cdot 10^{16}$ möglichen Schlüssel. Im Jahr 1998 konnte dies aufgrund der enorm gestiegenen Leistung der Computer zum ersten Mal auch praktisch durchgeführt werden, so dass das Verfahren heute nicht mehr sicher ist. Nach einer internationalen Ausschreibung wurde 2002 als Nachfolger von DES ein AES (Advanced Encryption Standard) eingeführt, der von den belgischen Kryptologen J. Daemen und V. Rijmen unter dem Namen Rijndael entwickelt worden war. Es handelt sich um ein Blockverschlüsselungs-Verfahren mit einer Blocklänge und einer Schlüssellänge von 128 Bits (= 16 Bytes). Statt 128 sind auch 192 oder 256 Bits möglich.

Die genannten Blockverschlüsselungs-Verfahren sind ebenso wie die klassischen Verfahren sog. symmetrische Krypto-Systeme, d.h. Sender und Empfänger müssen im Besitz desselben Schlüssels sein, und es stellt sich, insbesondere bei der heutigen massenhaften Verwendung, das Problem der Übermittlung der Schlüssel. Dies Problem wird durch die sog. *Public-Key*-Kryptographie gelöst.

Das RSA-Verfahren

Ein Public-Key-Kryptosystem ist ein asymmetrisches Verschlüsselungs-Verfahren.

Das bedeutet: Derjenige Kommunikations-Partner (nennen wir ihn Bob), der verschlüsselte Nachrichten empfangen will, muss ein zusammengehöriges Schlüsselpaar (E, D) aufstellen, bestehend aus einem öffentlichen Schlüssel (Public Key) E und einem privaten Schlüssel D. Man kann sich E (encryption function) und D (decryption function) als Funktionen vorstellen, die Klartexte in Geheimtexte (bzw. umgekehrt) transformieren, so dass $D \circ E = \mathrm{id}$. Der private Schlüssel muss von Bob geheim gehalten werden. Der öffentliche Schlüssel wird bekannt gemacht (analog einer Telefonnummer in einem Telefonbuch). Will nun Alice[1] eine Nachricht x an Bob senden, die nur dieser lesen darf, verschlüsselt sie x mit dem öffentlichen Schlüssel E von Bob und sendet ihm den Geheimtext $y := E(x)$. Bob kann die Nachricht mit seinem privaten Schlüssel D rekonstruieren, $D(y) = D(E(x)) = x$. Das System muss so beschaffen sein, dass es praktisch unmöglich ist, aus dem öffentlichen Schlüssel den privaten Schlüssel zu berechnen.

Das bekannteste Public-Key-System ist das RSA-Verfahren, das 1977 von R. Rivest, A. Shamir und L. Adleman erfunden worden ist. (Auf andere Public-Key-Systeme, z.B. solche, die mit dem Problem des Diskreten Logarithmus zusammenhängen, gehen wir hier aus Raumgründen nicht ein.) Beim RSA-Verfahren geht Bob wie folgt vor: Er wählt zwei große Primzahlen $p \neq q$, etwa von der Größenordnung 2^{512} oder mehr. Dazu stehen interessante und effiziente Primzahltests zur Verfügung, auf die wir hier aber nicht eingehen können. Mit diesen Primzahlen wird der sog. RSA-Modul $N := p \cdot q$ berechnet. Außerdem wählt Bob eine ganze Zahl $e \geqslant 3$, die zu $\varphi(N) = (p-1)(q-1)$ teilerfremd ist, und berechnet (mit dem erweiterten Euklidischen Algorithmus) eine Zahl d mit

$$ed \equiv 1 \bmod \varphi(N).$$

Nun dient (N, e) als öffentlicher Schlüssel und (N, d) als privater Schlüssel von Bob. Die Zahlen p, q und $\varphi(N)$ sind ebenfalls geheim zu halten, denn mit ihrer Hilfe lässt sich d aus e berechnen. Beim RSA-System werden die zu versendenden Nachrichten als Elemente des Restklassenrings $\mathbb{Z}/N$ aufgefasst. Ist z.B. $N > 2^{1024}$, so kann jede Bitfolge der Länge $\leqslant 1024$ Bits $= 128$ Bytes eindeutig mit einem Element $x \in \mathbb{Z}/N$ identifiziert werden. In der Praxis benutzt man heute RSA (oder andere Public-Key-Verfahren) meist zum Austausch eines Sitzungs-Schlüssels für ein symmetrisches Kryptosystem wie AES und setzt dann die weitere Kommunikation mit diesem symmetrischen Verfahren fort.

