NR. 19 – JANUAR 2009

LMU

MATHE-LMU.DE

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

Jahr der Mathematik - Seite 10 – 12 und 14 – 17
Mathematik und Geheimhaltung - Seite 28

Liebe Leserinnen und Leser,

das Jahr der Mathematik ist vorüber – was hat es gebracht? Mein subjektiver Eindruck war einerseits ein massives Medieninteresse zu Beginn des Jahres, das aber schnell und gründlich nachließ, andererseits eine überraschend positive Resonanz in der Öffentlichkeit während des ganzen Jahres. So steht z.B. im Abschlussbericht der dem Fach Mathematik gewidmeten 8. Münchner Wissenschaftstage: „Obwohl oder gerade weil viele Menschen Probleme mit der Mathematik in der Schule hatten, war der Zustrom an Besuchern und insbesondere an jungen Menschen … größer als in den Vorjahren, insgesamt kamen etwa … 30000 Besucher“ (siehe auch Seite 14).
Dies lehrt uns Mathematiker, noch intensiver und phantasievoller unser Fach in der Öffentlichkeit darzustellen – genügend Motivation auch für die zukünftige Arbeit der Redaktion von „mathe-lmu.de“.
Das Jahr der Mathematik ist übrigens noch nicht ganz Geschichte: Bis zum 31. Januar läuft die interessante und „berührende“ Ausstellung „Jüdische Mathematiker in der deutschsprachigen akademischen Kultur“ in der Bibliothek des Deutschen Museums (siehe Titelbild). Gehen Sie hin – es lohnt sich!

Mit den besten Wünschen für 2009

Heinrich Steinlein

Liebes Vereinsmitglied,

vor wenigen Tagen ist das Wissenschaftsjahr 2008 unter dem Motto „Mathematik – Alles, was zählt“, eine Initiative des Bundesministeriums für Bildung und Forschung und der Initiative Wissenschaft im Dialog, zu Ende gegangen. Dem überaus großen Engagement auch vieler Vereinsmitglieder ist es zu verdanken, dass zahlreiche interessante und gut besuchte Veranstaltungen des Mathematischen Instituts zum „Jahr der Mathematik“ stattfinden konnten; wir haben in unserer letzten Ausgabe ausführlich darüber berichtet. Besondere Erwähnung verdient der Festakt zum Jahr der Mathematik am 25. September 2008 mit der Eröffnung der faszinierenden Ausstellung „Imaginary – mit den Augen der Mathematik“ sowie der Preisverleihung an die Hauptgewinner des Preisausschreibens für Schüler, bei dem unter anderem die Zahl der Fußbälle abzuschätzen war, die in die Münchner Allianz-Arena passen. Über den ersten Preis, eine Reise für zwei Personen zum „Mathematikum“ nach Gießen, gesponsert von unserem Förderverein, freute sich Michael Ossiander vom Louise-Schroeder-Gymnasium. Es bleibt zu hoffen, dass auch künftig die Mathematik als faszinierende Wissenschaft in Bewusstsein der Öffentlichkeit bleibt.

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	Heinrich Steinlein, Mathematisches Institut, Universität München, Theresienstr. 39, 80333 München, Tel. 2180-4448, steinl@mathematik.uni-muenchen.de
Redaktion	Bernhard Emmer, Daniel Rost, Ingrid Schehrer, Erwin Schörner, Katharina Schüller, Heinrich Steinlein, Vitali Wachtel
Auflage	5500
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.

Mathematik am Samstag

Samstag, den 14.02.2009, 14.15 – 15.30 Uhr

Prof. Dr. Hubert Kalf	**Wie viel Platz braucht man, um eine Nadel zu drehen?**

Diese die Phantasie herausfordernde Frage hat eine überraschende Antwort. Wie bei vielen tiefliegenden mathematischen Problemen zeigt sich auch hier, dass die Lösung eines zunächst etwas exotisch klingenden Problems unerwartete Auswirkungen auf andere Teile der Mathematik haben kann, hier Integrationstheorie, Kombinatorik und sogar partielle Differentialgleichungen.

Samstag, den 07.03.2009, 14.15 – 15.30 Uhr

Dr. Heribert Zenk	**Eine Differentialgleichung und ein möglicher Nachweis für eine Fälschung**

Viele Vorgänge in der Natur laufen nach strengen Gesetzmäßigkeiten ab, die durch Differentialgleichungen beschrieben werden. Die Lösung einer solchen Differentialgleichung erlaubt uns einen Blick in Vergangenheit und Zukunft zu werfen. Anhand der Lösung eines einfachen Beispiels wollen wir die Mathematik hinter einer Methode verstehen, mit der schon einige Bilder als Fälschung nachgewiesen wurden.

Samstag, den 21.03.2009, 14.15 – 15.30 Uhr

Prof. Dr. Heinrich Steinlein	**Schokoladensoße, Passstraßen und Ringe: Wie man symmetrischen Gleichungen ihre Geheimnisse entlockt.**

Ungerade Funktionen haben stets eine Nullstelle, gerade stetige Funktionen ein lokales Extremum. Diese trivialen Aussagen für reelle Funktionen legen nahe, auch bei Abbildungen in höherdimensionalen Räumen und unter allgemeineren Symmetriebedingungen nach bestmöglichen Informationen über das Lösungsverhalten zu suchen. Ein weites Feld tut sich auf, dem wir uns mit vielfältigen Beispielen nähern wollen.

Nach allen Vorträgen gibt es Getränke und Gebäck

Mathematisches Institut der LMU München, Theresienstraße 39, Hörsaal B051

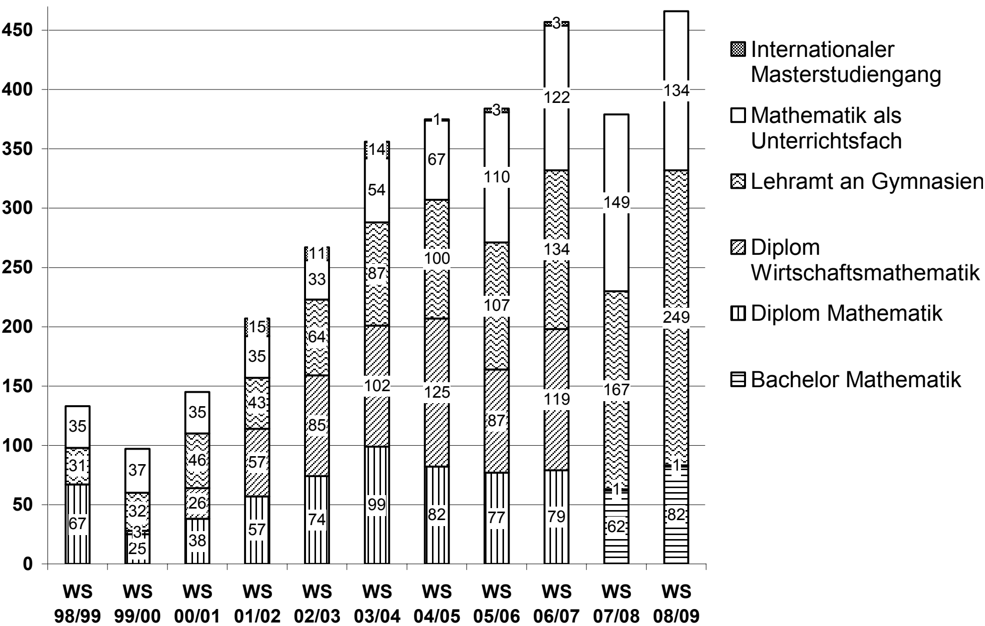
Berichte aus dem Mathematischen Institut

Studentenzahlen Bemerkenswert war in diesem Semester der gewaltige Anstieg der Anfängerzahl für das gymnasiale Lehramt (siehe Grafik), womit sogar die Rekordzahlen in diesem Studiengang aus den Jahren 1987 bis 1989 um 10 – 15 % übertroffen wurden. Bei einer gleichzeitigen geringen Einbuße bei den Zahlen für das nichtvertiefte Lehramtsstudium und einem Zuwachs bei den Bachelor-Anfängern um ein Drittel kommt unser Institut mit 466 Anfängern auf eine neue Rekordmarke. Auch die Gesamtzahl der Studierenden in den Diplom-, Bachelor-, Master- und Lehramtsstudiengängen ist mit 1841 so hoch wie noch nie. Die Anfängerzahlen im einzelnen sind (in Klammern die entsprechenden Zahlen vom Wintersemester 2007/08):

Bachelor Mathematik	82	(62)
Lehramt an Gymnasien	249	(167)
Mathematik als Unterrichtsfach	134	(149)

Personalien Zum Ende dieses Semesters werden Herr Prof. Dr. Hubert Kalf und Herr Prof. Dr. Heinrich Steinlein in den Ruhestand treten.
Als Nachfolger von Herrn Prof. Dr. Helmut Pruscha trat Herr Dr. Vitali Wachtel eine Stelle als Akademischer Rat im Bereich Stochastik an.

Wiederzuweisung von Professorenstellen Im Rahmen des Strategieprozesses „50-40-10" hatte das Institut bzgl. der im Zeitraum 2007 bis 2011 frei werdenden Professorenstellen eine Priorisierung vorzunehmen und gegebenenfalls eine Neuausrichtung zu beantragen. Von den betroffenen Stellen wurden inzwischen eine W3-Stelle (Nachfolge Filipović) und vier W2-Stellen wieder zugewiesen – bei allen läuft inzwischen das Berufungsverfahren –, eine W3- und zwei W2-Professuren wurden eingezogen. Es ist zu hoffen, dass



letztere über neu beantragte Zentren wieder ans Institut zurückfließen werden. Die Entscheidung darüber wird für Februar erwartet.

Neuzuweisung von Stellen Im Rahmen eines Ausbauprogramms des Bayerischen Staatsministeriums für Wissenschaft, Forschung und Kunst wurden unserem Institut zwei Assistenten- und eine Akademische Rats-Stelle zugewiesen.

Berufungen Wie schon erwähnt laufen an unserem Institut derzeit mehrere Berufungsverfahren für Professorenstellen:
Weit fortgeschritten ist das Verfahren für die W3-Professur in Finanzmathematik (Nachfolge Filipović). Bei den Verfahren für je eine W2-Professur in Angewandter Mathematik (Nachfolge Sachs) und in Mathematik (Nachfolge Schneider) endete die Bewerbungsfrist am 15. Dezember, bei zwei weiteren W2-Professuren in Mathematik bzw. Angewandter Mathematik (Nachfolge Georgii bzw. Steinlein) läuft sie noch bis 31. Januar.
Herr Prof. Urs Frauenfelder hat einen Ruf an die Seoul National University angenommen.
Herr Dr. Sebastian Kuntze ist einem Ruf auf eine Professur an der Pädagogischen Hochschule Ludwigsburg gefolgt.

LMUexcellent Im Rahmen des Projekts „Quantitative Finance and Insurance“ von Frau Professor Biagini besuchte Herr Prof. Harris Schlesinger (University of Alabama) unser Institut von August bis Dezember 2008, von Juni bis Dezember 2009 wird sich ein Gastaufenthalt von Herrn Prof. Wolfgang Runggaldier (Università degli Studi di Padova) anschließen.

Planungen für 2011 Im Jahre 2011 werden sowohl G9- als auch G8-Abgänger von den Gymnasien an die Universitäten strömen. Zur Entzerrung dieses verstärkten Ansturms werden spezielle Programme erarbeitet.

Studiengangskoordinator Das Mathematische Institut plant in Kürze die Besetzung einer aus Studienbeitragsmitteln finanzierte Stelle eines Studiengangskoordinators. Neben der Planung der Studiengänge und der Organisation der Lehre ist die Stelle Kontaktadresse, Informationsportal und Vermittler für Studierende und umfasst alle das Studium betreffenden Probleme und Fragen.

Verwendung der Studienbeitragsmittel Die Mittelverwendungsnachweise werden in der Studienbeitragsmittel-Kommission im Januar diskutiert und voraussichtlich auf der Fakultätsseite im Internet veröffentlicht.
Die mit Studienbeitragsmitteln finanzierte Neugestaltung der Wartezonen im Mathematischen Institut steht kurz vor der Vollendung.

Lehrassistentenstellen Um Lehrassistentenstellen attraktiver zu gestalten, sollen diese künftig mit einer gemischten Finanzierung (1/4 Lehrassistentenstelle mit 4,5 Stunden Lehrdeputat plus 1/4 Stelle aus Mitteln ohne Lehrdeputat) angeboten werden. Im Sommersemester stehen 6 derartige halbe Stellen zur Verfügung.

Bachelor-Studiengänge Zu den aktuell möglichen Nebenfächern Informatik, Statistik, BWL, VWL und Insurance and Risk Management sollen in Kürze auch die Nebenfächer Experimentalphysik und Theoretische Physik kommen. Für schon eingeschriebene Studierende wird eine Umschreibemöglichkeit angeboten werden.
Der Bachelor-Studiengang „Wirtschaftsmathematik“ ist vorbereitet und wird, abhängig von der Bearbeitung durch die Rechtsabteilung der Universität, baldmöglichst starten.

Master-Studiengang Auch für einen Master-Studiengang in Mathematik laufen die Vorbereitungen, so dass hier ebenfalls, abhängig von der Bearbeitung durch die Rechtsabteilung, mit einem baldmöglichsten Beginn gerechnet werden kann.

Bafög-Leistungsbescheinigungen Im Gegensatz zur bisherigen Regelung ist nur mehr eine kleine Auswahl an Lehrpersonen berechtigt, die Bafög-Leistungsbescheinigungen auszustellen. Die zuständigen Personen für die jeweiligen Studiengänge erfährt man, wenn die Bereitstellung erfolgt ist, auf der Internetseite des Mathematischen Instituts.

