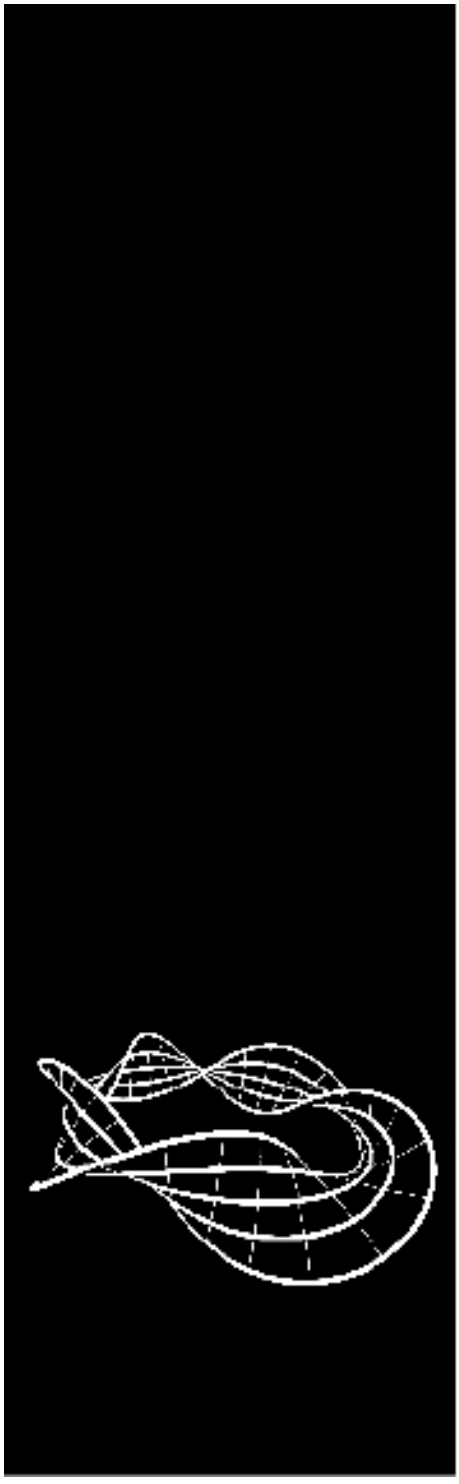


IMN

Internationale
Mathematische
Nachrichten
Nr. 190

Interview mit L. Vietoris
Faktorisierungsalgorithmen
CEIC: Best Current Practices
Das IMCC in Linz
Känguru der Mathematik

Österreichische
Mathematische
Gesellschaft

August 2002

Internationale Mathematische Nachrichten
International Mathematical News
Nouvelles Mathématiques Internationales

Die IMN wurden 1947 von R. Inzinger als „Nachrichten der Mathematischen Gesellschaft in Wien“ gegründet. 1952 wurde die Zeitschrift in „Internationale Mathematische Nachrichten“ umbenannt und war bis 1971 offizielles Publikationsorgan der „Internationalen Mathematischen Union“.

Von 1953 bis 1977 betreute W. Wunderlich, der bereits seit der Gründung als Redakteur mitwirkte, als Herausgeber die IMN. Die weiteren Herausgeber waren H. Vogler (1978–79), U. Dieter (1980–81, 1984–85), L. Reich (1982–83) und P. Flor (1986–99).

Herausgeber:

Österreichische Mathematische Gesellschaft, Wiedner Hauptstraße 8–10/1182, A-1040 Wien. e-mail *imn@tuwien.ac.at*, *http://www.oemg.ac.at/*

Bezug:

Die IMN erscheinen dreimal jährlich und werden von den Mitgliedern der Österreichischen Mathematischen Gesellschaft bezogen.
Jahresbeitrag: 18,– EUR (250,– ATS)

Bankverbindung: Scheckkonto Nr. 229-103-892 der Bank Austria AG, Zweigstelle Wieden, oder PSK Kto. Nr. 7823-950, Wien.

Eigentümer, Herausgeber und Verleger: Österr. Math. Gesellschaft. Satz: Österr. Math. Gesellschaft. Druck: Grafisches Zentrum, Wiedner Hauptstraße 8–10, 1040 Wien.

ISSN 0020-7926

Österreichische Mathematische Gesellschaft

Gegründet 1903

Sekretariat:

TU Wien, Wiedner Hauptstr. 8–10,
Inst. 1182, A-1040 Wien.
Tel. (+43)1-58801-11823

Vorstand des Vereinsjahres 2002:

H. Engl (Univ. Linz): Vorsitzender.
R. Tichy (TU Graz): Stellvertretender Vorsitzender.
M. Drmota (TU Wien): Herausgeber der IMN.
W. Woess (TU Graz): Schriftführer.
M. Oberguggenberger (Univ. Innsbruck): Stellvertretender Schriftführer.
W. Schachermayer (TU Wien): Kassier.
I. Troch (TU Wien): Stellvertretende Kassierin.

Vorsitzende der Landessektionen:

L. Reich (Univ. Graz)
M. Oberguggenberger (Univ. Innsbruck)
H. Kautschitsch (Univ. Klagenfurt)
J. B. Cooper (Univ. Linz)
P. Zinterhof (Univ. Salzburg)
H. Kaiser (TU Wien)

Beirat:

A. Binder (Linz)
H. Bürger (Univ. Wien)
C. Christian (Univ. Wien)
U. Dieter (TU Graz)
G. Gottlob (TU Wien)
P. M. Gruber (TU Wien)
P. Hellekalek (Univ. Salzburg)
H. Heugl (Wien)
E. Hlawka (TU Wien)
W. Imrich (MU Leoben)
M. Koth (Univ. Wien)
W. Kuich (TU Wien)
R. Mlitz (TU Wien)
W. G. Nowak (Univ. Bodenkult. Wien)
A. Plessl (Wien)
B. Rossboth (Wien)
N. Rozsenich (Wien)
H. Sorger (Wien)
H. Stachel (TU Wien)
H. Strasser (WU Wien)
G. Teschl (Univ. Wien): Web-Beauftragter.
H. Troger (TU Wien)
H. K. Wolff (TU Wien)

Mitgliedsbeitrag:

Jahresbeitrag: 18,– EUR (250,– ATS).