Die Verschlüsselungs-Funktion bei RSA ist

$$E : \mathbb{Z}/N \to \mathbb{Z}/N, \quad x \mapsto x^e \bmod N,$$

die Entschlüsselungs-Funktion

$$D : \mathbb{Z}/N \to \mathbb{Z}/N, \quad x \mapsto x^d \bmod N.$$

Da die multiplikative Gruppe $(\mathbb{Z}/N)^*$ die Ordnung $\varphi(N)$ hat, folgt aus $ed \equiv 1 \bmod \varphi(N)$, dass $D \circ E = \mathrm{id}$.

Wie schwer ist es für jemand, der nur den öffentlichen Schlüssel kennt, daraus den privaten Schlüssel zu berechnen, d.h. das System zu brechen? Theoretisch ist das möglich, denn der Entschlüsselungs-Exponent d ist einfach das Inverse des bekannten Verschlüsselungs-Exponenten e modulo $\varphi(N)$. Aber zur Berechnung von $\varphi(N) = (p-1)(q-1)$ braucht man die Primfaktorzerlegung von N. Es kommt also darauf an, wie schwer es ist, eine zusammengesetzte Zahl zu faktorisieren. Als RSA geschaffen wurde, stellte *Martin Gardner* es im Scientific American in einem Auf-

[1] In der neueren kryptographischen Literatur heißen die Kommunikations-Partner stets Alice und Bob

satz mit dem Titel "A new kind of cipher that would take millions of years to break" vor, zusammen mit einer Preisaufgabe der Erfinder von RSA, einen Geheimtext zu entschlüsseln, was auf die Faktorisierung einer 129-stelligen zusammengesetzten Zahl hinauslief. Es dauerte dann aber nicht Millionen, sondern nur 17 Jahre, bis diese Zahl in seine Primfaktoren zerlegt war. Um dies zu erläutern, betrachten wir einige Faktorisierungs-Algorithmen.

Das Pollardsche Rho-Verfahren

Die naive Methode zur Faktorisierung einer Zahl N ist die Probedivision: Man dividiert N der Reihe nach durch 2 und alle ungeraden natürlichen Zahlen $d = 3, 5, 7, \ldots$ solange, bis die Division aufgeht. (Man könnte sich bei der Probedivison auf Primzahlen d beschränken, aber dann hat man die zusätzliche Arbeit, zu entscheiden welche Zahlen prim sind.) Falls N zusammengesetzt ist, hat es mindestens einen Teiler $d \leqslant \sqrt{N}$. Die Anzahl der nötigen Probedivisionen ist also von der Ordnung $O(\sqrt{N})$.

Von J. Pollard stammt ein wesentlich besserer Algorithmus, der zur Zeit der Entstehung von RSA einer der effizientesten Faktorisierungs-Algorithmen war. Das Pollardsche Verfahren ist ein probabilistischer Algorithmus und beruht auf dem bekannten *Geburtstags-Paradoxon:* Wählt man aus einer Menge M von m paarweise verschiedenen Elementen zufällig und unabhängig $s \geqslant 1.2\sqrt{m}$ Elemente (Wiederholungen sind erlaubt), so ist die Wahrscheinlichkeit, dass zwei der gewählten Elemente gleich sind, mindestens $1/2$. Für $s \geqslant 2\sqrt{m}$ ist die Wahrscheinlichkeit schon größer als 85%, für $s \geqslant 3\sqrt{m}$ fast 99%. Der Name kommt von folgender Anwendung ($m = 365$): Sitzen z.B. in einem Hörsaal 40 oder mehr Personen, so haben mit großer Wahrscheinlichkeit mindestens zwei von ihnen am selben Tag Geburtstag.