Jahr der Mathematik Am kürzlich zu Ende gegangenen Jahr der Mathematik hat sich unser Institut in vielfältiger Weise sehr erfolgreich beteiligt: So entstand unter der Federführung des Deutschen Museums die Aktion „Zahllose Abenteuer! Mit mathematischem Blick“, es wurden die Filmwoche und die Ausstellungen „Imaginary“ sowie „Jüdische Mathematiker in der deutschsprachigen akademischen Kultur“ nach München geholt, bekannte Aktionen wie „Mathematik am Samstag“ und der „Tag der Mathematik“ eingebracht und mit dem „Mobilen MatheLabor“ etwas geschaffen, das weit über dieses Jahr hinaus wirken soll. Lesen Sie hierzu auf den Seiten 10 – 17 Beschreibungen von einigen der Aktionen.

Bundesverdienstkreuz für Mathematik-Professorin Kristina Reiss

Kristina Reiss, Professorin für Didaktik der Mathematik und Informatik an unserem Institut, erhielt im Juli 2008 das Bundesverdienstkreuz am Bande. Es wurde ihr vom damaligen bayerischen Wissenschaftsminister Thomas Goppel überreicht.
Mit dem Bundesverdienstkreuz wurde ihr weitreichendes Engagement in der Lehrerausbildung und interdisziplinären Didaktikforschung gewürdigt. Gerade in einer Zeit, in der Bildungsplanung hinterfragt und erneuert wird, erscheint diese Ehrung in einem besonders strahlenden Licht, das dem Mathematischen Institut als Ganzes einen neuen Glanz verschafft und zur notwendigen Erhöhung von Studentenzahlen, gerade im Bereich des Lehramtes, gewaltig beiträgt. Die Lehramtsausbildung ist traditionell am Mathematischen Institut verankert, sie muss aber nun im kulturellen Wandel bestehen können. Dafür wurde Frau Reiss 2005 an das Mathematische Institut berufen, und sie hat seitdem die Lehramtsausbildung in vorbildlicher Weise weitergeführt und unser Institut im Bereich der Mathematik-Didaktik national und international vernetzt. Frau Reiss ist eine der führenden Didaktikerinnen weltweit.
Das Mathematische Institut gratuliert Frau Reiss zur Ehrung mit dem Bundesverdienstkreuz, und wir sind stolz, sie in unserer Mitte zu haben.

Detlef Dürr

Liebe Leserinnen und Leser,

zugegeben, manchmal hat mir der Stress zu schaffen gemacht und den Schlaf geraubt, etwa wenn wir einen Tag vor Drucklegung noch eine Seite leer hatten oder gar das Titelbild fehlte – es ging dennoch immer gut aus. Doch all die Sorgen waren vergessen, wenn ich die Palette mit den neuen Heften von der Spedition übernehmen konnte, den ersten Karton auspackte und mich wieder einmal über die perfekte Arbeit der Druckerei Siller freuen durfte.

Die Idee zur Institutszeitschrift „mathe-lmu.de“ wurde aus der Not geboren: 1999 sank die Zahl der Anfängerstudenten des Mathematischen Instituts auf ein inakzeptables Niveau, gleichzeitig war ein Förderverein gegründet worden, der sinnvolle Aufgabenfelder brauchte. So entstand die etwas aberwitzige Idee, sich für eine Verbesserung der Außenwirkung des Instituts journalistisch zu betätigen. Am Ende durften wir Initiatoren überrascht sein, dass das recht bescheiden geplante Blatt sich weit größer und auch in gewissem Sinne professioneller entwickelte.

Zu einem beträchtlichen Teil verdanken wir dies unserem Layouter Gerhard Koehler. Ohne sein Wissen und seine ideenreiche gestalterische Arbeit wären wir nicht weit gekommen. Dass er auch dann noch Änderungswünsche einarbeitet, wo anderen längst der Geduldsfaden gerissen wäre, ist für uns ein Geschenk, das wir leider manchmal überstrapazieren.

Ganz wichtig war all die Jahre die Harmonie im Redaktionsteam – die Aufgabenteilung hat stets hervorragend geklappt. Ganz wichtig waren aber auch die vielen, die außerhalb des Teams mitarbeiteten, allen voran Volker Eberhardt, dem zu verdanken ist, dass unser Heft stets fast fehlerfrei in Druck geht.

Eine der größten positiven Überraschungen war für mich, dass wir fast nie einen Korb bekamen, wenn wir um einen Artikel baten, und dass sich die überwiegende Mehrheit der Autoren streng an die Termin- und Längenvorgaben hielt. Der Spitzenplatz gebührt dabei eindeutig Cornelius Greither, der mir trotz Überlastung zusagte und schon zwei Tage später den wunderschönen Artikel auf Seite 28 im aktuellen Heft zusandte.

Mit Ablauf dieses Semesters endet meine Berufstätigkeit. Da die Zeitschrift von einem aktiven Institutsmitglied herausgegeben werden sollte, ist dies das letzte Heft, das ich als Verantwortlicher und Leiter des Teams gestalte. Wie es weitergehen wird, ist leider noch unklar, doch ist der Neuzugang Vitali Wachtel zu unserem Team ein gutes Zeichen, dass „mathe-lmu.de“ eine Zukunft haben wird. Ich selbst bin bereit, in gewissem Umfange auch weiterhin mitzuarbeiten, und lade alle ein, ebenfalls zum Team zu stoßen: Die Arbeit macht Spaß, und man muss sich nur im Rahmen der zeitlichen Möglichkeiten engagieren.

In den knapp 10 Jahren seit der Gründung haben etwa 300 bis 400 Leute in irgendeiner Weise zu unserer kleinen Zeitschrift beigetragen. Ich danke allen ganz herzlich für die wertvolle Hilfe, ohne die das Projekt zum Scheitern verurteilt gewesen wäre, zugleich aber auch den Anzeigenkunden, die unserer Arbeit die finanzielle Basis gaben, und den vielen treuen Leserinnen und Lesern für ihr anhaltendes Interesse.

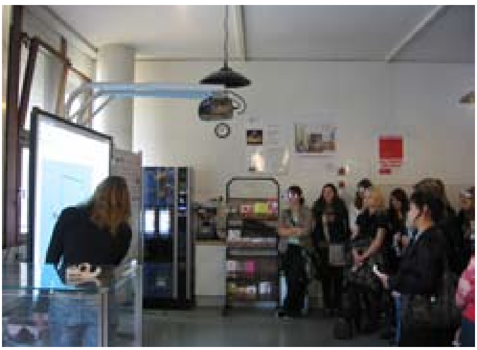
Heiner Heinle


Ihre Vision: Der optimale Start in Ihre Zukunft.
Unser Versprechen: Ausgezeichnete Einstiegsprogramme.
Jetzt bewerben!
Für viele ist der Hochschulabschluss die Erfüllung eines lang gehegten Traums. Doch für Sie ist es erst der Anfang – und der Zeitpunkt für eine der wichtigsten Entscheidungen für Ihre Zukunft. Die Deutsche Bank gibt Ihnen die Möglichkeit, Ihre Ziele zu erreichen. Als eines der weltweit führenden Finanzunternehmen bieten wir Ihnen das geeignete Umfeld, um Ihre Karriere ideal zu starten und voranzutreiben. Steigen Sie bei uns ein und finden Sie Ihren Weg in einem der besten Teams der Finanzbranche!
Bewerben Sie sich jetzt.
Mehr Infos unter www.db.com/careers/de.
Expect the better career.
Asset Management
Corporate Development
Finance
Global Banking
Global Markets
Group Technology & Operations
Human Resources
Inhouse Consulting
Legal, Risk & Capital
Private & Business Clients
Private Wealth Management
Regional Management
Leistung aus Leidenschaft.
Deutsche Bank

„IMAGINARY – mit den Augen der Mathematik" – ein echtes Erlebnis

„Ich freue mich, euch bei Imaginary begrüßen zu dürfen. Ich heiße Diana und werde versuchen, euch in der nächsten Stunde mit Hilfe der Exponate dieser Austellung das Unvorstellbare anschaulich zu präsentieren" – so fingen die Führungen für die Schüler an. Die Wanderausstellung „IMAGINARY – mit den Augen der Mathematik", konzipiert und betreut vom Mathematischen Forschungsinstitut Oberwolfach, war vom 25. September bis 20. Oktober 2008 zu Gast am Mathematischen Institut der Ludwig-Maximilians-Universität, unter der Koordination von Professor Martin Schottenloher.

Und dazu habe ich gleich eine Warnung ausgesprochen: „Hat jemand schon bemerkt, dass ich keine Deutsche bin? Ich werde deswegen eure Unterstützung während der Führung brauchen". Denn Imaginary ist als eine interaktive Ausstellung erdacht worden, was die Vielfalt ihrer Exponate zeigt, und der Sinn der Führungen war es tatsächlich, die Neugier zu wecken und die Schüler oder Besucher zum eigenen Ausprobieren anzuregen. Darüber hinaus waren die Besucher immer ermutigt, die Gleichungen, deren Lösungen als witzige Figuren auf den interaktiven Tafeln dargestellt waren, selbst zu ändern und eigene Bilder zu erzeugen und auszudrucken.



Imaginary begeistert jeden, der sich traut, diese Interaktivität auszunutzen. Das hat mich auch ermutigt, Führungen selbst zu machen und unsere BetreuerInnen Jenny Zeiser, Sonja Stockert und Dominik Ostermayr dabei zu unterstützen. Das war nötig, weil bei 24 angemeldeten Schulen – einige davon mit zwei Klassen oder mit mehr als 30 Schülern – es sich nicht anders organisieren ließ als durch parallele Führungen. Überzeugend für mich war auch der internationale Charakter der Austellung, da Mathematik an sich eine internationale Sprache ist. Imaginary hat mich als Rumänin oder Basil Karadais als Griechen genauso verblüfft wie die Mathematik- oder Physikstudenten, die Schüler (insgesamt ca. 600), aber auch andere Leute mit unterschiedlichem Hintergrund, welche die Ausstellung besucht haben.

Man hat während der Führungen auch versucht, den Besuchern zu zeigen, dass Mathematik Teil des Alltags ist und dass sich hinter komplizierten Konstruktionen oft interessante Formeln verstecken. Um das dem Publikum plausibel zu machen, musste man das Abstrakte anschaulich beschreiben, z.B. die Minimalflächen durch das Modell eines Parkhauses. Darüber hinaus hat jeder Besucher das Parkhaus in der Form eines Computerspiels mit einem Steuerungssystem erkunden können. Das Schneckenhaus ist vor den Augen des Besuchers erzeugt worden, und durch 3-D-Brillen wurde es sogar noch vorstellbarer und fast greifbar gemacht. Bei Singularitäten war der Schwerpunkt auf Weltrekorde gelegt, und dabei wurden die Besucher auf offene Probleme in der Mathematik aufmerksam gemacht. Und was kann für die Leiterin einer Führung und Promotionsstudentin erstrebenswerter sein, als während der Erklärung von einer Lehrerin gesagt zu bekommen: „Wissen Sie, ich habe am Lehrstuhl an der Friedrich-Alexander-Universität in Erlangen-Nürnberg promoviert, als Herr Prof. Barth seinen Weltrekord erzielt hat“.

Mathematik war bei Imaginary nicht nur eine Naturwissenschaft, sondern auch Kunst. Klassische Holzbilder waren mit modernen interaktiven Tafeln verknüpft, und man hatte auch die Möglichkeit, sich Einblicke in die Geschichte der Mathematik durch den Film MESH geben zu lassen. An unserem Mathematischen Institut haben die Umstände zu Improvisation gezwungen, aber das ist von den Organisatoren zu einem Vorteil umgedreht worden. Zum Beispiel hat Dr. Andreas Matt, der Koordinator vom Forschungsinstitut Oberwolfach, die Holzbilder zu einem Labyrinth gestaltet. Andererseits wurde die von der Fachschaft für Erstsemester organisierte Begrüßungsfeier als Gelegenheit benutzt, die lockere Universitätsatmosphäre zu präsentieren und den Schülern zu zeigen, dass man am Mathematischen Institut in einer freundlichen Umgebung studiert.

Imaginary wurde am 25. September 2008 mit einer Festveranstaltung mit kleinem Buffet eröffnet. Das Zielpublikum waren alle, deren Neugier durch die intensive Werbung mit Flyern und Einladungen geweckt wurde. Speziell zum Festakt wurden alle Gymnasien im Münchner S-Bahn-Bereich durch Briefe eingeladen. Ferner wurde den Schülern, die am Preisausschreiben teilgenommen haben, mit persönlichen Briefen und Urkunden gratuliert. Viele Preise wurden verliehen: Laptops, Handys, IPods, FC Bayern-Karten, Arena-Führungen, Galaxy-Karten, Fußbälle usw. Ziel des Preisausschreibens und des Festaktes war es, die Vernetzung zwischen den Schulen und der Universität zu verfestigen.