Bankverbindung: Kto. Nr. 229-103-892 der Bank Austria AG, Zweigstelle Wieden, oder PSK Kto. Nr. 7823-950, Wien.

Wir bitten unsere ausländischen Mitglieder, bei Überweisungen die Zweckbestimmung „Mitgliedsbeitrag“ anzugeben und den Betrag so zu bemessen, dass nach Abzug der Bankspesen der Mitgliedsbeitrag der ÖMG in voller Höhe zufließt.

http://www.oemg.ac.at/

Internationale Mathematische Nachrichten

International Mathematical News

Nouvelles Mathématiques Internationales

Nr. 190 (56. Jahrgang) **August 2002**

Inhalt

Das Titelblatt zeigt einen Ausschnitt aus einer Minimalfläche in der 3-Sphäre mit der quaternionellen Parametrisierung $f(u,v) = \exp(2iu)\cos(v) + j\exp(5iu)\sin(v)$. Die Fläche trägt eine einparametrige Schar von geodätischen Linien, und der gezeigte Ausschnitt ist ein Möbiusband. Zur Visualisierung wurde eine lineare Perspektvie aus dem konformen Modell $S^3 = \mathbb{R}^3 \cup \infty$ verwendet.

Internat. Math. Nachrichten
Nr. 190 (2002), 1–11

Video-Gespräch mit Leopold Vietoris*

Gilbert Helmberg

Universität Innsbruck

Herr Professor Vietoris, der Name „Vietoris“ klingt ja nicht ausgesprochen bajuwarisch. Kann man sagen, woher er kommt?

Ja, der Name „Vietoris“ ist ein sogenannter Humanistenname. Es gibt ein lateinisches Wort „viere“ – vieo, viere. Es heißt „binden’, und ein „vietor“ ist ein Binder, Fassbinder oder auch Korbflechter.

Und Ihre Familie kommt also woher?

Um das Jahr 1800 sind zwölf Vietoris nach Österreich eingewandert und von denen sind zehn wieder zurückgewandert. Zwei sind geblieben, und von einem davon stamme ich ab.

Sie sind geboren am 4. Juni 1891, das ist also vor hundertdrei Jahren und fünf Tagen, und zwar in Radkersburg. Sie haben aber dann nicht in Graz studiert, sondern in Wien?

Ja. Mein Vater war Ingenieur. Bei seiner Staatsprüfung – die sind ja öffentlich, die Staatsprüfungen – da war ein Kundschafter der Südbahn dort, um zu sehen, was für Leute ausgebildet werden. Wie mein Vater fertig war mit der Prüfung, ist der hingegangen zu ihm und hat ihn gefragt, ob er bei der Südbahn Ingenieur werden will. Mein Vater hat sofort angenommen. Und da hat er dann in Radkersburg mitgebaut an der Bahn von Radkersburg nach Luttenberg. Meinem Vater hat es bei der Südbahn nicht gefallen und da ist er zur Gemeinde Wien gegangen. Mein

*Niederschrift des am 9. 6. 1994 an der Universität Innsbruck, Fakultät für Bauingenieurwesen und Architektur, Institut für Mathematik, Institutsbereich Mathematik 1, geführten Video-Interviews. Das Gespräch mit Leopold Vietoris führte Gilbert Helmberg.
Kamera: Erwin Janka, Assistenz: Bernhard Schuster, Schnitt: Peter Rose, Klavier (J. S. Bach, Goldberg-Variationen): Norbert Riccabona.

ISSN 0020-7926

Vater hat beim Bau der zweiten Wiener Hochquellenleitung mitgearbeitet. Er hat dann ein Baulos gehabt von Böheimkirchen bis Preßbaum. Das hat begonnen im Jahr 1902. Da war ich gerade am Ende der Volksschule. Damals sind wir nach Scheibbs übersiedelt. Da war das Zentralbüro dieses Baues. Und da waren dann meine Eltern zwei Jahre in Scheibbs. Und damals im Jahre 1902 bin ich ans Gymnasium gekommen und zwar nach Melk ins Stift, und dort war ich acht Jahre.

Und dann haben Sie begonnen, zu studieren, aber nicht auf der Universität glaube ich?

Im Jahr 1910 hab' ich meine Matura gemacht. Mein Vater war Ingenieur, ich hab' nicht gewusst, was ich studieren soll. Da hat er gesagt, „Na, studierst halt auch Ingenieur!". Da bin ich an die Wiener Technik gegangen, nachdem ich die Darstellende Geometrie gelernt hab', aus dem Lehrbuch von Smolik-Heller. Das hat mir mein Vater gekauft, und daraus hab' ich die Darstellende Geometrie gelernt. Dann hab' ich die Aufnahmsprüfung an der Technik gemacht. Der Professor Müller hat das angeschaut und hat gefunden, es ist schon richtig, „aber wie kann man denn so schmieren", hat er gesagt. Dann hab' ich ihm meine Dreiecke gezeigt. Das waren so Kunststoff-Dreiecke, die den Graphitstaub anziehen und dann an das Papier abgeben.

Dann haben Sie also Mathematik auf der Universität. . .