Zur Anwendung des Geburtstags-Paradoxons auf das Problem der Faktorisierung sei N eine zusammengesetzte Zahl, die also einen (noch unbekannten) Primteiler $p \leqslant \sqrt{N}$ besitzt. Wir betrachten nun die Mengen $\mathbb{Z}/N$ und $\mathbb{Z}/p$ sowie die natürliche Abbildung $\phi : \mathbb{Z}/N \to \mathbb{Z}/p$. Wir wählen zufällig s Elemente $x_1, x_2, \ldots, x_s \in \mathbb{Z}/N$, wobei $s = \lambda\sqrt[4]{N}$, $\lambda > 1.2$. Mit großer Wahrscheinlichkeit sind die x_i paarweise verschieden. Auf die Bildelemente $\overline{x}_i := \phi(x_i) \in \mathbb{Z}/p$ lässt sich wegen $s > \lambda\sqrt{p}$ das Geburtstags-Paradoxon anwenden. Es gibt also wahrscheinlich Indizes $i \neq j$ mit $\overline{x}_i = \overline{x}_j$. Dies bedeutet $\phi(x_i - x_j) = 0$, also ist p ein Teiler von $x_i - x_j$. Berechnet man nun (mit dem Euklidischen Algorithmus) den größten gemeinsamen Teiler

$$d := \gcd(x_i - x_j, N)$$

(dies ist ohne explizite Kenntnis von p möglich), so hat man einen echten Teiler von N gefunden. Als ein Beispiel haben wir für $N = 10823$ zufällig 15 Elemente $x_i \in \mathbb{Z}/N$ ausgewählt, siehe Fig. 1.

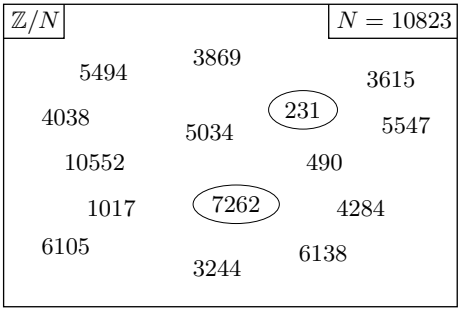


Fig. 1

Für die beiden oval umrandeten Elemente $x_i = 7262$ und $x_j = 231$ gilt

$$\gcd(7262 - 231, N) = 79,$$

also ist $p = 79$ ein Teiler von N und $N = 79{\cdot}137$ die Primfaktorzerlegung von N. Der Haken dabei ist: Wie findet man ein geeignetes Paar x_i, x_j? Würde man alle $\frac{s(s-1)}{2}$

Paare durch Bildung des $\gcd$ einzeln testen, käme man wieder auf eine Komplexität von $O(\sqrt{N})$, also kein Vorteil gegenüber der Probedivision. Hier kommt nun folgender Trick zum Einsatz: Man verwendet keine beliebige Zufallsfolge, sondern eine Pseudo-Zufallsfolge, die durch eine nichtlineare Funktion $f : \mathbb{Z}/N \to \mathbb{Z}/N$, z.B. $f(x) := x^2 + 1$ gegeben wird. Ausgehend von einem zufälligen $x_0 \in \mathbb{Z}/N$ konstruiert man x_i rekursiv durch $x_{i+1} := f(x_i)$. Für diese Folge gilt: Ist $x_j - x_i$ durch p teilbar, so sind für alle $r \geqslant 0$ auch die Differenzen $x_{j+r} - x_{i+r}$ durch p teilbar, d.h. $\overline{x}_{j+r} = \overline{x}_{i+r}$ in $\mathbb{Z}/p$. Da $\mathbb{Z}/p$ nur endlich viele Elemente hat, mündet die Folge $\overline{x}_0, \overline{x}_1, \overline{x}_2, \ldots$ deshalb in einem Zykel. In Fig. 2 ist das in dem Beispiel $N = 10823$, $p = 79$ und $x_0 = 6105$ ausgeführt.