Der Festakt wurde durch Prof. Dr. Kristina Reiss, die Dekanin der Fakultät für Mathematik, Informatik und Statistik und durch Herrn Adolf Präbst vom Bayerischen Staatsministerium für Unterricht und Kultus eröffnet. In einem eindrucksvollen Vortrag über „Die Mathematik des Unmöglichen“ zeigte Prof. Dr. Martin Grötschel aus Berlin, dass man in der Mathematik manche Sackgasse in Gold verwandeln könnte, weil ein grosses Potenzial für neue Erfindungen existiert. Prof. Dr. Otto Forster von der LMU hat zum Thema „Offene Probleme der Mathematik“ ein konkretes Beispiel beschrieben, um auf die Schönheit und gleichzeitig den Aufwand der Mathematik hinzuweisen. Zum Schluss hat Dr. Andreas Daniel Matt vom MFO in wenigen Worten die Teilnehmer aufgefordert, sich das „Imaginäre“ vorzustellen und dazu gleich eine Führung durch die Ausstellung angeboten, um auf Fragen einzugehen. Ein Buffet hat den Teilnehmern die Möglichkeit gegeben, sich zu unterhalten und Kontakte zu schließen.

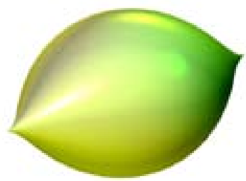
Die Vernetzung zwischen den Gymnasien und der Universität war auch das Ziel des „Tages der Mathematik“ am 18. Oktober 2008 und des Messestandes „Mathematik zum Anfassen“ im Rahmen der Münchner Wissenschaftstage (siehe Seite 14 – 17). Imaginary war bei beiden Aktivitäten dabei, und am 18. Oktober fand die Ausstellung sogar parallel statt: Ein Teil der Ausstellung ist für den „Tag der Mathematik“ an unserem Institut geblieben und hat die jungen Mathematiker begeistert, die in Scharen rund um die Tastatur eines Laptops standen und die Fähigkeiten des Roboters vom Programm Cinderella ausprobiert haben und sich dabei alle amüsiert haben. Am Mathematischen Institut sind auch 3-D-Skulpturen weiterhin ausgestellt worden, um die Funktionsfähigkeit vom Rapid Prototyping Drucker vorzustellen.

Statt des Labyrinths ist im Speerträger-Foyer des Hauptgebäudes ein komplexer Aluminiumwürfel aufgebaut worden, der die Glasbilder ausstellte. Die Präsentation auf der Messe war anspruchsvoll, und trotz der kurzen Zeitspanne haben die Münchner Wissenschaftstage eine große Besucherzahl angelockt.

Wir alle vom Organisationsteam an der LMU – Prof. Schottenloher, die BetreuerInnen

IMAGINARY

mit den Augen der Mathematik



Zitrus $x^2+z^2 = y^3(1-y)^3$

Eine Ausstellung des Mathematischen Forschungsinstituts Oberwolfach

Jenny Zeiser, Sonja Stockert, Dominik Ostermayr, Basil Karadais, Henrike Verfürth und ich, sowie alle unsere MithelferInnen – haben unser Bestes getan, dass man uns keine „Zitrone“ verleiht. Als einen Beweis dafür, dass Imaginary am Mathematischen Institut zu einem Erfolg geworden ist, werten wir die Reaktion der Besucher, die ihre Begeisterung im Gästebuch ausgedrückt haben, und die der Mitwirkenden, die festgestellt haben, dass trotz der Höhen und Tiefen der Organisation Imaginary ein echtes Erlebnis war. Natürlich haben sich nicht alle Besucher entschieden, Mathematiker zu werden, nachdem sie Imaginary oder die Wissenschaftstage besucht haben. Die Hoffnung ist aber, dass man dadurch Mathematik den Menschen näher gebracht hat und auf ihre Schönheit und Greifbarkeit aufmerksam gemacht hat.

Diana Ratiu

Mathematik – mitten im Leben
Die Münchner Wissenschaftstage 2008

Vogelperspektive (Bild Thorsten Naeser)

Ziel der Münchner Wissenschaftstage ist es seit acht Jahren, in der Öffentlichkeit, insbesondere bei jungen Menschen, Interesse, Verständnis und Begeisterung für Wissenschaft, Forschung und Innovationen, die dem Leben dienen, zu wecken. Die Veranstaltung steht im Rahmen der vom Bundesministerium für Bildung und Forschung ausgerufenen Wissenschaftsjahre, heuer also des vom Präsidenten der Deutschen Mathematiker-Vereinigung, Prof. Dr. Günter M. Ziegler (ehemals Student an unserer Fakultät) organisierten Jahres der Mathematik. So erklärt sich der Titel der diesjährigen Wissenschaftstage, „Mathematik – mitten im Leben“, die vom 18. bis 21. Oktober in den Räumen und Foyerflächen der LMU am Geschwister-Scholl-Platz stattfanden. Die Popularität der Mathematik führte dazu, dass der Zustrom größer war als in den Vorjahren; insgesamt kamen etwa 30.000 Besucher.

Unter der Konzeption durch den bienenfleißigen emeritierten Biologieprofessor Dr. Karl Daumer, einem Schüler von Nobelpreisträger Karl von Frisch, und der Leitung durch die nicht minder emsige Steffi Bucher fanden Vorträge mit Diskussion statt sowie Workshops, Filmvorführungen und Ausstellungen, darunter die auch in den Räumlichkeiten unseres Instituts gezeigte mit dem Titel „Imaginary“ aus dem Mathematischen Forschungsinstitut Oberwolfach. Höhepunkt war die Abendveranstaltung in der Aula, auf der der umtriebige Popularisator der Mathematik, Prof. Dr. Albrecht Beutelspacher aus Gießen, mittels topologischer Einsichten verschlungene Herzen aus einem simplen Papierband entstehen ließ und der scheidende bayerische Staatsminister für Wissenschaft, Forschung und Kunst, Dr. Thomas Goppel in einem launigen Gespräch mit Prof. Daumer das Landtagswahlergebnis und die Kabinettsbildung in statu nascendi erläuterte. Zuvor wurde der Minister von Prof. Dr. Rudolf Fritsch und dessen Frau Gerda mit einem originellen Dialog daran erinnert, dass während der gesamten 850-jährigen Geschichte Münchens die Mathematik als Kulturgut in der Stadt eine Rolle gespielt hat und dass in die wenigen Perioden der Vernachlässigung dieses Gutes auch der Wegfall des ältesten Mathematik-Lehrstuhls in Bayern vor wenigen Jahren fiel.

Das 900 Plätze bietende Audimax der LMU war während der 40 Vorträge stets gut besucht, mitunter sogar überfüllt. Neben auswärtigen Referenten und Sprechern verschiedenster Forschungs- und Lehrinstitutionen des Münchner Raums boten auch zwei Mitglieder des Mathematischen Instituts allgemein verständliche Einblicke in mathematische Sachverhalte hinter den Dingen des täglichen Lebens. Prof. Dr. Detlef Dürr zeigte in seinem Vortrag über *Kausalität, Zufall und Wahrscheinlichkeit*, wie sich unser Verständnis vom Zufall aus den Erklärungsproblemen physikalischer Phänomene entwickelt hat, die ja eigentlich auf regelmäßigen Naturgesetzen basieren sollten, aber leider (oder Gott sei Dank?) in einem untypischen, nämlich nichtgleichgewichtigen Universum stattfinden. Der Beweis der Universalität der Mathematik hätte gar nicht schöner erbracht werden können als mit der Tatsache, dass ein physikalisches Phänomen, die Brownsche Bewegung, und seine mathematische Beschreibung auch die Grundlage für das gängige Black-Scholes-Modell zur Ermittlung eines fairen Preises bei Optionsstrategien bildet, das von Prof. Dr. Francesca Biagini in ihrem Beitrag *Money out of nothing?* vorgestellt wurde, um Grundkonzepte eines effizienten Finanzmarktes darzustellen. Die mathematische Modellierung, meist mit stochastischen Methoden, von Strategien wie der Hedge-Strategie zeigt dessen Charakteristikum auf, nämlich die Unmöglichkeit, einen risikofreien Gewinn zu erzielen. Die folgenden Wochen sollten es jedem vor Augen geführt haben!

Guten Besuchs, ja manchmal geradezu eines Andrangs, konnten sich auch die beiden Marktstände erfreuen, die Mitglieder unseres Instituts dank des freiwilligen Einsatzes zahlreicher Studierender vier mal acht Stunden geöffnet halten konnten. Über den Stand *Mathe zum Anfassen* wird in diesem Heft an anderer Stelle berichtet. Der Beitrag *Türme säumen den Weg (von London nach Hanoi und zurück)* stellte ein Gemeinschaftsprojekt von Prof. Dr. Andreas M. Hinz mit der Arbeitsgruppe Kognitive Neurologie (Leitung: Prof. Dr. Adrian Danek) der Neurologischen Klinik am Klinikum Großhadern der LMU bereits zum zweiten Mal auf den Wissenschaftstagen vor, nachdem im Vorjahr, dem Jahr der Geisteswissenschaften, die Neuropsychologen federführend waren. Mathematik passt eben überall hinein!

Ziel des auf mathematischen Solitärspielen wie dem Turm von Hanoi (siehe mathe-lmu.de 4(2001), 20-25) basierenden multidisziplinären Forschungsprojekts ist die Entwicklung eines Pakets von Denkaufgaben, das zum Verständnis psychologischer Prozesse eingesetzt, aber auch spielerisch zum Hirnleistungstraining für Kinder und Erwachsene angewendet werden kann, wie dies jedermann auf dem Marktstand ausprobieren konnte. Gleichzeitig wurde das mathematische Modell vorgestellt, das auf Graphen basiert. Diese dienen schon seit langem zur Lösung oder Beschreibung von spielerischen Problemen wie dem bekannten Königsberger Brückenproblem oder dem in der Mitte des 19. Jahrhunderts in London auf dem Markt erschienenen Icosian Game mit seiner Frage nach einem an jedem von zwanzig Orten genau einmal vorbeikommenden Weg.

Das Projekt, das auch Teilnehmer(inn)en des Elite-Masterstudiengangs *Neurocognitive Psychology* der LMU einbezieht, zeigt die Nützlichkeit mathematischer Modelle in der Psychologie, die im Gegensatz z.B. zur Physik bislang vergleichbar wenig Gebrauch hiervon gemacht hat. Am Marktstand zeigte sich beim Publikum auch der Überraschungseffekt

Spieler (Bild Thorsten Naeser)

des „Du kannst mehr Mathe, als du denkst." (Motto des Jahres der Mathematik), wenn klar wurde, dass wir mathematische Graphen in Gestalt von U-Bahn-Netzplänen kennen und täglich zur Routenplanung nutzen. Durch das nachträgliche Betrachten des eigenen Lösungsweges erkannten die Versuchsteilnehmer sowohl psychologische Barrieren bei der Problemlösung als auch mathematische Methoden zu deren Analyse und begegneten dabei Themen der modernen Mathematik wie Optimierung und Graphentheorie.

Mathematik steht eben mitten im Leben!

Andreas M. Hinz

Das Mobile MatheLabor – unser Beitrag zu den Wissenschaftstagen

Da steckt Mathe drin? Diese Frage mit Überraschung und Neugier zu stellen kann oft der erste Schritt zu mathematischem Interesse und Verständnis sein. Dass mathematische Strukturen, auch abseits der Physik, mit Fragen und Antworten beliebigen Schwierigkeitsgrades in Situationen des Alltags stecken, ist vielen nicht unmittelbar klar – wird Mathematik doch leider häufig als etwas Weltfremdes wahrgenommen, das wenn überhaupt nur als Rechentechnik brauchbare Antworten liefert, aber ansonsten mit sich selbst beschäftigt ist. Dem die Faszination „Mathe“ gegenüberzustellen und spannende, teils sehr aktuelle Fragestellungen ohne großen mathematischen Überbau an die Schulen zu transportieren, war deshalb der Ausgangspunkt des *Mobilen MatheLabors (MML)* des Mathematischen Instituts, das bei den diesjährigen *Münchner Wissenschaftstagen* (18. – 21. Oktober) vorgestellt wurde.

Das Programm: An der Universität werden in Zusammenarbeit mit den Schulen mathematische Inhalte jenseits des Lehrplans in „mundgerechte“ Schulstundenkonzepte aufbereitet, gedacht für Projekt- oder Verfügungsstunden und über verschiedene Klassenstufen und Schulformen hinweg. Nach der Devise „Mathe zum Anfassen“ soll jedem Projekt ein realer Bezug zugrunde liegen und viel Zeit für selbstständiges spielerisches Entdecken vorgesehen sein. Konzept und nötiges Material dafür wird an der Universität bereitgehalten und kann kostenfrei von Schulen angefordert werden – auf Wunsch inklusive eines Referenten, der das Projekt vorstellt oder selbst eine Stunde abhält.

Das Echo in den ersten Schulstunden und während des 4-tägigen Standes auf den Wissenschaftstagen war durchwegs positiv. Dort konnten die Besucher, insbesondere Schüler und Lehrer, selbst ausprobieren, basteln, diskutieren, Fragen stellen und so die verschiedenen Projekte kennenlernen:


Polyeder und Fußball, gebastelt mit dem Bausatz

Dass Polyeder „uralte mathematische Objekte“ sind, würde kaum jemand bestreiten. Mittels eines Bausatzes konnten die Besucher solche nun frei selbst basteln. Dabei führte etwa die Systematik der platonischen Körper zu einigen „Aha“-Erlebnissen. Warum gibt es nur diese 5? Woher der mysteriöse Zusammenhang, wenn man Ecken, Kanten und Flächen von Dodekaeder, Ikosaeder und Fußball zählt (Dualitäten)? Auch die Eulersche Polyederformel (also Ecken - Kanten + Flächen = 2) konnte begeistern, zumal die Vermutung einiger Besucher, es handle sich um einen „Zahlentrick“, durch einen Torus-förmigen Polyeder leicht widerlegt werden konnte. Denn: die Euler-Charakteristik 2 liegt an der gemeinsamen „Kugelförmigkeit“ der Figuren – und hat einen starken Zusammenhang mit der „Kämmbarkeit“. Die Polyeder waren aber auch Anlass zu Diskussionen etwa über Symmetrien von Ornamenten und Kristallen.