Ja, da hab' ich also an der Technik den ersten Jahrgang Bauingenieurschule studiert. Außerdem habe ich schon damals Projektive Geometrie beim Professor Schmid gehört. Und das war natürlich für mich das einfachste jetzt, Mathematik und Darstellende Geometrie zu studieren. Da bin ich also im Jahr 1911 an der Universität inskribiert worden. Da waren der Professor Escherich, der Professor Wirtinger und der Professor Furtwängler. Die waren die drei Ordinarien. Dann hat es noch den Professor Kohn gegeben, Gustav Kohn, der hat Analytische Geometrie und überhaupt Geometrie gelesen, und auf diese Weise bin ich in die Geometrie gekommen.

Aber wie sind Sie dann zur Topologie gekommen?

Ich habe auch in den weiteren Jahren – nicht nur im ersten Jahr, im ersten Jahr war ich ordentlicher Hörer an der Technik, und in den weiteren Jahren war ich dann außerordentlicher Hörer an der Technik, hauptsächlich, weil ich bei Müller studiert hab', Darstellende Geometrie studiert hab' – in der Zeit habe ich auch eine Vorlesung von Rothe, Hermann Rothe, gehört, der nachher auch Professor an der Technik geworden ist, aber früh gestorben ist, leider früh gestorben ist. Bei dem habe ich auch Mathematik 1 gehört, der hat an der Tafel geschrieben, wenn man das fotografiert hätte jeden Tag, hätte man ein Buch gehabt, so sauber hat der geschrieben. Er hat sehr gute Vorlesungen gehalten. Und bei dem habe ich auch eine Sondervorlesung gehört in den späteren Semestern. Und da hat er gesagt: „Der Begriff der Mannigfaltigkeit ist noch nicht befriedigend definiert." Das

war für mich die Anregung, über diese Dinge nachzudenken. Natürlich habe ich die Topologie gebraucht dazu und die Mengenlehre. Da hab' ich bei Professor Groß – er war damals noch nicht Professor, sondern er war Dozent, er hat eine Vorlesung über Mengenlehre gehalten, eine dreistündige Vorlesung im Wintersemester 1913/1914. Und davon habe ich eigentlich meine ersten Kenntnisse über Topologie. Damals ist auch gerade das Lehrbuch von Hausdorff erschienen. Diesem Lehrbuch verdanke ich so wie alle Mathematiker der damaligen Zeit meine topologischen Kenntnisse.

Zu dieser Zeit hat doch der Weltkrieg begonnen, und der wird sich doch auch etwas störend für Ihr Studium bemerkbar gemacht haben?

Ja, natürlich. Im Jahr 1914 habe ich acht Semester gehabt, im August 1914 ist dann der Krieg angegangen, und ich war gerade im Endstudium für die Lehramtsprüfung. Dann bin ich eingerückt, und war dann fünf Jahre im Krieg, das letzte Jahr in Gefangenschaft.

Ich glaube, Sie sind ja auch einmal verwundet worden?

Ich bin im Jahr 1915 verwundet worden, und dann bin ich in Wien ausgeheilt worden. Und es war dann üblich, dass man wieder an den selben Kriegsschauplatz zurückgeschickt wird. Ich wollte aber an einen anderen Kriegsschauplatz, ich wollte ins Gebirge gehen. Damals hat unser Regiment drei Bataillone in Russland gehabt, ein Bataillon in Bosnien. Und da hab' ich mich zu einer Marschkompanie gemeldet, die, wie ich meinte, nach Bosnien gehen wird, ein Jahr früher, als ich hätte müssen nach Russland gehen. Das ist sehr dankbar angenommen worden, und ich bin also dann am Westbahnhof eingestiegen in den Zug, der uns wegführen sollte. Der ist aber nicht nach Bosnien gefahren, sondern immer nach Westen, Westen, Westen, Salzburg, zum Schluss sind wir in Meran auswaggoniert worden. Das war also im Februar – 1916, ja. Diese Marschkompanie in Meran hat dann einen Schikurs organisiert und zwar in Kurzras im obersten Schnalstal, auf 2000 Meter. Zu dem hab' ich mich natürlich sofort gemeldet – ich hab' noch nicht schifahren können. Und dann war ein dreiwöchiger Schikurs, und nach drei Wochen hab' ich noch nicht schifahren können. Man hat damals den Leuten nicht erklären können, wie man schifährt. Und dann war noch ein dreiwöchiger Kurs oben, den hab' ich nicht besucht. Und nachdem der aus war, bin ich noch einmal nach Kurzras gegangen, auf drei Wochen, schifahren. Und da ist ein Zdarsky-Mann gekommen, beim dritten Kurs war der Zdarsky-Mann da. Wie der gesehen hat, wie ich mich da plag', sagt er: „Da, hast den Stecken" – hat aus der Wiese so einen Pfahl ausgerissen, auf dem man das Heu aufhängt – „da hast den Stecken, jetzt werd' ich dir zeigen, wie man fahrt!" Und nach zwei Stunden hab' ich fahren können. Und da hab' ich dann alle Touren dort gemacht, wir waren zweimal auf der Weißkugel, auf der Vinailspitze, und auf noch anderen Gipfeln dort – wunderbare Sachen gibt's dort.

Im Jahr 1916 ist ja glaube ich Ihre erste Arbeit erschienen. Wie war das überhaupt möglich?