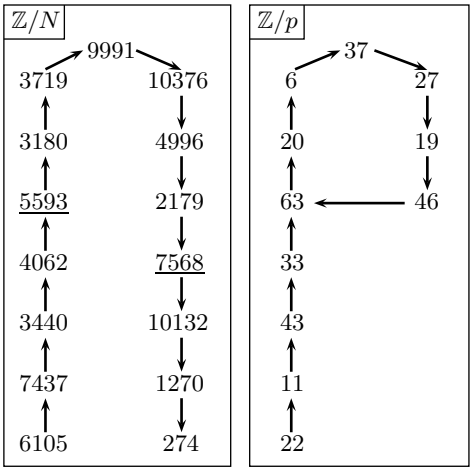


Fig. 2

Hier ist $x_4 = 5593$ und $x_{11} = 7568$ das erste Paar von Elementen, deren Differenz durch p teilbar ist, also $\overline{x}_{11} = \overline{x}_4$. Das Bild der Folge (x_i) in $\mathbb{Z}/p$ hat also eine dem griechischen Buchstaben ρ ähnliche Gestalt, daher der Name des Verfahrens. Systematisch kann man ein solches Paar wie folgt finden: Außer der Folge (x_i) betrachtet man die Folge $y_i := x_{2i}$, die durch $y_0 := x_0$ und $y_{i+1} := f(f(y_i))$ rekursiv berechnet werden kann. Für jedes $k > 0$ untersucht man, ob

$$d := \gcd(y_k - x_k, N) = \gcd(x_{2k} - x_k, N) > 1.$$

Dies tritt sicher dann ein, wenn k größer als die Länge der Vorperiode und ein ganzzahliges Vielfaches der Periodenlänge der Folge $(\overline{x}_i)$ in $\mathbb{Z}/p$ ist. (In unserem Beispiel ist $\overline{y}_7 = \overline{x}_{14} = \overline{x}_7$.) Damit hat man dann einen echten Teiler d von N gefunden, wenn nicht ausnahmsweise schon $x_{2k} = x_k$ in $\mathbb{Z}/N$. Dann hilft es oft, mit einem anderen Anfangswert x_0 zu starten. Mit verschiedenen technischen Verbesserungen, die man noch anbringen kann, stellt das Pollardsche Rho-Verfahren einen probabilistischen Faktorisierungs-Algorithmus mit einer Komplexität $O(\sqrt[4]{N})$, genauer $O(\sqrt{p})$ dar, wobei p den kleinsten Primfaktor von N bezeichnet. Mit einer Variante dieses Verfahrens wurde 1980 zum ersten Mal die 8-te Fermatzahl $F_8 := 2^{256} + 1$ (mit 78 Dezimalstellen) faktorisiert, die einen 16-stelligen Primfaktor besitzt. Zum Angriff auf das RSA-System ist das Rho-Verfahren aber nicht geeignet, da dort der Modul N aus zwei fast gleich langen Primfaktoren besteht.

Quadratisches Sieb, Zahlkörpersieb

Von Fermat stammt ein interessantes Faktorisierungs-Verfahren, das wie folgt funktioniert: Sei N eine ungerade zusammengesetzte Zahl und $m = \lceil \sqrt{N} \rceil$ die kleinste ganze Zahl $\geqslant \sqrt{N}$. Für $k = 0, 1, 2, \ldots$ untersucht man nun, ob die Differenz $(m + k)^2 - N$ eine Quadratzahl ist. Sei etwa

$$(m + k)^2 - N = y^2.$$

Mit $x := m + k$ gilt dann $x^2 - y^2 = N$, also hat man die Zerlegung $N = (x + y)(x - y)$. Für unser obiges Beispiel $N = 10823$ erhält

man $m = 105$ und

$$\begin{aligned} 105^2 - N &= 202 \\ 106^2 - N &= 413 \\ 107^2 - N &= 626 \\ 108^2 - N &= 841 = 29^2, \end{aligned}$$

also $N = (108+29)(108-29) = 137 \cdot 79$. Für nicht zu große N funktioniert die Fermatsche Methode erstaunlich gut, für große N allerdings nur, wenn $N = uv$ ein Produkt von zwei Faktoren mit kleiner Differenz ist. Von Legendre und Gauß stammt eine Erweiterung dieser Methode, die auch auf größere Zahlen anwendbar ist. Sei etwa