Im Gegensatz dazu erschloss sich der mathematische Gehalt der ausgelegten Knoten dem Besucher meist nicht sofort. Wieviele verschiedene Knoten einer gegebenen „Größe“ gibt es? Kann man den Knoten entwirren oder in sein Spiegelbild verwandeln? Dafür war die Überraschung umso größer: Diese Fragen werden spätestens seit einem fehlgeschlagenen „Periodensystem auf Knotenbasis“ systematisch erforscht und sind durch die Entwicklung der polynomialen Knoteninvarianten teilweise geklärt. Dass es sich hier um ein verhältnismäßig explizites und dennoch „junges Stück Mathe“ handelt, an dem ausgiebig geforscht wird, schien insbesonders diejenigen zu faszinieren, für die Mathematik etwas „Altes“ und „Fertiges“ war. Mit besonders Interessierten konnten wir solche Knoteninvarianten am Stand sogar berechnen und das „Rätsel“ um die Ungleichheit zweier Knoten damit abschließend klären – auch dieses Thema erstreckt sich also von der Unterstufe bis in den Leistungskurs.

Screenshot einer Wie-Du-Mir-So-Ich-Dir-Strategie, die um ein gelegentliches zufälliges Entgegenkommen verbessert wurde. Rechts ist die Historie der vergangenen Spiel-Runden zu sehen.

Ähnlich erging es den meisten Besuchern beim Thema „Spieltheorie“. Dafür steht neben einer „Papier“-Fassung auch eine Internetplattform zur Verfügung, auf der das „Gefangenendilemma“ in Gruppen oder gegen virtuelle Gegner gespielt wird, wobei graphisch eine eigene automatisierte Strategie aufgebaut werden kann. So soll kritische Reflexion des eigenen Verhaltens, Abschätzung der Reaktionen des Gegners und „Algorithmisierung“ geschult und die Vorzüge mathematischer Modellbildung demonstriert werden. Weil die zugrunde liegenden zwischenmenschlichen Konflikte und intuitive Lösungsansätze so klar scheinen, waren die Besucher beeindruckt, wie schnell der richtige Blickwinkel mathematische Strukturen enthüllt: Schon so genannte „gemischte“ Strategien (also randomisierte Mischungen mit festen Wahrscheinlichkeiten) lassen sich im gemeinhin als mysteriös beäugten n-dimensionalen Vektorraum formulieren – und dies ist etwa für Existenzbeweise unabdingbar. Während das „Nash-Gleichgewicht“ durch die Kinos erstaunlich bekannt geworden ist, war den wenigsten klar, dass dies nicht nur deskriptiv zu verstehen ist, sondern durch Mathe auch systematische Vorteile erzielt werden können – etwa durch ein bestimmtes, zufälliges Abweichen von der „Wie du mir …“-Strategie oder ein „Charakterdiagramm“ aus bedingten Wahrscheinlichkeiten für die Reaktion des Gegners.

Des Weiteren gab es ein Projekt zu Strichcodes, sowie ein Computerspiel zum intuitiven Erkennen von Term-Gleichheiten. Alle Projekte sind auf der gemeinsamen MML-Homepage verfügbar (Mathematisches Institut, Jahr der Mathematik). Dort finden sich neben Kontaktdaten und den Powerpoint-Präsentationen des Standes zu jedem Projekt auch weitere Materialien, wie etwa das oben genannte Internetangebot zur Spieltheorie, sodass sich Besucher ein umfassendes Bild von Tiefe, Umfang und Schwerpunkten der jeweiligen Themen machen können.

Simon Lentner

Hochschule, Wirtschaft und zurück

Als ich gefragt wurde, ob ich einen Artikel für die Zeitschrift mathe-lmu.de des Fördervereins Mathematik in Wirtschaft, Universität und Schule an der Ludwig-Maximilians-Universität München e. V. über meine Karriere als Mathematiker schreiben möchte, war das ein guter Anlass, über die letzten doch schon fast 20 Jahre meines (Berufs-)Lebens mit der Mathematik etwas gründlicher nachzudenken.
Außerdem stellte sich mir die Frage, in wieweit sich meine Karriere von anderen Mathematiker-Laufbahnen unterscheidet und was da eigentlich den Leser interessieren könnte.
Eins gleich vorneweg, das besondere meiner Karriere, oder ich würde lieber meines beruflichen Lebenslaufs sagen, ist, dass ich tatsächlich immer mit Mathematik bzw. Statistik zu tun hatte. Dies gilt natürlich für die Zeiten an den Hochschulen, aber auch für meine Tätigkeiten in der Wirtschaft. Und die zweite Besonderheit ist, dass ich nach der Hochschule in die Wirtschaft ging, aber dann wieder zur Hochschule wechselte und dennoch weiter mit der Wirtschaft zusammenarbeite. Aber ich glaube, das muss ich etwas geordneter erläutern.

Wie hat das alles begonnen? Zunächst studierte ich bis zum Vordiplom an der Technischen Universität München Physik. Mathematik oder Physik? Ich sah da zunächst aufgrund meiner schulischen Erfahrungen keinen so großen Unterschied. Doch nach zwei Jahren des Physikstudiums war mir klar, dass mir die scheinbar unbegrenzten möglichen Modellierungen von Problemstellungen mit der Sprache der Mathematik viel näher waren als die physikalische Beschreibung der Welt. Vor allem die Beschreibung des Zufalls (Wahrscheinlichkeitstheorie) und die Zähmung des Zufalls (Statistik) sollten mich bis heute nicht mehr loslassen.

Wie ging es dann weiter? Ich wechselte zum Studium der Mathematik an die Ludwig-Maximilians-Universität München und spezialisierte mich auf mathematische Statistik. In diesem Bereich fertigte ich bei Herrn Prof. Dr. H. Pruscha am Lehrstuhl von Herrn Prof. Dr. P. Gänßler meine Diplomarbeit an und konnte dann, dank der Initiative von Herrn Pruscha, im Rahmen des Sonderforschungsbereichs 386 der Deutschen Forschungsgemeinschaft „Statistische Analyse diskreter Strukturen" mein Promotionsstudium beginnen. Durch die Erst-Betreuung der Dissertation am Mathematischen Institut durch Herrn Pruscha war ich mit der typischen mathematischen Arbeitsweise vertraut. Durch den Zweit-Betreuer Herrn Prof. Dr. L. Fahrmeier (dem damaligen Sprecher des SFB) und andere Kooperationen lernte ich aber auch das Institut für Statistik und die etwas anwendungsorientiertere Herangehensweise der Statistiker kennen.
Bei meinen Forschungsarbeiten standen die mathematische Basierung moderner statistischer Methoden im Mittelpunkt. Ich lernte, dass die Entwicklung und tatsächliche Anwendung von statistischen Methoden an Daten eine eigene, schwierige Aufgabe ist, die mathematisch exakte Fundierung der Verfahren ein anderer, ebenso schwieriger Bereich ist und die Kombination der beiden Bereiche wohl am schwierigsten ist.

Wann kommen die praktischen Anwendungen der Verfahren? Nach erfolgreicher Beendigung des Promotionsstudiums wechselte ich zur Allianz Versicherungs-AG in München.
Es war Zeit zu sehen, ob man all die modernen Verfahren und Modelle auch in der Realität verwendet. Ich hatte das große Glück, in der Aufbauphase eines Bereichs mitarbeiten zu können, der sich mit den Anwendungen von statistischen Verfahren auf Versicherungs- und Marketing-Fragestellungen beschäftigte. Das Themengebiet solcher Bereiche wird auch als Data Mining, Scoring oder Business Intelligence bezeichnet. Trotz einiger feiner Unterschiede handelt es sich hierbei in der Regel um die praktische Datenanalyse mithilfe von Verfahren aus der Statistik oder auch der künstlichen Intelligenz.
Dieselben Modelltypen, die ich noch vor kurzem in meiner Dissertation theoretisch beleuchtete, konnte ich jetzt auf echten Daten für echte Problemstellungen anwenden. Plötzlich stand die Realität der Daten mit fehlenden Daten, Datenfehlern, riesigen Stichprobenumfängen usw., die wirkliche betriebliche Anwendung der erstellten Modelle und die Software-technische Umsetzung der Verfahren im Fokus. Die große und spannende Herausforderung war es, die Welt der realen Daten und die Welt der theoretisch fundierten Verfahren erfolgreich zusammenzuführen und eine Akzeptanz der Modellierungen im Unternehmen zu schaffen.
Nach einigen Jahren war aus einem kleinen Team von Spezialisten ein eigenes Referat entstanden, das sich ausschließlich mit der Entwicklung und Umsetzung entsprechender Verfahren und unterschiedlichsten Modellierungen beschäftigte.
Ich wurde zum Leiter des Referats ernannt und hatte nun neben den fachlichen Tätigkeiten auch vermehrt Führungsaufgaben zu erfüllen.

Wo ist die Lehre geblieben? Diese Frage stellte sich nach einiger Zeit in der Wirtschaft. Ich hatte erst gar nicht bemerkt, dass mir die Lehrtätigkeit, die ich während meines Promotionsstudiums ausübte, doch sehr fehlte. Ich wollte gerne von meinem theoretischen Wissen und auch von meinen praktischen Erfahrungen etwas weitergeben. Außerdem fehlte mir, trotz der anspruchsvollen, mathematischen Themen in der Wirtschaft, etwas „bodenständige“ Mathematik, wie z.B. ein Vektorraum oder die komplexen Zahlen.
Eine Verbindung von praktischer Tätigkeit in der Wirtschaft und Lehrtätigkeit an einer Hochschule sollte es also jetzt sein. Allerdings ist so ein Vorhaben, meiner Meinung nach, aus verschiedenen Gründen gar nicht so leicht zu realisieren.
Zunächst ergab sich dank der Unterstützung von Herrn Dr. Rost und meinen Vorgesetzten in der Allianz Versicherungs-AG die Möglichkeit, zusätzlich zu meiner Tätigkeit in der Wirtschaft einen Lehrauftrag für Mathematik an der Hochschule München zu erfüllen. Dabei merkte ich jetzt so richtig, wie wichtig mir die mathematische, statistische Lehrtätigkeit ist und ich den Schwerpunkt meiner beruflichen Tätigkeiten wieder auf Forschung und Lehre legen möchte.
Im März 2003 erhielt ich einen Ruf für eine Professur für Mathematik an der Hochschule Rosenheim. Hier halte ich nun seit einigen Jahren Mathematik- und Statistik-Vorlesungen. Durch angewandte Abschlussarbeiten und Projekte mit Wirtschaftsunternehmen aus den unterschiedlichsten Bereichen habe ich auch weiterhin die Möglichkeit der prak-

tischen Anwendung mathematischer, statistischer Verfahren.
Abschließend möchte ich noch einmal auf die Tatsache zurückkommen, dass ich immer – auch in der Wirtschaft – mit mathematisch, statistischen Themen zu tun hatte. Dies ist für das breite Spektrum der Berufe, in die ein Mathematiker nach seiner Ausbildung gehen kann, nicht selbstverständlich und individuell vielleicht auch gar nicht gewollt. Für mich war das aber immer ein wichtiges Kriterium, ich wollte mit Mathematik bzw. Statistik arbeiten. An dieser Stelle sollte man erwähnen, dass hier die Rolle der angewandten Mathematik und Statistik entscheidend ist. Denn in diesen Gebieten findet man in der Wirtschaft vermehrt Bereiche, in denen man methodisch arbeiten kann.
Auch heute ist es für mich immer noch faszinierend, in welch unterschiedlichen Anwendungsgebieten (von Ingenieursthemen über wirtschaftswissenschaftliche Fragestellungen bis hin zur Versicherungs- und Finanzwirtschaft) man mithilfe der mathematischen, statistischen Sprache anwendungsorientiert mathematisch arbeiten kann.

Ulrich Wellisch

Rätselecke

Mit Hilfe der Kanten eines Würfels der Seitenlänge a lassen sich leicht drei paarweise windschiefe Geraden finden, deren Abstand jeweils a ist. Wer findet vier Geraden, die paarweise windschief sind und den Abstand a besitzen?

Max hat in einer Broschüre zum „Jahr der Mathematik 2008“ folgendes klassisches Rätsel gefunden:

$$\begin{array}{cccccc} & \mathrm{G} & \mathrm{A} & \mathrm{U} & \mathrm{S} & \mathrm{S} \\ + & \mathrm{R} & \mathrm{I} & \mathrm{E} & \mathrm{S} & \mathrm{E} \\ \hline \mathrm{E} & \mathrm{U} & \mathrm{K} & \mathrm{L} & \mathrm{I} & \mathrm{D} \end{array}$$

Dabei sollen die zehn Buchstaben in den Namen der drei Mathematiker so durch die Ziffern $0,\ldots,9$ ersetzt werden, dass die Rechnung (im Dezimalsystem) stimmt.

Ein hochrangig besetztes Gremium kümmert sich um wichtige Projekte, die es stets in dieselben sieben Arbeitsbereiche gliedert; bei jedem Projekt ist nun jedes der sieben Mitglieder für einen Bereich zuständig. Nach dem völligen Scheitern eines Projekts P wendet sich das Gremium dem nächsten Projekt Q zu, wobei jedes Mitglied diesmal einen anderen Arbeitsbereich als beim Projekt P übernehmen soll. Wie viele Möglichkeiten gibt es für die neue Aufgabenverteilung?