Ja, ich hab' ja bei Professor Müller Darstellende Geometrie studiert die ganze Zeit. Und da hab' ich schon von ihm – vielleicht 2 Jahre früher, vielleicht schon 1912 – eine Arbeit von Danzer in die Hand bekommen. Der hat über die Striktionslinie des Hyperboloids geschrieben und herausgefunden, dass diese Striktionslinie entsteht dadurch, dass man zwischen zwei bestimmten ebenen Schnitten des Hyperboloids den Mittelpunkt dieser Strecke zwischen den zwei Kegelschnitten sucht, und das gibt eine Kurve vierter Ordnung zweiter Art. Und der Müller hat mir die Aufgabe gestellt: „Schaun's amal nach, was überhaupt da herauskommt, wenn man zwischen zwei Kegelschnitten auf dem Hyperboloid, nicht nur den besonderen Kegelschnitten, die zu der Striktionslinie führen, sondern was herauskommt, wenn man überhaupt zwischen zwei Kegelschnitten, zwei ebenen Schnitten, die Mittellinie sucht, den Ort der Mittelpunkte." Na, ich hab' sehr bald gesehen, dass es allgemeiner geht. Dass man also – wenn man drei Kegelschnitte hat und auf den Erzeugenden einer Schar zu den drei Schnittpunkten nach einem gewissen Doppelverhältnis einen vierten Punkt konstruiert – dass dann eine Kurve vierter Ordnung herauskommt. Und dass jede Kurve vierter Ordnung zweiter Art auf unendlich hoch drei Arten auf diese Weise konstruiert werden kann. Und das hab' ich – das war also eine Seminararbeit bei Wirtinger, nein, bei Müller; die war ziemlich fertig, wie ich eingerückt bin. Und wie ich dann – dann hat es damals im Ersten Weltkrieg hat's sogenannte Studienurlaube gegeben. Und da hab' ich im Laufe meiner vier Jahre Dienstzeit dort zwei solche Studienurlaube gehabt. Und bei dem ersten Studienurlaub, das war im Jahr 1916, da hab' ich diese Arbeit fertiggemacht, und der Müller hat sie dann publiziert in der Akademie.

Im Jahr 1919 hatten Sie ja dann schon Ihre Dissertation fertig, glaube ich?

Ja, das war so: ich bin im Jahr 1915 verwundet worden. Und dann bin ich natürlich eine Zeit rekonvaleszent gewesen. In der Zeit habe ich einmal an der Arbeit geschrieben, und dann hab' ich auch sonst immer nachgedacht. Ich hab' ja großes Glück gehabt. Ich bin also nicht nach Russland das zweite Mal, sondern mit dem Zug nach Meran gefahren. Und hab' dann Dienst gemacht – ja da bin ich dann ausgebildet worden auf der Regensburger Hütte und auf der Berliner Hütte zum Militär-Bergführer. Und als solcher hab' ich dann später Dienst gemacht. Und da hab' ich ziemlich viel Zeit gehabt auch nachzudenken über meine Probleme. Und wie ich dann in der Gefangenschaft war, hab' ich mich hergesetzt und das zusammengeschrieben. Und dann bin ich mit einem fertigen Manuskript sozusagen im Jahr 1919 entlassen worden aus der Gefangenschaft. Literatur hab' ich verhältnismäßig wenig gebraucht für meine Arbeit, die hab' ich mir in einem zweiten Studienurlaub verschafft, und im Dezember 1919 hab' ich dann meine Dissertation eingereicht.

Unter dem Titel „Stetige Mengen", glaube ich?

Ja, stetige Mengen. Der Titel ist natürlich irgendwie sonderbar, aber es handelt sich natürlich um zusammenhängende Mengen. Aber der Begriff „zusammenhängend“ war damals noch besetzt vom „Zusammenhang“ im Sinne von Cantor. Und ich wollte diesen Sinn nicht aufgeben und hab’ gefunden: „stetig“, so wie ich mir’s vorstelle, ist genau die Dedekindsche Stetigkeit.

Bei wem haben Sie Ihre Dissertation eingereicht?

Der Pedell hat mich gefragt: „Bei wem reichen Sie . . . , wem sollen wir denn die Dissertation geben?“ Sag’ ich „Ja, . . . ?“ Sagt er Bei wem haben Sie denn die Dissertation gemacht?“ Sag’ ich „Die hab’ ich bei mir gmacht!“ Dann hat er halt die Dissertation übernommen und hat sie dem Wirtinger oder Escherich gegeben, und nach einer Weile hab’ ich eine Korrespondenzkarte gekriegt von Escherich, ich soll ihn besuchen. Und dann hat er mir gesagt, dass ihm die Dissertation sehr gut gefällt und dass in Graz eine Assistentenstelle frei ist, ob ich nach Graz als Assistent zu Professor Weizenböck gehen möcht. Da hab’ ich gsagt – habe ich gebeten um einen Tag Bedenkzeit, ich möchte mit meinem Vater darüber reden. Und mein Vater hat gefunden, „naja, mach das nur“. Dann habe ich also diese Stelle in Graz bekommen beim Professor Weizenböck.

In welcher Zeit waren Sie also in Graz?

Von 1920 bis 1922, und zwar in 1920/1921 war ich bei Professor Weizenböck Assistent, und da ist Weizenböck nach Amsterdam berufen worden, und an seiner Stelle dann Professor Baule berufen worden, da war ich ein Jahr bei Baule Assistent. Und dann bin ich nach Wien ans Mathematische Institut als Assistent gegangen.

Wie ist denn das zugegangen, dass Sie von Graz nach Wien gekommen sind; Sie haben sich ja auch habilitiert in Wien?

Na ja, als Student war ich in Wien natürlich bekannt bei den Professoren, bei Wirtinger, bei Furtwängler, die haben mich halt vorgeschlagen.

Und sie haben also einmal eine Nachricht bekommen, dass Sie eingeladen wurden, von Graz nach Wien zu gehen.