$$x_k^2 - N = v_k, \quad k = 1, \ldots, r,$$

wo die v_k keine Quadrate sind, jedoch ihr Produkt $V := v_1 v_2 \cdots v_r = y^2$. Dann gilt für $x := x_1 x_2 \cdots x_r$, dass

$$x^2 \equiv y^2 \bmod N.$$

Daher ist $(x+y)(x-y)$ durch N teilbar. Falls nicht beide Faktoren einzeln durch N teilbar sind, ist $\gcd(x+y, N)$ oder $\gcd(x-y, N)$ ein echter Teiler von N. Das Problem ist nun, wie man quadratische Reste $v_k = x_k^2 - N$ finden kann, deren Produkt eine Quadratzahl ist. Hier geht man wie folgt vor: Man wählt sich eine sog. Faktorbasis aus kleinen Primzahlen q_i, $i = 1, 2, \ldots, s$ zusammen mit $q_0 = -1$, und nimmt nur solche quadratische Reste, die sich vollständig mit der Faktorbasis zerlegen lassen:

$$v_k = q_0^{\alpha_{k0}} q_1^{\alpha_{k1}} \cdots q_s^{\alpha_{ks}}.$$

Sei $\mathcal{K}$ eine Teilmenge aller Indizes k. Ein Produkt $V = \prod_{k \in \mathcal{K}} v_k$ ist genau dann ein Quadrat, wenn die Summen der Exponenten

$$\alpha_i := \sum_{k \in \mathcal{K}} \alpha_{ki}, \quad i = 0, 1, \ldots, s$$

sämtlich gerade Zahlen sind. Bezeichnet man mit $\overline{\alpha}_{ki} \in \mathbb{Z}/2$ die Restklassen von α_{ki} modulo 2, so läuft das Auffinden aller möglichen Teilmengen $\mathcal{K}$ auf die Lösung eines homogenen linearen Gleichungssystems mit der Matrix $(\overline{\alpha}_{ki})$ über dem Körper $\mathbb{F}_2 = \mathbb{Z}/2 = \{0, 1\}$ hinaus.

Betrachten wir ein einfaches Beispiel für $N := 278449$. Dann ist $m = \lceil \sqrt{N} \rceil = 528$. Wir benutzen das quadratische Polynom $Q(t) = (m+t)^2 - N$. Damit ist

$$\begin{aligned} Q(-55) &= -54720 = -2^6 \cdot 3^2 \cdot 5 \cdot 19, \\ Q(-17) &= -17328 = -2^4 \cdot 3 \cdot 19^2, \\ Q(-10) &= -10125 = -3^4 \cdot 5^3, \\ Q(-1) &= -720 = -2^4 \cdot 3^2 \cdot 5, \\ Q(7) &= 7776 = 2^5 \cdot 3^5, \\ Q(25) &= 27360 = 2^5 \cdot 3^2 \cdot 5 \cdot 19, \\ Q(44) &= 48735 = 3^3 \cdot 5 \cdot 19^2, \\ Q(55) &= 61440 = 2^{12} \cdot 3 \cdot 5. \end{aligned}$$

Für alle anderen t mit $|t| \leqslant 60$ lässt sich $Q(t)$ nicht als Produkt von Primzahlen $q < 20$ darstellen. (Dass die Primzahlen $7, 11, 13, 17$ hier nicht vorkommen, liegt daran, dass N kein quadratischer Rest modulo dieser Primzahlen ist.) Aus der obigen Tabelle sieht man z.B.

$$\begin{aligned} Q(-10)Q(-1) &= (2^2 \cdot 3^3 \cdot 5^2)^2, \\ Q(44)Q(55) &= (2^6 \cdot 3^2 \cdot 5 \cdot 19)^2. \end{aligned}$$

Aus der ersten dieser Gleichungen folgt $x^2 \equiv y^2 \bmod N$ mit

$$\begin{aligned} x &= (m-10)(m-1) = 272986, \\ y &= 2^2 3^3 5^2 = 2700. \end{aligned}$$

Nun ist $d = \gcd(x-y, N) = 907$ ein Teiler von N, was zur Faktorzerlegung $N = 907 \cdot 307$ führt. Ebenso würde man mit der zweiten Gleichung zu dieser Faktorzerlegung kommen.