Lösungen zu den Rätseln von Ausgabe 18

Fünf äußerlich nicht zu unterscheidende Kugeln, die allerdings verschieden schwer sein können, sollen mit Hilfe einer Balkenwaage nach ihrem Gewicht geordnet werden. Wie ist dies mit nur sieben Wägungen möglich?

Die fünf Kugeln werden derart durchnummeriert, dass die ersten beiden Wägungen $K_1 \leq K_2$ und $K_3 \leq K_4$ sowie der direkte Vergleich der schwereren Kugeln in der dritten Wägung $K_2 \leq K_4$ ergeben haben; insgesamt ist also $K_1 \leq K_2 \leq K_4$. In diese Reihung lässt sich nun in zwei weiteren Wägungen die noch nicht berücksichtigte Kugel K_5 einordnen: dabei erfolgt zunächst der Vergleich mit der mittleren Kugel K_2 und danach im Falle von $K_5 \leq K_2$ mit der leichteren Kugel K_1 sowie im Falle von $K_2 \leq K_5$ mit der schwereren Kugel K_4. Entsprechend lässt sich in den beiden abschließenden Wägungen die Kugel K_3 in eine Reihung mit K_1, K_2 und K_5 bringen, so dass wegen $K_3 \leq K_4$ die Gesamtreihenfolge aller fünf Kugeln feststeht.

Die Zahlen von 1 bis 16 sollen so in das magische Quadrat eingetragen werden, dass die Summe über die vier Zeilen, die vier Spalten und die beiden Diagonalen sowie über die mit M bzw. A bzw. T bzw. H gekennzeichneten Felder identisch ist.

M	A	A	M
T	H	H	T
T	H	H	T
M	A	A	M

13	3	2	16
8	10	11	5
12	6	7	9
1	15	14	4

Max zeichnet n Punkte auf ein Blatt Papier, von denen keine drei Punkte auf einer gemeinsamen Geraden liegen, und verbindet je zwei dieser Punkte durch eine rote, blaue oder grüne Strecke, wobei keines der entstehenden Dreiecke drei gleichfarbige Seiten besitzt. Wie groß kann dann n höchstens sein?

Bei $n \geq 17$ Punkten sind unter den 16 von einem Punkt A ausgehenden Strecken wenigstens sechs von einer Farbe F_1; die zugehörigen Eckpunkte seien neben B auch $P_1,\ldots,P_5$. Ist eine der Strecken $[BP_1],\ldots,[BP_5]$ von der Farbe F_1, so gibt es ein F_1-farbiges Dreieck; ansonsten sind aber wenigstens drei dieser Strecken von einer Farbe F_2, wobei die zugehörigen Eckpunkte (bis auf Umnummerierung) P_1, P_2, P_3 sind. Ist nun eine der Strecken $[P_1P_2]$, $[P_2P_3]$, $[P_3P_1]$ von der Farbe F_1 oder F_2, so gibt es ein F_1-farbiges oder ein F_2-farbiges Dreieck; ansonsten sind alle drei Strecken von der Farbe F_3, so dass sie ein F_3-farbiges Dreieck bilden.
Damit ist $n \leq 16$. Im Höchstfall $n = 16$ lassen sich die Punkte mit $(x_1, x_2, x_3, x_4) \in \{0,1\}^4$ bezeichnen; die Strecke zwischen (x_1, x_2, x_3, x_4) und (y_1, y_2, y_3, y_4) werde durch $[z_1, z_2, z_3, z_4]$ mit $z_i = +$ für $x_i = y_i$ und $z_i = -$ für $x_i \neq y_i$ $(i = 1,2,3,4)$ charakterisiert. Färbt man nun die Strecken mit [+,+,+,-], [+,+,-,+], [+,-,+,+], [-,+,+,+], [-,-,-,-] rot, die Strecken mit [+,+,-,-], [+,-,-,+], [-,-,+,+], [-,-,-,+], [+,-,-,-] grün und die Strecken mit [+,-,+,-], [-,+,-,+], [-,+,+,-], [-,-,+,-], [-,+,-,-] blau, so besitzt keines der entstehenden Dreiecke drei gleichfarbige Seiten.

Fragen zu platonischen Körpern

In den Medien hört man immer wieder, dass sich Prominente mit ihrer mathematischen Unkenntnis brüsten und dem Fach fehlende Praxisnähe vorwerfen. Als Lehrer hingegen erlebe ich, dass Kinder oft von sich aus abstrakte mathematische Fragen aufwerfen und sich in deren Lösung verbeißen, ohne nach der unmittelbaren Anwendung zu fragen.

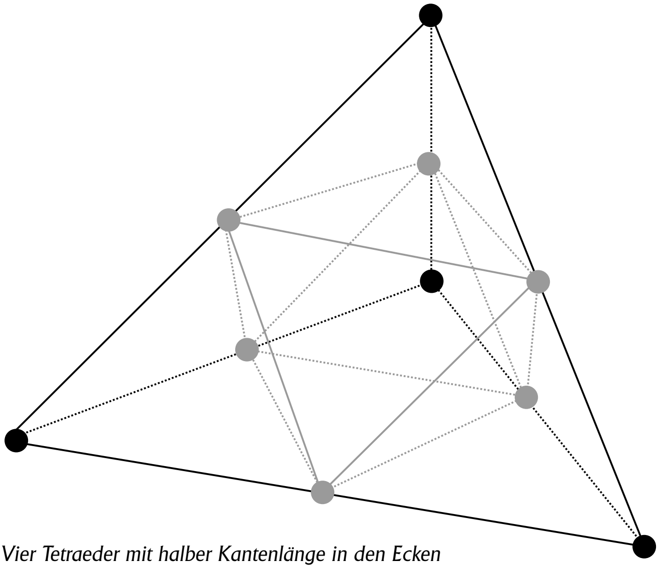
Am Rottmayr-Gymnasium Laufen wird allen Schülern der Unterstufe ein schulintern durchgeführter Mathematik-Wettbewerb, der so genannte „Rottfuchs“ angeboten. Er wird von einer Gruppe von Mathematiklehrern der Schule erarbeitet und in drei Runden pro Schuljahr durchgeführt. Die Schüler haben ca. zwei Wochen Zeit, die Aufgaben zu bearbeiten. Natürlich ist die Teilnahme freiwillig. In der 5. Klasse nehmen anfangs bis zu einem Drittel teil, in manchen Klassen auch niemand. Bei einigen Schülern merkt man, dass sie nur Lösungsversuche abgeben, um damit dem Lehrer zu gefallen. Manchmal ist sogar an der Handschrift erkennbar, dass nicht der Schüler die Aufgaben bearbeitet hat, sondern die Eltern. In der zweiten und dritten Runde lässt die Teilnahme nach.

Zwischen dem schulinternen Wettbewerb in der Unterstufe und dem Landeswettbewerb liegt eine große Kluft. Die Aufgaben für die Fünft- bis Siebtklässler, die neben den Grundrechenarten kaum mathematische Techniken verlangen, sind mit einer gewissen Ausdauer, der Fähigkeit zu logischem Denken und dem Vermögen, Überlegungen einigermaßen strukturiert zu Papier zu bringen, zu lösen. Bei den Aufgaben zum Landeswettbewerb sind schon viele Techniken aus dem Unterricht und aus Bereichen, die eher am Rande des Schulstoffs liegen, verlangt. Vor allem in der mathematisch sauberen Darbietung der Lösung, dem Erkennen, dass eine logisch erscheinende Schlussfolgerung eines korrekten mathematischen Beweises bedarf, liegen für die meisten, durchaus auch guten Schüler, Probleme.

Dass sich aber immer wieder Schüler auch gerne mit genau solchen Problemen auseinandersetzen, zeigt der Pluskurs Mathematik, der seit 14 Jahren – manchmal weniger, manchmal stärker besetzt – ununterbrochen angeboten werden kann. Natürlich geht es darum, besonders begabte Mathematiker zu fördern, doch ist es an einer Landschule generell schwer, Wahlunterricht über längere Jahre durchzuführen. Aber auch interessierte Schüler, die nicht als Mathematiker geboren sind, sind willkommen.

Die im Pluskurs behandelten Themen richten sich natürlich danach, aus welchen Jahrgangsstufen die Kursteilnehmer kommen. Im Schuljahr 2007/08 kamen außergewöhnlich viele, nämlich 20 Schüler aus den Jahrgangsstufen 5 bis 7. Als Thema für das erste Halbjahr wählte ich als Kursleiter „Die platonischen Körper“, letztendlich auch deshalb, um den schwächeren Schülern gewisse Erfolgserlebnisse beim Basteln von Körpern zukommen zu lassen.

Genauer berichten will ich von einer Stunde, die einen für den Kursleiter besonders interessanten, wenn auch nicht geplanten Verlauf nahm. Schüler bastelten unterschiedlich große Würfel und irgendwann kam die Frage, wie viele kleine Würfel denn in einen größeren Würfel mit doppelter Kantenlänge passen würden. Die ersten, weniger überlegten Antworten lauteten „Zwei“, dann „Vier“, bis schließlich schnell allen klar war, dass tatsächlich genau acht Würfel in einen Würfel doppelter Kantenlänge passen würden. Und jetzt kam die interessante Frage eines Siebtklässlers: „Kann man denn aus Tetraedern von z.B. 8 cm Kantenlänge einen Tetraeder mit doppelter Kantenlänge basteln?“, und nach kurzem Überlegen, „und wie viele kleine Tetraeder passen in den großen?“ (Glücklicherweise hat sich der Kursleiter die spontane Antwort „Na klar, acht!“ verkniffen). Keine Lehrerfrage hätte das Interesse der übrigen Schüler so wecken können wie das von dem Schüler aufgeworfene Problem. Relativ schnell stand fest, dass in jeder Ecke des großen Tetraeders jeweils ein kleiner liegen muss. „Und in den Hohlraum in der Mitte passt ein weiterer rein! Also: Fünf Tetraeder der Kantenlänge 8 cm passen in einen der Kantenlänge 16 cm.“ – „Nein, der Hohlraum in der Mitte ist größer. Da passen 2 kleine Tetraeder rein. Also: Sechs kleine passen in einen großen.“ „Wir probieren das einfach aus!“ Schnell wurden sechs Tetraeder von 8 cm Kantenlänge aus dünnem Karton gebastelt. Vier davon bildeten die „Ecken“ des großen Tetraeders. Und es war nach einigem Probieren klar, dass sich der Raum in der Mitte nicht vollständig mit weiteren kleinen Tetraedern ausfüllen lassen würde. Die Schüler überlegten weiter: „Welche Form hat der Raum in der Mitte?“ „Wir schauen uns die Begrenzungsflächen an, zeichnen das Netz und basteln ihn!“ Gesagt, getan und die Überraschung war groß – auch beim Kursleiter –, als sich dieser Restkörper als weiterer platonischer Körper, nämlich als Oktaeder, herausstellte.

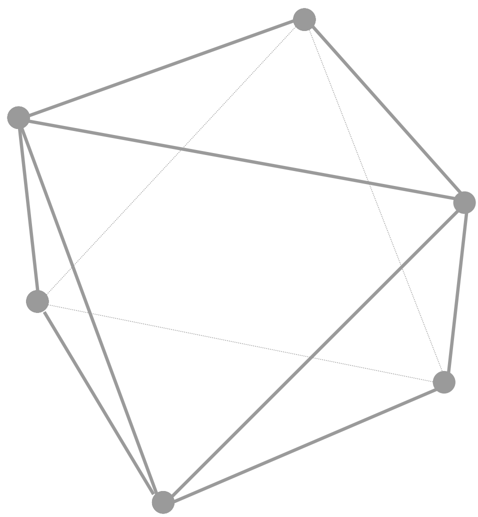


Vier Tetraeder mit halber Kantenlänge in den Ecken eines Tetraeders (Grafik von Dr. Joachim Georgii)

Für Schüler der Oberstufe kann dies als Motivation dazu dienen, durch Rechnung zu zeigen, dass ein Oktaeder das vierfache Volumen eines Tetraeders mit gleicher Kantenlänge hat.

Wenn dann auch noch in der Sprechstunde Eltern zu den platonischen Körpern nachfragen, bin ich vollauf zufrieden.

Mathias Gantner,
Rottmayr-Gymnasium Laufen



Schneidet man die Ecken weg, bleibt ein Oktaeder übrig.

Praktikum bei der Deutschen Bundesbank

Praktikum

Ein Praktikum zu machen kann ich nur empfehlen. Nicht nur, dass man später bei Bewerbungen gegenüber Studenten ohne Praktikumszeugnis einen Vorteil hat, man lernt vor allem, worauf das oft sehr theoretische Studium der Mathematik hinausläuft und wie man sein erworbenes Wissen praktisch anwenden kann. Da ich mich während meines Hauptstudiums auf den Bereich Finanzmathematik spezialisiert habe, erschien mir ein Praktikum bei der Deutschen Bundesbank in München für zwei Monate besonders sinnvoll. Der Unterschied zu anderen Praktika ist, dass man vor allem selbständiges und eigenverantwortliches Arbeiten lernt. Es gibt keinen Chef, der tagtäglich neue anspruchslose und auch sinnlose Arbeiten für Studenten hat. Ganz im Gegenteil!

Mein Praktikum lief so ab: Am ersten Arbeitstag erhielt ich ein Thema für meine Praktikumsarbeit, einen eigenen Computer mit Internetzugang und etwas Informationsmaterial, um mit der Materie vertraut zu werden. Der Titel meiner Arbeit lautete „Die Subprime-Krise: Eine empirische Analyse der Interdependenzen zwischen den verschiedenen volkswirtschaftlichen Teilmärkten“. Als Quellen hatte ich zuerst hauptsächlich das Internet zur Verfügung, allerdings merkte ich schnell, dass ohne Datensätze keine gute empirische Analyse möglich sein würde. Deswegen arbeitete ich mit der Zentrale in Frankfurt und mehreren Mitarbeitern der Stadtsparkasse München zusammen, um durch gegenseitigen Informationsaustausch beide Seiten zu begünstigen. In meinem Handeln hatte ich volle Freiheiten. Was zählt, ist die Praktikumsarbeit, die am Ende des Praktikums abgegeben werden muss.