Ja, das hab’ ich natürlich angenommen.

Und in Wien waren noch andere Assistenten?

Ja, da war nur ein anderer Assistent, der Doktor Lense: wir zwei Assistenten für drei Professoren. Jeder Professor hat zwei Drittel Assistent gehabt.

Können Sie sagen, dass einer der damals in Graz oder Wien Lehrenden auf Sie besonderen Eindruck gemacht hat?

Na ja, den größten Eindruck hat für mich die Vorlesung von Privatdozent Dr. Wilhelm Groß gemacht. Der Groß ist leider Ende des – also nicht Ende – im Jahr 1917 an Typhus, der damals in Wien endemisch war, gestorben.

Als Sie nach Wien kamen, haben Sie dann Ihre Habilitationsschrift schon fertig gehabt oder haben Sie die erst in Wien geschrieben, und bei wem haben Sie sich habilitiert?

Ich glaube, die war sogar schon gedruckt. Die hat geheißen – na, wie hat denn die …

„Bereiche zweiter Ordnung“

Bereiche zweiter Ordnung, ja. Die, mein’ ich, war schon gedruckt.

Die haben Sie in Graz gemacht?

Die hab’ ich in Graz gearbeitet, ja.

Mit der haben Sie sich in Wien habilitiert, und dann haben Sie in Wien Vorlesungen selber gehalten.

Ja natürlich, nachdem ich habilitiert war, habe ich Vorlesungen gehalten über Mengenlehre, und da hab’ ich unter anderem den Felix Frankel gehabt als Hörer, der ist in Russland ein ziemlich bedeutender Topologe gewesen. Ich hab’ natürlich damals auch Vorlesungen bei den Professoren gehört, weil sie mich interessiert haben. Zum Beispiel hab’ ich viele Vorlesungen bei Furtwängler gehört, der war ja gelähmt. Ich mein’, es war Kinderlähmung oder so ‘was. Der hat müssen sitzend vortragen. Der ist gesessen, und irgendein Hörer hat müssen schreiben an der Tafel. Und ich hab’ viele Vorlesungen von Furtwängler auf diese Weise gehört, als Schreiber an der Tafel. Er hat also ziemlich flott gesprochen, und ich hab’ da geschrieben.

Wie ist Ihr Aufenthalt in Amsterdam zustande gekommen?

Der Professor Weizenböck war ja mein Professor in Graz. Der war in Amsterdam mit Brouwer sehr befreundet. Der Brouwer hat ja dort seine – na, wie soll ich sagen – da war ein Zentrum, Topologen-Zentrum, da sind also Alexandrov, Urysohn, dann ein gewisser Willison, so sechs, sieben Topologen waren dort schon eingeladen mit irgendwelchen Stipendien, und Weizenböck oder Brouwer haben gefunden, ich gehöre auch dorthin. Und da hat mir Weizenböck geschrieben, ob ich gehen will, kommen will. Ich hab’ natürlich angenommen, und da hab’ ich ein Rockefeller-Stipendium bekommen, das das Sommersemester 1925 und Wintersemester 1925/1926 gedauert hat. Und dann hat mir der Brouwer noch ein Semester verschafft, indem er mich als Assistenten angestellt hat. Nicht als Privatassistenten mit seinem Geld, sondern da war eine Assistentenstelle, die war frei, die hat er mir verschafft.

Können Sie sich erinnern, wer damals noch in Amsterdam als Professor oder Assistent war?

Na ja, als Professor war da noch der Mannoury. Der war auch ein Topologe. Der hat gar nicht so schlechte Sachen gemacht. Dann war der Professor Brouwer, und Weizenböck war auch, der hat aber keine Topologie getrieben. Und an Hörern war damals der Alexandrov – der Urysohn war schon gestorben, wie ich hingekommen bin. Er ist ja in der Ost... im atlantischen Ozean beim Schwimmen verunglückt. Dann war noch Hurewicz dort – nach mir erst, der Hurewicz ist erst nach mir gekommen, der Menger war dort, gleichzeitig mit mir ...

Haben Sie Menger nicht schon aus Wien gekannt?

Menger habe ich aus Wien gekannt, ja, nämlich, wie ich nach Wien gekommen bin von Graz, da war der Menger, ich meine, im dritten Semester. Er hat aber schon ziemlich viel gehabt von seiner Dimensionstheorie. Und damals war ungefähr meine erste Aufgabe, mit ihm seine Entdeckungen zu diskutieren.

Um diese Zeit, glaube ich, haben Sie ja auch mit Tietze zusammengearbeitet an seinem Enzyklopädie-Artikel?

Jaja, das war natürlich ... Damals hat Tietze auf Anregung von Felix Klein einen Artikel geschrieben über die verschiedenen Zweige der Topologie. Und die Fahnen dazu hat auch Klein bekommen. Der Klein hat sie dann an Brouwer weitergegeben, und der Brouwer war nicht recht zufrieden damit, und das ist auch dem Menger und dem Alexandrov bekannt geworden, und da war eine große Aufregung, dass da die Dimensionstheorie so schlecht behandelt ist. Und da war eine Versammlung, und in der Versammlung bin ich sozusagen verurteilt worden, als Mitarbeiter Tietzes ernannt zu werden und dafür zu sorgen, dass da die Dimensionstheorie ordentlich vorkommt. Der Klein war mit dieser ... der Brouwer hat das dem Klein vorgeschlagen, und Klein war damit zufrieden, und ich bin also jetzt dem Tietze als Mitarbeiter sozusagen aufoktroyiert worden. Mir war das sehr peinlich. Ich hab' mich nicht wehren können dorten in Amsterdam und hab' das angenommen. Der Tietze hat aber in seiner Gelassenheit das sehr gut behandelt. Ich hab' schon in ... bei einer ersten Zusammenkunft konnte ich schon sein Vertrauen gewinnen, und es hat sich dann ein sehr gutes Arbeitsverhältnis zwischen ihm und mir herausgestellt. Ich war auch eine Woche zum Beispiel bei ihm in München, wo wir miteinander gearbeitet haben. Da hab' ich bei ihm gewohnt, seine Frau hat sehr für mich gesorgt, und dann ist halt der Artikel unter dem Namen von Tietze und mir erschienen.