Das hier skizzierte Verfahren wurde von C. Pomerance zum sog. Quadratischen Sieb

ausgebaut. Zur Faktorisierung großer Zahlen hat man quadratische Polynome $Q(t)$ für sehr große Intervalle der ganzzahligen Variablen t auf Zerlegbarkeit durch die Primzahlen einer Faktorbasis zu untersuchen. Hier kommen Siebmethoden (ähnlich dem Sieb des Eratosthenes) zum Einsatz. Denn ist $Q(t)$ durch die Primzahl q teilbar, so auch $Q(t+\nu q)$ für alle ganzen Zahlen ν. Mit einer optimierten Version des Quadratischen Siebs wurde 1994 der 129-stellige RSA-Modul der erwähnten Preisaufgabe faktorisiert. Dabei kamen 1600 Computer zum Einsatz. Das Gleichungssystem über dem Körper $\mathbb{F}_2$, das gelöst werden musste, hatte über eine halbe Million Unbekannte.

Die Komplexität des Quadratischen Siebs ist bei optimaler Wahl der Parameter

$$O(\exp((\log N)^{1/2+\varepsilon}))$$

für jedes $\varepsilon > 0$. Dies ist eine sog. subexponentielle Komplexität. Man betrachtet die Komplexität als Funktion der Länge der Eingabedaten. In unserem Fall ist dies die Stellenlänge der zu faktorisierenden Zahl N. Diese ist proportional zu $\log N$. Das Pollardsche Rho-Verfahren hatte die Komplexität $O(\sqrt[4]{N})$. Da $\sqrt[4]{N} = \exp(\frac{1}{4}\log N)$, ist dies eine exponentielle Komplexität. Polynomiale Komplexität wäre $O((\log N)^k)$ mit einem $k \geqslant 0$. Da

$$(\log N)^k = \exp(k \log\log N),$$

liegt die Komplexität des Quadratischen Siebs zwischen exponentieller und polynomialer Komplexität.

Lange Zeit war das Quadratische Sieb das effizienteste Verfahren zur Faktorisierung von zusammengesetzten Zahlen ohne kleine Primfaktoren, bis das sog. *Zahlkörpersieb* [3] entwickelt wurde, das Methoden der Algebraischen Zahlentheorie benutzt. Es hat eine Komplexität von

$$O(\exp((\log N)^{1/3+\varepsilon}))$$

für jedes $\varepsilon > 0$. Damit wurde kürzlich ein RSA-Modul der Bitlänge 768 (231 Dezimalstellen) faktorisiert. Das bedeutet, dass RSA-Moduln der Bitlänge 1024 nicht mehr lange als sicher zu betrachten sind und man zu größeren Moduln übergehen sollte. Es fragt sich natürlich, ob es noch bessere Faktorisierungs-Algorithmen gibt. Es wird vermutet, das es keine solche mit polynomialer Komplexität gibt. Dies ist aber schwierig zu beweisen, denn dadurch hätte man zugleich das Millenium-Problem NP $\neq$ P gelöst. Hier steht P für die Klasse der Probleme, die in polynomialer Zeit lösbar sind und NP für die nicht-deterministisch in polynomialer Zeit lösbaren Probleme. Das Faktorisierungs-Problem gehört zu NP, denn die Verifikation einer Zerlegung kann in polynomialer Zeit durchgeführt werden. Dies bezieht sich auf herkömmliche Computer. Für sog. Quanten-Computer fand P. Shor einen Faktorisierungs-Algorithmus mit polynomialer Komplexität. Es ist jedoch zweifelhaft, ob Quanten-Computer, die Zahlen von der Größe der RSA-Moduln faktorisieren, tatsächlich gebaut werden können.