Positiv zu erwähnen ist vor allem die Gleitzeit, die man als Praktikant nutzen kann. Anwesenheitspflicht herrscht bei der Deutschen Bundesbank jeden Tag von 9 Uhr bis 15 Uhr. Am Ende sollte man einen wöchentlichen Schnitt von 39 Arbeitsstunden erreichen. Wie man diese zusammenbringt, bleibt jedem selbst überlassen. So konnte ich mir die Zeit perfekt einteilen. Dies ist ein Plus zu vielen anderen Arbeitgebern, die Praktikanten diesen Luxus nicht zusprechen.

Unangefochten sind auch die angenehme Arbeitsatmosphäre und die netten Kollegen bei der Deutschen Bundesbank, die einem immer gerne mit Rat und Tat zur Seite stehen. Sei es in fachspezifischen Fragen, oder aber auch in Fragen, wo es zum Beispiel die besten „Leberkassemmeln“ in der Nähe gibt.

Da man als Praktikant der Deutschen Bundesbank dem öffentlichen Dienst angehört, kann man nicht nur die hauseigene Kantine nutzen, sondern auch mehrere andere wie zum Beispiel die des Landwirtschafts- oder des Finanzministeriums.

Abschließend kann ich jedem Mitstudenten nur empfehlen, auch ein Praktikum dieser Art zu machen, da man viel fürs spätere Berufsleben lernt und vor allem auch viele Sachen, die man in der Universität niemals erwähnen würde.

Peter Götzinger

Praktikum

Was ist ein Unternehmen wert?
Praktikumsbericht im Bereich Unternehmensbewertung bei PricewaterhouseCoopers

Während meines Auslandsemesters in Sydney im Sommersemester 2007 habe ich mich um eine Praktikumstelle bei PricewaterhouseCoopers im Bereich Advisory, Valuation & Strategy in München bemüht. Dieser Bereich ist für Unternehmensbewertungen, Finanzierungskonzepte und Ähnliches zuständig. Der Plan war, zügig nach meiner Rückkehr nach München ein wenig Praxisluft in den nachfolgenden Semesterferien zu schnuppern. Dafür habe ich mich zunächst online bei PwC beworben. Trotz einiger Telefonate bestanden meine Kontaktpersonen jedoch auf einem persönlichen Treffen. Deshalb vertrösteten sie mich auf die übernächsten Semesterferien und sagten mir, ich solle mich nach meiner Rückkehr persönlich vorstellen. Somit begann das Praktikum erst im März 2008.

Das Team von ungefähr 20 Leuten in meiner Abteilung war relativ jung, und fast die Hälfte der Mitarbeiter war seit maximal einem Jahr bei PwC. Sie alle waren stets hilfsbereit und freundlich und gaben mir das Gefühl, zum Team zu gehören. Insgesamt herrschte eine sehr positive Arbeitsatmosphäre.

Nun zum Fachlichen. Wie oben bereits angedeutet besteht ein Großteil des Aufgabenbereichs in dieser Abteilung aus der Bewertung von Patenten, Marken, Unternehmensteilbereichen, ganzen Unternehmen und auch kompletten Konzernen. Da ich nicht die volle Zeit über an ein einzelnes Projekt gebunden war, bekam ich einen Einblick in verschiedene Branchen mit den dazugehörigen Besonderheiten. So half ich unter anderem bei Projekten in der Textilbranche, der Baubranche oder auch im Landwirtschaftsbereich.

Es gibt verschiedene Verfahren für eine Unternehmensbewertung (oder auch Patent- oder Markenbewertung). Bei der Discounted Cash-Flow-Methode werden grob gesprochen die zukünftigen Erträge des Unternehmens auf einen Stichtag abgezinst und die Summe der Erträge ergibt dann den Unternehmenswert. Das Problem dabei ist, auf den ‚richtigen' Wert der zukünftigen Erträge zu gelangen. Dabei bestand meine Aufgabe zunächst aus viel Recherche. Ziel ist es, ein Gefühl für das Unternehmen zu bekommen. Was macht das Unternehmen? Wo ist das Unternehmen tätig? Was sind die Stärken und Schwächen des Unternehmens? Wie ist es im Vergleich zu Konkurrenten positioniert? Dafür beschäftigte ich mich viel mit Bilanzen, Gewinn- und Verlustrechnungen, Planrechnungen, Umsatzzahlen aller Art und Geschäftsberichten des Unternehmens, sowie seiner wichtigsten Konkurrenten. Auf den Vergangenheitsdaten aufbauend werden dann mit geeigneten Prognoseverfahren die zukünftigen Zahlungsströme (Umsätze, Kosten, Steuerzahlungen, …) abgebildet. Diese werden anschließend zur Berechnung der zu erwartenden Erträge verwendet.

Es sind also keine höheren mathematischen Kenntnisse erforderlich, die man nur durch ein Mathematikstudium bekommt. Vielmehr ist ein Gespür und eine gewisse Freude für den Umgang mit Zahlen vonnöten. Falls dann

noch das Interesse an wirtschaftlichen Konzepten und Zusammenhängen dazukommt, hat man die besten Voraussetzungen für ein Praktikum in diesem Bereich.
Zum Schluss noch ein paar Worte zu PwC: Als Arbeitgeber kann ich PwC nur empfehlen. Die Anzugspflicht gehört in diesem Bereich einfach dazu und wurde an den ‚casual fridays' sogar auf Jeans und Poloshirt oder Ähnliches gelockert. Des Weiteren gibt es viele positive Aspekte. Neben der schon angesprochenen angenehmen Atmosphäre bietet PwC ein vergleichsweise hohes Praktikantengehalt, die Möglichkeit, Vorträge von Mitarbeitern zu verschiedensten Themen zu hören oder auch nur Kleinigkeiten, wie ein Antritts- und Abschiedsgeschenk. Auch für das Mittagessen war gesorgt. Nachdem die hauseigene Kantine vor einigen Jahren geschlossen wurde, bekommt nun jeder Angestellte einen Essensgutschein von 5,60 Euro pro Tag, der in umliegenden Restaurants und Geschäften eingelöst werden kann.

Christoph Loy

Praktikum

Praktikum bei der Europ Assistance Versicherungs-AG

Nach meinem Vordiplom in Wirtschaftmathematik habe ich angefangen, mich nach einem Praktikumsplatz umzuschauen. Eines Abends, beim Internetsurfen, bin ich zufällig auf eine sehr interessante Stellenausschreibung der Europ Assistance Versicherungs-AG gestoßen. Gesucht wurden Studenten in Mathematik, Statistik und Informatik als Praktikanten für den Bereich Datawarehouse und Business Intelligence. Am gleichen Abend habe ich meine Bewerbung ausgearbeitet und per E-Mail verschickt und bekam bereits wenige Tage später einen Anruf von der Personalabteilung mit der Einladung zum Vorstellungsgespräch. Das Gespräch verlief ganz entspannt, wobei ich einiges über die Aufgabenbereiche der Abteilung und über das gesamte Unternehmen erfahren habe.

Die Europ Assistance Versicherungs-AG und ihre Services GmbH sind Unternehmen der Generali Versicherungsgruppe mit derzeit rund 170 Mitarbeitern. Neben der Vermarktung der eigenen Versicherungsprodukte und -leistungen steht für die Groß- und Privatkunden die Organisation weltweiter telefonischer Hilfeleistungen im Vordergrund. Die beiden Unternehmen stehen mit derzeit 71 weiteren Schwestergesellschaften in Kontakt. Die Europ Assistance liefert Dienstleistungen in fünf Kernbereichen: Automotive, Reise, Gesundheit, Haushaltsdienstleistungen und Dienstleistungen für Unternehmen.
Bei der Europ Assistance, die ihre Niederlassung in München-Schwabing hat, hatte ich bereits wenige Tage nach dem Vorstellungsgespräch meinen ersten Arbeitstag. Ich

wurde in der Abteilung Business-Intelligence und Datawarehouse eingestellt und hatte die Möglichkeit, Statistiken für die Analyse und Steuerung der Versicherungsprodukte im Unternehmen zu erstellen. Diese Statistiken dienten als Entscheidungsgrundlage für die externen Kunden sowie für die einzelnen Abteilungen im Unternehmen. Insbesondere unterstützte ich die Abteilung Controlling bei der Durchführung von Halbjahres- und Jahresabschlüssen durch die Erstellung automatisierter Reports, die beispielsweise die Kennzahlen wie Schadenquoten, Schadenhäufigkeiten, Durchschnittsschaden berechnen. Außerdem setzte ich die versicherungsmathematische Analyse für Großversicherer im Bereich Schadensmanagement um. Die Aufgabenbereiche waren sowohl sehr interessant als auch anspruchsvoll und ich bekam die Möglichkeit meine Kenntnisse aus den Versicherungsvorlesungen in der Praxis anzuwenden. Das Team griff mir bei Fragen und Problemen immer tatkräftig unter die Arme, ich fühlte mich immer wohl und das Arbeitsklima war sehr angenehm.

Nach dem Ablauf meines Praktikantenvertrages wurde mir angeboten, weiter bei der Europ Assistance in der Abteilung Business-Intelligence und Datawarehouse als Werkstudent für 12 bis 20 Stunden pro Woche zu arbeiten. Als ich mit meinem Wirtschaftsmathematikstudium beim Schreiben der Diplomarbeit angelangt war, hatte mein Chef interessante Ideen und Vorschläge bezüglich des Themas gemacht. Daraus hat sich ein Teil meiner Diplomarbeit, die über die statistischen Methoden für Seniorenunfall- und Lebensversicherungsprodukte handelte, entwickelt. Mit Hilfe statistischer Tools konnte ich die Daten bezüglich des Seniorenunfallprodukts im Zeitablauf auswerten und somit die Zeitreihenanalyse durchführen, die ein wesentlicher Bestandteil meiner praxisbezogenen Diplomarbeit wurde.

Meine Werkstudententätigkeit wurde durch die zahlreichen Firmenfeiern, Veranstaltungen und Partys ergänzt, wobei ich viele nette und interessante Leute kennen lernen durfte und neue Freunde gefunden habe.

Meine Tätigkeit bei der Europ Assistance Versicherungs-AG war eine sehr interessante Abwechslung zu dem abstrakten Studium der Mathematik. Ich würde es jedem Studenten empfehlen sich schon während des Studiums einen Einblick ins Berufsleben zu verschaffen.

Galina Gulenko

Mathematik und Geheimhaltung

Cornelius Greither

Wer sich von diesem Artikel eine gründliche Ausbildung in moderner Kryptographie erwartet, wird enttäuscht sein. Dem Autor geht es, von einer allgemeinen Einführung abgesehen, um eine detaillierte Fallstudie, die belegt, wie im Jahre 1932 die Mathematik eine entscheidende Rolle beim Brechen eines wichtigen Kryptosystems spielte. Die heutige Rolle der Mathematik in der Kryptographie wird am Schluss kurz erwähnt.

Wir beginnen mit der Frage: Was ist Kryptographie, was ist sie nicht? Die Grundaufgabe der Kryptographie geht aus folgendem Schema hervor.

$$
\begin{tikzcd}
\text{Klartext} \arrow[d, "\textit{Chiffrierung}"'] & & \text{Klartext} \\
\text{Chiffretext} \arrow[rr, "Kanal", "\textit{Sender} \to \textit{Empfänger}"'] & & \text{Chiffretext} \arrow[u, "\textit{Dechiffrierung}"]
\end{tikzcd}
$$

Es geht darum, Botschaften (Klartexte) so zu verschlüsseln, dass nur der oder die Empfänger in der Lage ist (sind), die Klarbotschaft herauszulesen. Die Übertragung erfolgt durch einen offenen Kanal, denn geheime Kanäle sind unrealistisch oder doch im Normalfall zu teuer (wir denken da etwa an Kurierdienste). Natürlich soll die Verschlüsselung sicher sein, aber nicht zu aufwendig. Wie in vielen anderen Situationen besteht ein Antagonismus Effizienz gegen Sicherheit; die Entscheidung hängt stark von der Situation ab, in der das kryptographische Verfahren zum Einsatz kommt. Staatsgeheimnisse müssen noch stärker geschützt werden als private E-mails.

Kryptographie kümmert sich nicht um die Details des Datentransports und die Reparatur von Übertragungsfehlern, die durch Kanaldefekte entstehen. Dies ist die Aufgabe der *Codierungstheorie.* (Dieser fundamentale Unterschied zwischen Kryptographie und Codierungstheorie ist auch manchen professionellen Mathematikern nicht klar bewusst.) Kryptographie ist auch nicht dasselbe wie Steganographie. Von Steganographie spricht man, wenn in einem offen sichtbaren Bild eine versteckte Botschaft enthalten ist, von deren Existenz fast niemand etwas weiß (vergleichbar einem toten Briefkasten: nur eine Person weiß, dass dort etwas zu finden ist). Ein Beispiel aus einem anderen Gebiet wären etwa die Notenfolgen A-F-F-E und (E)s-C-H-A-F-E in einem Stück von Max Reger. Er meinte damit seine Kritiker. Natürlich gibt es viele Musikstücke, die bedeutungsvolle Tonfolgen bewusst und als Programm verwenden (das bekannteste Beispiel ist wohl B-A-C-H).