Tietze hat, glaube ich, auch in Wien studiert?

Aber lang vor mir.

... und war dann zu der Zeit, wo der Enzyklopädie-Artikel geschrieben wurde, in München...

... war Professor in München.

In Amsterdam, haben Sie da Deutsch oder Holländisch gesprochen?

Beides. Ich hab' sehr bald Holländisch gekonnt.

Brouwer hat ja vor allem den Intuitionismus begründet. Haben Sie damals mit dem Intuitionismus auch zu tun bekommen?

Naja, der Brouwer hat damals eine Vorlesung über intuitionistische Mathematik gehalten. Die haben wir alle, die wir dort auf Studium waren, besucht. Aber wer von ihnen, von uns da überzeugter Intuitionist geworden ist, weiß ich nicht. Ich nicht. Aber Brouwer hat mir das nie übel genommen.

Ich hab' einmal gehört, dass Brouwer doch ein eher schwieriger Mensch war. Haben Sie einen Eindruck von Brouwer gewonnen?

Ja, für mich war er nie schwierig. Er hat mich immer sehr gut behandelt.

Wenn Sie zurück denken an die Zeit, in der Sie in Wien studiert haben, in Graz gearbeitet haben als Assistent, dann in Wien als Dozent, und schließlich in Amsterdam als Forschungsmitarbeiter, kann man da irgendwelche wesentlichen Unterschiede in der Arbeit der Mathematischen Institute noch feststellen?

Nein, nein, ein Unterschied hat nur bestanden in der Größe der Institute, aber in der Arbeitsweise nicht.

Auch in Holland nicht?

Auch in Holland nicht, nein. In Holland haben zum Beispiel die Promotionen ... die waren sehr feierlich damals. Van der Waerden hat damals sein Doktorat gemacht, wie ich dort war. Ich war bei der Promotion von Van der Waerden dabei.

Haben Sie damals Ihre Forschungen aus Algebraischer Topologie begonnen, oder war das schon früher?

Ich hab' in Wien immer nur mengentheoretische Topologie getrieben und bin dann zur Erkenntnis gekommen, dass ich damit nicht weiterkomm'. Mir war klar, dass solche Dinge wie die Bettischen Zahlen, die Torsionszahlen und so weiter auch in allgemeineren Dingen als in den geometrischen Polynom-Polyedern – dass es das geben muß. Aber ich hab' nicht gewusst, wie man da dazu kommt. Und in Amsterdam ist mir durch Brouwer da ein Licht aufgegangen. Brouwer hat nämlich seine Topologie mit Hilfe des simplizialen Aufbaus seiner Untersuchungsobjekte gemacht, und dieser simpliziale Aufbau, der hat mir weitergeholfen.

Von Amsterdam sind Sie dann nach Wien zurückgekommen ...

Ja, und da hab' ich dann eine Vorlesung gehalten über Topologie. Da hatte ich die Ehre, den Professor Hahn als Hörer zu haben und den Dozenten Mayer. Auch der Felix Frankel, von dem ich zuerst gesprochen hab', war damals mein Hörer.

Und aus diesen Kontakten hat sich dann ergeben, was später Mayer-Vietoris-Sequenzen genannt wurde.

Jaja.

Aber Sie waren ja dann, glaube ich, fast nach Art eines Ping-Pong Balles einmal in Wien, einmal in Innsbruck, dann wieder in Wien, und schließlich doch in Innsbruck.

Ja. Ich bin im Jahre 1927 nach Innsbruck als Extraordinarius berufen worden. Im Jahr 1928 ist in Wien an der Technik eine Vakanz gewesen, und man hat mich gefragt, ob ich kommen will. Dann hab' ich geschrieben, ja, ich komm' gern wenn ich Ordinarius werde dabei. Dann hat mir der Professor Schmid, der damals diese Korrespondenz gemacht hat, geschrieben, jaja, ich werd' schon Ordinarius. Da bin ich also nach Wien als Ordinarius gegangen, und dann ist in Innsbruck wiederum die Lehrkanzel frei geworden, und ich hab' der Fakultät geschrieben, wenn sie mit mir zufrieden war und sie mich wieder berufen, dann werd ich gerne kommen. Und darauf bin ich wieder berufen worden.

Die Arbeiten, die Sie über die Mathematik des Bergsteigens gemacht haben, haben Sie dann als Professor in Innsbruck hauptsächlich geschrieben?

Ja. Nämlich, da war einmal eine Tagung – eine pädagogische Tagung für Mathematik oder – wie man das halt sagt – Mittelschullehrer haben in Salzburg getagt über Mathematik. Da hab' ich einen Vortrag über die Geometrie des Bergsteigens gehalten. Und der damalige Redakteur, der hat mich gleich eingeladen, dass er den Vortrag drucken will. Und da ist das dann erschienen.

Woher kommt Ihr Interesse für Block-Gletscher?