Literatur

[1] J. Buchmann: Einführung in die Kryptographie. Springer 2010

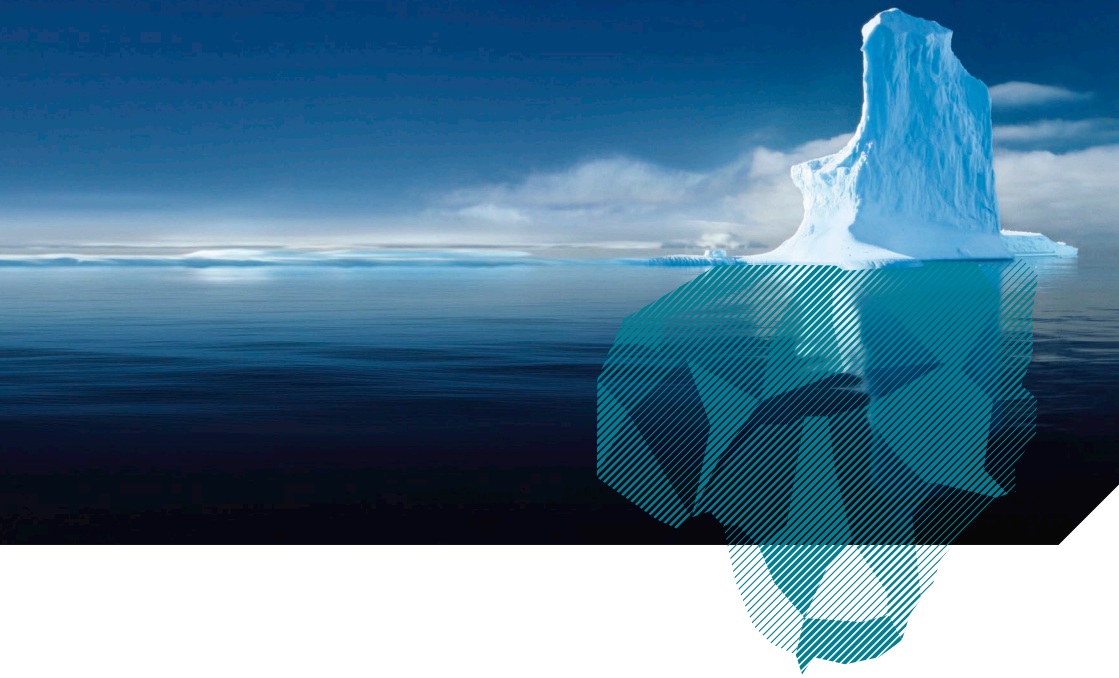
[2] H. Cohen: A course in computational algebraic number theory. Springer 2008

[3] A.K.Lenstra/H.W.Lenstra (eds.): The development of the number field sieve. Springer LNM Vol. 1554 (1991)

[4] Stinson: Cryptography. Theory and Practice. Taylor and Francis 2005

Wie könnten Sie Ihrer Karriere mehr Tiefgang verleihen?

- ☐ Wenn Sie außergewöhnliche Lösungen für globale Risiken finden
- ☐ Indem Sie statt der Spitze des Eisbergs das große Ganze sehen
- ☐ Durch eine Diskussion mit Geografen, Kapitänen und Ingenieuren
- ☐ Wenn Sie sich vor dem Schaden um das Risiko kümmern
- ☐ Mit jedem der genannten Punkte



Erfahren Sie, was es heißt, auf internationaler Ebene maßgeschneiderte Lösungen für Risiken zu entwickeln, die die Menschheit heute und in Zukunft beschäftigen. In interdisziplinären Teams meistern wir komplexe Aufgaben aus allen Bereichen der Wirtschaft und des täglichen Lebens, von Großbauprojekten über Raumfahrt bis zum Klimawandel. Wenn auch Sie Ihr Knowhow bei einem der führenden Rückversicherer der Welt einsetzen wollen, wenn auch Sie Projekte globaler Tragweite bewältigen möchten, dann sollten Sie Teil unseres Teams werden.

Warum keine Herausforderung zu groß ist, als dass wir sie nicht gemeinsam anpacken könnten, erfahren Sie unter **munichre.com/karriere**

Munich RE