Ein paar klärende Worte zur Terminologie: *Kryptographie* im engeren Sinne meint das Erfinden, Testen und Betreiben von Kryptosystemen, also von Verfahren zur Verschlüsselung und legalen Entschlüsselung von Texten. Unter *Kryptoanalyse* versteht man das Brechen von Kryptosystemen, also das Entziffern einzelner Nachrichten, ohne im Besitz des Schlüssels zu sein, oder realistischer, das Aufklären eines ganzen Kryptosystems, so dass man in die Lage kommt, *alle* mit diesem System chiffrierten Nachrichten lesen zu können. *Kryptologie* ist Oberbegriff zu Kryptographie und Kryptoanalyse; oft wird Kryptographie auch in diesem weiteren Sinn gebraucht, so auch in diesem Artikel.

Jedes Mal, wenn eine Verschlüsselung (Chiffrierung) stattfindet, wird ein Schlüssel verwendet. Die Schlüssel teilen sich aber in verschiedene Typen auf, je nach Verfahren. Ein *Kryptosystem* ist das Prinzip, nach dem chiffriert wird; der *Schlüssel* wählt ein ganz spezielles Verfahren aus vielen gleichartigen aus. Wir erklären das an einem Beispiel.

Gaius Iulius Caesar verwendete folgende Verschlüsselung, in der ein gegebener Klarbuchstabe immer durch denselben Chiffrebuchstaben verschlüsselt wurde:

$$a \to d, \quad b \to e, \quad c \to f, \ldots, \quad z \to c.$$

Diese Zuordnung ist eine sogenannte Permutation der Menge $A = \{a, b, \ldots, z\}$. (Eine Permutation ist eine bijektive Abbildung einer Menge auf sich selbst, d.h. zwei verschiedene Elemente werden auch verschieden abgebildet, und jedes Element kommt als Bild vor.) Diese Chiffriermethode lässt sich kurz und knapp mitteilen: verschiebe alle Buchstaben zyklisch um drei Plätze nach rechts. Eine beliebige Permutation von A lässt sich nicht so knapp mitteilen. Es gibt $26! = 403291461126605635584000000$ Permutationen von A, und im Allgemeinen muss man den kompletten Werteverlauf zur Spezifikation angeben. Caesars Permutation gehört zu einer ganzen Serie von Permutationen:

$$\begin{array}{ll}
\pi_0: & a \to a, \quad b \to b, \ldots, \quad z \to z; \\
\pi_1: & a \to b, \quad b \to c, \ldots, \quad z \to a; \\
\pi_2: & a \to c, \quad b \to d, \ldots, \quad z \to b; \\
\pi_3: & a \to d, \quad b \to e, \ldots, \quad z \to c; \\
\ldots &
\end{array}$$

Das Caesar-Kryptosystem besteht aus allen diesen 26 Permutationen; π_i ist zyklischer Rechtsshift um i Plätze. Der Schlüssel ist einfach die Zahl i, also 3 im historischen Fall. Die Verschlüsselungsabbildung kann man durch Angabe von i ganz leicht angeben, und die Entschlüsselungsabbildung ergibt sich auch leicht: der Umkehrschlüssel ist $-i$, oder $26 - i$, wenn man keine negativen Zahlen will. In Caesars Fall also 23.

Die Menge aller Caesar-Permutationen $\{\pi_0, \pi_1, \ldots, \pi_{25}\}$ ist eine Gruppe. In diesem Artikel reicht folgende Definition: Unter einer Gruppe verstehen wir eine Menge G von Permutationen auf einer festen Menge M, welche die identische Permutation enthält und unter Komposition von Permutationen abgeschlossen ist. Man kann dann zeigen, dass G auch unter Inversenbildung abgeschlossen ist (das liegt an der Endlichkeit von M; im Allgemeinen fordert man es einfach zusätzlich). Es gilt $\pi_i \pi_j = \pi_{i+j}$ und $\pi_i^{-1} = \pi_{-i}$.

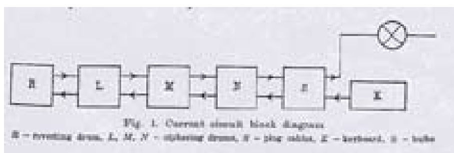
Es ist interessant, sich zu einem gegebenen Kryptosystem die Frage zu stellen, ob die involvierten Permutationen eine Gruppe bilden. Wenn das der Fall ist, dann bringt Überchiffrieren (zweimaliges Chiffrieren mit verschiedenen Schlüsseln) gar nichts, denn ebenso gut hätte man einmalig, mit der zusammengesetzten Permutation, die ja auch zum Kryptosystem gehört, chiffrieren können. (Die Maxime "viel bringt viel" trügt hier also.) Zweimaliges Chiffrieren kann nur dann sinnvoll sein, wenn die beiden Chiffrierungen zu verschiedenen Gruppen gehören. (Diese Idee wird bei den Private-Key-Systemen DES und AES systematisch genutzt.) Außerdem ist von Belang, dass es in Gruppen oft spezielle Algorithmen zur Ermittlung der Inversen gibt. Dies ist wichtig zur Ermittlung des Umkehrschlüssels.

Wir wollen uns hier mehr auf die Entzifferung (also die Kryptoanalyse) konzentrieren. Für alle Entzifferungen benötigt man eine Kombination aus systematischer Arbeit und einem "Einstiegspunkt". Bei der Entzifferung der ägyptischen Hieroglyphen durch Champollion war der Einstiegspunkt die Beobachtung, dass Königsnamen durch eine ovale Linie (genannt Kartusche) umschlossen sind; die Namen kannte man aus der griechischen Textversion. Kompliziertere Systeme chiffrieren nicht buchstabenweise; wir betrachten einen deutschen Marinecode von 1932, in dem ganze Wörter anhand eines Lexikons chiffriert wurden. Alle Chiffrewörter hatten vier Buchstaben. Der Hauptfehler des Codes war, dass die Chiffrierung die alphabetische Anordnung erhielt. Deshalb reichte ein und dasselbe Lexikon für Chiffrierung und Dechiffrierung aus. Die polnischen Mathematiker Rejewski, Różycki und Zygalski bemerkten, dass das erste Wort in vielen Depeschen mit Y begann. Oft ist das erste Wort ein Fragewort, Y sollte also W entsprechen. Es wurden zwei Funksprüche abgefangen. Der erste bestand aus 6 Wörtern; das erste war $YOPY$, also vermutlich ein Fragewort. Man vermutete, dass er zur Übung gedacht war, also ohne militärisch aktuellen Inhalt. Der kurz danach gesendete zweite Funkspruch hatte 4 Wörter; die Vermutung lag nahe, dass dies die Antwort war. Rejewski und Kollegen hatten die brillante Idee, dass die Antwort eine vierstellige Jahreszahl sein sollte, denn Zahlen wurden über die Ziffern als Wortfolge codiert. Also muss $YOPY$ “wann” bedeuten. Nach diesem “Einbruch” ergab sich die Lösung des Rätsels: *Wann wurde Friedrich der Große geboren? — Eins sieben eins zwei.* In der Folge wurde der ganze Code gebrochen.

Der zentrale Punkt dieses Artikels soll der Versuch sein, den mathematischen Hintergrund des ersten Durchbruchs gegen die ENIGMA zu erklären. Viele Details werden wir auslassen müssen. Die ENIGMA war von etwa 1926 bis 1945 im Einsatz bei der Wehrmacht, mit mehr als 100000 Exemplaren. Es war eine automatische Chiffriermaschine, die leicht zu bedienen war. Man musste anfangs gewisse Einstellungen vornehmen, genauer gesagt: drei Walzen in eine Position drehen. Der eigentliche Chiffriervorgang war simpel: wenn man eine Buchstabentaste drückte (andere gab es nicht), leuchtete ein kleines Feld mit einem Buchstaben auf, das war der zugehörige Chiffrebuchstabe.

Mit jeder festen Einstellung erzeugte die ENIGMA also eine gewisse Permutation π des Alphabets $\{a, b, c, \ldots, z\}$. Weil sich aber die Walzen regelmäßig weiterdrehten (wie ein Kilometerzähler im Auto), war die Permutation nicht konstant, sondern änderte sich fortlaufend. Die rechts liegende Walze drehte sich bei jedem Anschlag um eine 26stel-Drehung; die mittlere drehte sich, wenn die rechte eine komplette Drehung absolviert hatte (also bei jedem 26sten Anschlag), und die linke drehte sich, wenn die mittlere sich einmal ganz gedreht hatte, also bei jedem 676sten Anschlag.

Jede Walze bewirkte eine gewisse Permutation; sie wurde aber zweimal durchlaufen. Weitere Bauteile sind der so genannte Reflektor und die Eingangswalze. Schematisch:



Die Walzen hat man sich als flache Trommeln zu denken, die auf jeder Seite 26 Kontakte hatten. Die Kontakte der linken Seite waren durch Drähte auf irgendeine bijektive Weise mit den Kontakten der rechten Seite verbunden. Die Kontakte benachbarter Walzen berührten sich. Weil gewisse Bauteile der ENIGMA (Eingangswalze, Steckerbrett) den polnischen Kryptologen durch nachrichtendienstliche Informationen bekannt waren, erlauben wir uns hier, sie der Einfachheit halber ganz wegzulassen. Der Stromfluss in der ENIGMA kann also wie folgt veranschaulicht werden (wir nehmen an, dass auf Druck der Taste a die Lampe v leuchtet):

$$\begin{tikzcd}
\text{Walze L} \arrow[r] & \text{Walze M} \arrow[r] & \text{Walze N} \arrow[r] & v \\
& \text{Reflektor R} \arrow[ul] & & \\
\text{Walze L} \arrow[ur] & \text{Walze M} \arrow[l] & \text{Walze N} \arrow[l] & a \arrow[l]
\end{tikzcd}$$

Wir bezeichnen die durch L, M, N sowie R bewirkten Permutationen durch λ, μ, ν sowie ρ. Die Reflektor-Permutation ρ war immer selbstinvers (involutorisch), also $\rho^2 = id$ oder äquivalent hierzu $\rho = \rho^{-1}$. Dies war beabsichtigt, denn hieraus folgt, dass die von der Maschine verursachte Gesamtpermutation (wir nennen sie π) involutorisch war, und dies war sehr wichtig: Entschlüsselung und Verschlüsselung waren exakt derselbe Vorgang (bei gleichen Maschineneinstellungen), eine wichtige Vereinfachung für den Einsatz der Maschine unter schwierigen Bedingungen.

Wir wollen die Behauptung $\pi = \pi^{-1}$ auch mathematisch nachvollziehen. Im Gegensatz zum Üblichen schreiben wir die Komposition von Permutationen so, dass die später ausgeführte Permutation rechts steht. Wir verwenden obiges Schema; die Inversionen in der folgenden Formel kommen daher, dass die Walzen am Ende rückwärts durchlaufen werden:

$$\pi = \nu\ \mu\ \lambda\ \rho\ \lambda^{-1}\ \mu^{-1}\ \nu^{-1}.$$

Daraus folgt leicht

$$\begin{aligned}
\pi\pi &= \nu\mu\lambda\rho\lambda^{-1}\mu^{-1}\nu^{-1}\ \nu\mu\lambda\rho\lambda^{-1}\mu^{-1}\nu^{-1} \\
&= \nu\mu\lambda\rho\rho\lambda^{-1}\mu^{-1}\nu^{-1} \\
&= \nu\mu\lambda\lambda^{-1}\mu^{-1}\nu^{-1} = id.
\end{aligned}$$

Die wesentliche Schwierigkeit bei der Entschlüsselung der ENIGMA im Jahr 1932 war (abgesehen von den unbekannten Walzenverkabelungen) das ständige Weiterdrehen der Walzen (s.o.). Wir überlegen uns deshalb, wie die durch eine Walze gegebene Permutation sich beim Weiterdrehen ändert, und konzentrieren uns auf die rechte Walze, also die Permutation ν. Bezeichne σ den zyklischen Rechtsshift um eine Position. Jede Permutation kann als Produkt disjunkter Zyklen geschrieben werden, und es ist insbesondere

$$\sigma = (abcd \ldots z).$$

Nur zur Übung der Zyklenschreibweise führen wir an, dass

$$\sigma^2 = (ace \ldots y)(bdf \ldots z)$$

ist; wie man sieht, besteht σ^2 aus zwei disjunkten Zyklen der Länge 13.

Sei nun ν die durch die umgedrehte Walze N bewirkte Permutation, und ν' diejenige, die zur um eine Position gedrehten Walze gehört. Die gedrehte Walze liest sozusagen einen Input a als b, b als c usf.; ebenso wird Output b als a umgedeutet, c als b, und so weiter. Es ergibt sich also

$$\nu' = \sigma\, \pi\, \sigma^{-1}.$$

Ausdrücke der Form $\alpha\beta\alpha^{-1}$ kommen in der Gruppentheorie häufig vor. Man nennt dies Konjugation von β durch α, und kürzt es mit β^α ab. Es gelten viele praktische Rechenregeln für diese "Potenz". Wir wiederholen: $\nu' = \pi^\sigma$. Ebenso ist die Permutation der zweimal gedrehten Walze gleich π^{σ^2}, und so fort.

Es fragt sich natürlich: Was nützt das? Natürlich braucht man Beobachtungsmaterial, um einen Einbruch zu schaffen. Dieses Beobachtungsmaterial wurde letzten Endes geliefert durch einen Fehler der Chiffreure, die dachten "sicher ist sicher", und einen dreibuchstabigen so genannten Spruchschlüssel doppelt versandten. Wir erklären nun genauer, was hier passierte, und wie dies von Marian Rejewski ausgenützt wurde.