Ja, zuerst einmal bin ich mit den Gletschern in Bekanntschaft gekommen. Nämlich im Jahr 1930, wie ich zum zweiten Mal nach Innsbruck gekommen bin, da hat der Professor Finsterwalder, der damals – also der Gletscherforscher Finsterwalder, hat damals seine Arbeit übergeben an den Professor Schatz. Und ich bin dann mit Schatz Gletscher messen gegangen, sozusagen als sein Gletscherknecht, nicht wahr. Und da haben wir miteinander die Gletscher also dort vermessen, den Hintereis-Ferner, Vernagt-Ferner, Guslar-Ferner, Kesselwand-Ferner, Hochjoch-Ferner. Zum Blockgletscher bin ich gekommen dadurch, dass ich von der Universität für die Forschungsstelle in Obergurgl als Kurator bestellt worden bin. Da bin ich also nach Obergurgl gekommen, und dort hab' ich halt das Ding gesehen. Von dem Augenblick an hat's mich interessiert und hab' ich halt Untersuchungen gemacht.

Damals hat ja auch wieder eine sehr bewegte Zeit begonnen – die Zeit vor dem Krieg, die Zeit während des Krieges, die Zeit nach dem Krieg – die ganze Zeit über waren Sie an der Universität tätig. Haben Sie Erinnerungen daran, wie sich die Arbeit damals am Mathematischen Institut gestaltet hat?

Zunächst einmal stimmt's nicht, dass ich die ganze Zeit an der Universität war, sondern ich bin ja eingerückt. Ich bin am Beginn des Zweiten Weltkrieges eingerückt, und bin beim ersten Gefecht, das wir mitgemacht haben, schon verwundet worden. Ich bin dann zur Ausheilung nach Wien gekommen in ein Spital da in Lainz. Dann bin ich noch einmal mit einer Marsch … – na, wie hat man … – mit einer Tragtierkompanie an die Eifel gekommen. Und dort sind dann meine … – von dort aus bin ich dann beurlaubt worden für meine Arbeit an der Universität. Erst gegen Ende des Krieges hat man mich wieder geholt zur Heimatflak. Da sind wir nach … – das war in Rum, diese Heimatflak, und das war schon eine sehr ärmliche Sache.

Sie waren, glaube ich, bei Kriegsende oder nach Kriegsende Dekan, und wahrscheinlich war es doch schwierig, dann dafür zu sorgen, dass am Mathematischen Institut die Arbeit wieder aufgenommen wird in vollem Umfang?

Jaja. Damals habe ich erfahren, dass der Professor Radon arbeitslos ist. In Breslau war der Professor, das Breslau ist verloren gegangen gewesen, und der Radon war arbeitslos, und ich hab' mir gedacht, den werden wir jetzt berufen und hab' den Antrag gestellt, dass man den nach Innsbruck beruft. Da ist er nach Innsbruck gekommen, und von da ist er dann aber ziemlich bald nach Wien gegangen.

Eine mathematische Frage möchte ich Ihnen noch stellen: verschiedene Begriffe, die später in der Topologie eine große Rolle gespielt haben, sind explizit oder implizit in Ihrer Arbeit über „Stetige Mengen" schon enthalten. Ich glaube, es handelt sich um das Regularitäts-Axiom, um den Begriff der Kompaktheit, der von Ihnen, glaube ich, mit einem anderen Wort beschrieben worden ist …

Ja, das ist die … wie soll man denn sagen – nicht die gewöhnliche Kompaktheit, sondern es ist eine … wie nennt man das heute – ich hab's „lückenlos" genannt, der Alexandrov hat das, glaube ich, „vollkompakt" genannt, es ist also mehr als kompakt …

und der Begriff der „Filterbasis", den Sie glaube ich, anders genannt haben …

Ich habe das „Kranz" genannt, aber schon 15 Jahre bevor der … wie heißt denn das … bevor das in Frankreich gefunden worden ist.

Könnten Sie sagen, was Ihnen von Ihrer Arbeit die größte Befriedigung oder vielleicht auch die größte Enttäuschung bereitet hat?

Das ist sehr schwer. Das ist sehr schwer. Es fragt sich nur … man könnt' vielleicht fragen, welcher Lehrsatz mir am meisten Freude gemacht hat. Das ist viel-

leicht der Satz, dass jede Fußpunktkurve einer Regelfläche zweiten Grades eine Kurve vierter Ordnung zweiter Art ist und umgekehrt.

Das heißt eigentlich, wenn ich das richtig verstehe, dass Ihnen die Arbeit, mit der Sie eigentlich begonnen haben, die meiste Freude gemacht hat?

Jaja, kann man sagen; kann man sagen.

Gelegentlich wird die Meinung vertreten, naturwissenschaftliche Denkweise und Glaubenshaltung stehen miteinander im Widerspruch. Wie sehen Sie das?

Nein, von einem Widerspruch kann da gar keine Rede sein. Ich sehe in unserer Welt eine ganz überlegene Intelligenz wirken, diese Intelligenz ist nicht nur Intelligenz, sondern auch eine Tatkraft hat, und das ist für mich Gott; diese Intelligenz, diese tatkräftige Intelligenz.

Sie werden mit dieser Ansicht wahrscheinlich mit Ihrem ehemaligen Kollegen Professor Gröbner etwas in Widerspruch gelegen sein?

Ja, ja, aber wir waren trotzdem gut miteinander, sehr gut miteinander. Ich hab' mit ihm auch korrespondiert, schriftlich, aber ohne ihn bekehren zu können.

Sie nehmen ja immer noch Anteil am Geschehen an den Mathematischen Instituten in Innsbruck. Haben Sie sich auch ein Urteil bilden können über die universitäre Arbeit heutzutage oder wie Sie die Zukunft der Arbeit an der Universität in der Mathematik sehen?