Die Walzenlagen waren immer einen ganzen Tag lang gleich. Es gab aber eine weitere Sicherungsmaßnahme, den so genannten *Spruchschlüssel*. Dies war eine Kombination von drei Buchstaben, etwa lmu, die am Anfang jedes Spruchs mit der festen Tageseinstellung **zweimal** übertragen wurde. Danach wurden die drei Walzen gemäß dieser drei Buchstaben verdreht (also im Beispiel um 11,12,20 Positionen), und erst dann wurde der eigentliche Funkspruch chiffriert und gesendet.

Weil die Walzenlage sich fortlaufend änderte, kam bei der Übertragung von $lmulmu$ keineswegs zweimal dieselbe Dreiergruppe heraus. Der Witz war aber, dass in jedem chiffrierten Spruch der erste mit dem vierten Buchstaben fest korreliert war, ebenso der 2. mit dem 5., und der 3. mit dem 6. Und das hatte eine einfache Erklärung! Zur Vereinfachung wollen wir, wie Rejewski, annehmen, dass sich während der ersten sechs Buchstaben **nur** die Walze N bewegte (die Aussichten dafür stehen 21:5). Mit $\pi_1, \ldots, \pi_6$ bezeichnen wir die von der Maschine beim Tippen des 1-ten bzw. ... 6. Buchstabens bewirkte Permutation. Keine dieser Permutationen war den Kryptologen bekannt.

Wenn aber etwa eine Depesche mit dem Anfang $bnh\ chl$ auftrat, dann wusste man: Wenn ξ der erste Buchstabe des Spruchschlüssels ist (den man nicht kannte!), dann ist $\pi_1(\xi) = b$ und $\pi_4(\xi) = c$. Daraus folgt:

$$(\pi_1\pi_4)(b) = \pi_4(\pi_1(b)) = \pi_4(\xi) = c.$$

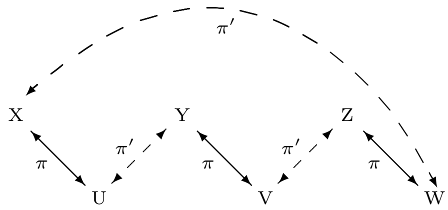
Wenn jeder Buchstabe an erster Stelle eines Spruchs im Laufe eines Tages auftrat, kannte man also die Produkt-Permutation $\alpha := \pi_1\pi_4$ komplett, und in ähnlicher Weise auch $\beta := \pi_2\pi_5$ und $\gamma := \pi_3\pi_6$. Andererseits hatte man vier unbekannte Permutationen λ, μ, ν, ρ, die auf komplizierte Weise in den π_i stecken.

Die Idee war, aus α, β, γ zunächst die sechs Permutationen $\pi_1, \ldots, \pi_6$ zu ermitteln. Bei Gleichungen mit reellen Zahlen kann das nicht gehen, denn drei Gleichungen mit 6 Unbestimmten ergeben normalerweise unendlich viele Lösungen. Hier ist die Situation aber anders: alle π_i sind selbstinvers, und obendrein ohne Fixpunkte. Die Anzahl dieser "strikt involutorischen" Permutationen ist nur 7905853580625 ($<< 26! \sim 4 \cdot 10^{26}$). Es gilt der

Satz: *Die Gleichung $\alpha = \pi\pi'$ hat außer in seltenen Ausnahmefällen höchstens hundert Lösungen in strikt involutorischen Permutationen π und π', und man kann für gegebenes α alle Lösungen mühelos explizit hinschreiben. Die Anzahl der Lösungen ist nur von der Zyklenstruktur von α abhängig.*

Die in diesem Satz verbleibende Mehrdeutigkeit eliminierte Rejewski im Wesentlichen durch die Beobachtung, dass die Chiffreure aus Bequemlichkeit nur sehr wenige Spruchschlüssel wirklich verwendeten. So waren aaa (später verboten), abc oder qay beliebt. Wir erklären den Satz an einem Beispiel, wobei wir umgekehrt vorgehen, nämlich durch Vorgabe von π und π'.

Seien X, Y, U etc. Variablen für Buchstaben. Sei $\pi X = U, \pi' U = Y, \pi Y = V, \ldots$ Hierdurch entsteht ein Zickzackmuster, von dem wir hier annehmen wollen, dass es sich nach drei Schritten schließt:



Folglich besteht $\pi\pi'$ aus zwei Dreierzyklen:

$$\pi\pi' = (X\ Y\ Z)(W\ V\ U).$$

Wenn die rechte Seite bekannt ist und $\pi X = U$, dann kann man laufmaschenartig π und π' zurückberechnen. Die obige Gleichung hat noch zwei weitere Lösungen in strikt involutorischen π, π', die aus den Startwerten $\pi X = V$ bzw. $\pi X = W$ entstehen. Etwas allgemeiner: In einem Produkt $\alpha = \pi\pi'$ treten Zyklen fester Länge k immer in Paaren auf. Wenn genau zwei k-Zyklen $(X_1 X_2 \ldots X_k)$ und $(U_1 \ldots U_k)$ auftreten, kann man einen Teil von π und π' ermitteln, indem man den zweiten Zyklus umdreht und unter den ersten schreibt:

$$\begin{array}{ccccccccc} X_1 & & X_2 & & X_3 & & \ldots & & \ldots \\ & U_k & & U_{k-1} & & U_{k-2} & & \ldots & \end{array}$$

Die einzige Unbestimmte ist die Phasenverschiebung. In Rejewskis Artikel [4] wird das Beispiel $\alpha = (dvpfkxgzyo)(eijmunqlht)(bc)(rw)(a)(s)$ angeführt. Die beiden Zweierzyklen $(bc)(rw)$ lassen nur die beiden Möglichkeiten $\pi = \ldots(br), \pi' = \ldots(cw)$ einerseits und $\pi = \ldots(bw), \pi' = \ldots(cr)$ zu. Die beiden Zehnerzyklen können in genau zehn Weisen zustande kommen. Insgesamt hat die Gleichung $\alpha = \pi\pi'$ genau 20 Lösungen in strikt involutorischen π, π'. Auf diese Weise (und durch Heranziehen von externen Informationen, sowie Plausibilität von Spruchschlüsseln) ermittelte Rejewski alle sechs Permutationen $\pi_1, \ldots, \pi_6$ aus den bekannten Permutationen α, β, γ (siehe oben).

Der (beinahe) abschließende Schritt ist nun die Ermittlung von ν, also der Verkabelung der ersten Walze. Dies ist wieder reine "Algebra mit Permutationen", aber komplizierter. Immerhin kann man die Hauptschritte hier darstellen. Wir bezeichnen jetzt den kumulierten Effekt der Walzen L, M und des Reflektors mit $\bar\rho$. Dies kann man sich als fiktiven Reflektor denken; die Maschine besteht nur noch aus der ersten Walze und einem fiktiven Reflektor. (Es ist $\bar\rho = \lambda\mu\rho\mu^{-1}\lambda^{-1}$; das Ziel ist aber, $\bar\rho$ ganz zu eliminieren.) Wir haben folgende drei Gleichungen:

$$\pi_1 = \nu\bar\rho\nu^{-1}, \tag{1}$$

$$\pi_2 = \nu^\sigma\,\bar\rho\,(\nu^{-1})^\sigma, \tag{2}$$

$$\pi_3 = \nu^{\sigma^2}\,\bar\rho\,(\nu^{-1})^{\sigma^2}. \tag{3}$$

Hierbei sind π_1, π_2, π_3 sowie σ bekannt und $\nu, \bar\rho$ sind unbekannt.

Durch Multiplikation von Gleichung (1) mit der mit σ^{-1} konjugierten Gleichung (2) bekommen wir eine Gleichung, wo links etwas Bekanntes steht (wir nennen es φ), und rechts steht $\nu\bar\rho\bar\rho^{\sigma^{-1}}\nu^{-1}$. In analoger Weise bekommen wir aus (2) und (3) eine Gleichung, in der links eine bekannte Permutation ψ steht und rechts $\nu\bar\rho^{\sigma^{-1}}\bar\rho^{\sigma^{-2}}\nu^{-1}$.

Setze $\xi = \bar\rho^{\sigma^{-1}}\bar\rho^{\sigma^{-2}}$. Dann ist

$$\psi = \xi^\nu, \quad \varphi = \xi^{\nu\sigma} = \psi^{\nu\sigma\nu^{-1}}.$$

Also gilt, noch einmal kurz hingeschrieben:

$$\varphi = \psi^{\sigma^\nu}.$$

Damit ist es endlich gelungen, $\bar{\rho}$ zu eliminieren: wir haben eine Doppel-Exponentialgleichung in der einzigen Unbekannten ν. Diese lässt sich zwar nicht eindeutig nach ν auflösen, wie im obigen Satz gibt es aber nicht allzu viele Lösungskandidaten. Die richtige Lösung muss wieder durch Versuch und Plausibilität bestimmt werden. Die Permutation ν beschreibt, wie gesagt, die Verdrahtung der “ersten” Walze N.

Weil Rejewski Daten aus den Monaten September und Oktober hatte, und am Quartalsende die Walzen N und M vertauscht wurden, konnte er auch die Verdrahtung der zweiten Walze M ermitteln. Der Rest ging danach verhältnismäßig einfach: das Kryptosystem ENIGMA war zu dieser Zeit (Dezember 1932) vollständig gebrochen. Die weitere Geschichte der ENIGMA ist äußerst komplex, und wir können nicht darauf eingehen, sondern nur auf [1] und [3] verweisen.

Zusammenfassend sei gesagt: Eine Kombination aus

- mathematischer Theorie,
- Beobachtungsgabe,
- Hilfe von Nachrichtendiensten,
- und Hartnäckigkeit

erlaubte es Rejewski, Różycki und Zygalski, die ENIGMA in den Jahren 1932-1939 zu brechen. (Durch die ständigen Änderungen an der ENIGMA seitens der Wehrmacht ging die Arbeit nicht aus.) Es spielte auch eine große Rolle, dass die beteiligten Kryptologen perfekt Deutsch konnten.

Die heute verwendeten Public-Key-Kryptosysteme, die wir hier auch nicht mehr behandeln können (siehe etwa [2]), verwenden schon in ihrem Design viel Mathematik (im Falle von RSA die Struktur von Restklassenringen $\mathbb{Z}/n\mathbb{Z}$ und ihrer Einheitengruppen), und sie sind nur mit Computerhilfe zu betreiben. Ihre Sicherheit beruht auf anerkannt harten Problemen der algorithmischen Zahlentheorie wie der Faktorisierung großer Zahlen. Die ENIGMA war ein Produkt von Einfallsreichtum und gutem mechanisch-elektrischem Handwerk; sie wurde durch Einsatz von Mathematik gebrochen. Es ist nicht klar, welche Wissenschaft den heutigen Kryptosystemen gefährlich werden könnte, die Mathematik alleine selbst wohl nicht, nach dem, was wir wissen. Sollte es jemals möglich werden, einen großen Quantenrechner zu bauen, so wäre RSA (und andere Systeme) allerdings höchst gefährdet; der Einbruch in die mathematisch basierten Kryptosysteme käme dann aus der Quantenphysik, unter Beteiligung der Mathematik. Im Moment sind diese großen Quantencomputer aber Utopie.

Literatur

[1] Friedrich Ludwig Bauer: Entzifferte Geheimnisse. Methoden und Maximen der Kryptologie. 3. Auflage. Springer, Berlin u.a. 2000

[2] J. Buchmann: Einführung in die Kryptographie. Springer-Lehrbuch, Springer 1999

[3] Marek Grajek: Enigma - bliżej prawdy. Rebis, Poznań 2007 (liegt noch nicht in deutscher Übersetzung vor)

[4] Marian Rejewski: An Application of the Theory of Permutations in Breaking the Enigma Cipher. Applicationes Mathematicae 16, No. 4, Warsaw 1980

Danksagung

Dieser Artikel beruht auf einem Vortrag, den ich im Rahmen der Münchner Wissenschaftstage am 21. Oktober 2008 gehalten habe. Ich danke den Veranstaltern der Wissenschaftstage, insbesondere Herrn Prof. Daumer und Frau S. Bucher, für die Gelegenheit zu diesem Vortrag und die perfekte Organisation.

Traineeprogramm
Bachelor of Arts
Bachelor of Science

Learning by Banking

Die BayernLB. Erfolgreiche deutsche Großbank mit starken Wurzeln. Wir sind Zentralbank der bayerischen Sparkassen, Hausbank des Freistaates Bayern – und geschätzter Partner von Unternehmen in Deutschland und in aller Welt.

Sie haben einen überdurchschnittlichen Abschluss in Wirtschaftswissenschaften oder Jura und bringen erste Praxiserfahrung im Finanzwesen mit? Sie sind engagiert und haben Spaß an der Dienstleistung? Dann haben Sie beste Voraussetzungen für die Aufnahme in unser Traineeprogramm. 15 Monate lang arbeiten Sie in einer international tätigen Großbank. In einem maßgeschneiderten Programm werden Sie dabei intensiv und individuell von uns gefördert – nach Ihren Fähigkeiten und nach Ihren Neigungen. Ihr Gewinn: Professionalität und eine faszinierende Berufsperspektive in der Welt der Wirtschaft.

Interessiert? Dann richten Sie Ihre Bewerbung an:

BayernLB
Corporate Center Bereich Personal
Nachwuchsentwicklung - 1631 -
80277 München

Telefon 089 2171-26952
trainee@bayernlb.de · www.bayernlb.de

Finanzgruppe Bayern

Bayern LB