Nein, da kann ich … da hab' ich kein Urteil. Ich staune nur darüber, dass so viele junge Leute so viele schöne Sachen machen. Aber – nicht wahr, ich bin ja mit meiner zweiten oder dritten Arbeit schon habilitiert worden. Heut' schreibt einer ja dreißig Arbeiten und ist noch nicht habilitiert. Ich bin dann nur dankbar dafür, dass ich überall so gut aufgenommen worden bin, dass man mir überall geholfen hat und dass ich überall viel gelernt hab'.

Herr Professor, ich danke Ihnen sehr für dieses Gespräch.

Bitte sehr.

Das Video-Interview im Leopold Vietoris ist das erste von bisher fünf Interviews, die von der ÖMG organisiert wurden. Neben Leopold Vietoris wurden Edmund Hlawka, Leopold Schmetterer, Wolfgang Schmidt und Harald Niederreiter interviewt. Demnächst werden die Kassetten – auch als Set – wieder angeboten werden.

Internat. Math. Nachrichten
Nr. 190 (2002), 13–36

Primzahltests und Faktorisierungsalgorithmen II

Johann Wiesenbauer

Technische Universität Wien

1 Einleitung

Wie schon erwähnt, war bereits Gauß die Entwicklung effizienter Methoden, „die Primzahlen von den zusammengesetzten zu unterscheiden und letztere in ihre Primfaktoren zu zerlegen“ ein Anliegen, und das Interesse an diesen Fragen hat heute im Zuge wichtiger Anwendungen in der Kryptographie sogar stark zugenommen. Nachdem der erste Teil dieses Artikels (s. [5]) ganz den Primzahltests gewidmet war, soll nun auch auf das Faktorisierungsproblem und den seit Gauß' Zeiten – teilweise aber auch schon vorher – erzielten Fortschritten bei seiner Behandlung eingegangen werden. Dabei kann man die zugrundeliegende Frage auch etwas einfacher stellen: Wie kann man von einer positiven ganzen Zahl N, von der man durch vorangegangene Primzahltests bereits weiß, dass sie zusammengesetzt ist, auf möglichst effiziente Weise nichttriviale Faktoren bestimmen? Indem man nämlich dieses Verfahren dann induktiv auf alle gefundenen Teiler – soweit nicht bereits Primzahlen – anwendet, kommt man natürlich sofort auch auf die Primfaktorzerlegung von N.

Obwohl das Faktorisierungsproblem für „große“ Zahlen – nach heutigen Maßstäben vesteht man darunter in diesem Zusammenhang Zahlen mit mindestens 150–200 Stellen – allgemein als schwer gilt und die Sicherheit wichtiger kryptographischer Verfahren, wie z.B. dem weitverbreiteten RSA-Verfahren, gerade auf dieser Annahme beruht, kann es doch entgegen einer weitverbreiteten Ansicht im Einzelfall auch für Zahlen dieser Größenordnung ganz einfach sein.

Ein Maß für die Schwierigkeit, ein konkret vorgelegtes zusammengesetztes N zu faktorisieren ist dabei die Größe des zweitgrößten Primfaktors von N. Ist dieser relativ klein, so können durch Anwendung verschiedener Faktorisierungsme-

ISSN 0020-7926

thoden, deren Aufwand, wie wir noch sehen werden, in der Regel stark von der Größe des jeweiligen kleinsten Primfaktors abhängt, sukzessive alle Primfaktoren von N bis zum zweitgrößten „ausgesiebt“ werden. Die Primalität des zum Schluss verbleibenden Kofaktors kann aber, wie wir im ersten Teil schon bemerkt haben, mit Hilfe moderner Primzahltests auch bei Zahlen mit mehr als tausend Stellen noch relativ leicht überprüft werden. Nicht ohne Grund wählt man daher bei dem erwähnten RSA-Verfahren den Modul N so, dass er das Produkt etwa gleich großer Primzahlen p und q ist, womit dann der zweitgrößte Primfaktor etwa die Größenordnung von $\sqrt{N}$ hat, d.h. so groß wie möglich ist.

2 Heuristische Betrachtungen zur Größe von Primfaktoren einer Zahl

Im Hinblick auf die eingangs angestellten Betrachtungen kommt also folgender Frage große Bedeutung zu: Wie groß ist „typischerweise“ der größte und zweitgrößte Primfaktor einer großen Zufallszahl N? Wie hoch ist allgemein die Wahrscheinlichkeit, dass der größte Primfaktor von N (und damit dann natürlich auch jeder andere!) unterhalb einer gewissen Schranke B liegt, dass also N, wie man auch sagt, „B-glatt“ ist?

Für die nachfolgenden heuristischen Überlegungen nehmen wir an, dass die absteigende Kette $P_1 > P_2 > \cdots > P_s$ aller verschiedenen Primfaktoren von N in einer für Zahlen dieser Größenordnung „typischen“ Weise abnehme. Da ganz allgemein nach einem Satz von Erdős-Kac die Anzahl der verschiedenen Primfaktoren einer Zahl N asymptotisch normalverteilt mit Mittel und Varianz $\log\log N$ ist, dürfen wir also dann $s \approx \log\log N$ annehmen.

Wir setzen nun $q_1 := (\log P_1)/(\log N)$, was man auch als „Stellenanteil“ von an der Stelligkeit von N interpretieren kann, und versuchen q_1 näherungsweise zu berechnen. Dazu verwenden wir, dass die Zahl N/P_1, für welche dann die entsprechende Primfaktorkette $P_2 > \cdots > P_s$ ebenfalls in einer „typischen“ Weise abnimmt, gerade einen Primfaktor weniger als N hat. Dies führt auf die Gleichung

$$\log\frac{1}{1-q_1} = \log\left(\frac{\log N}{\log N - \log P_1}\right) = \log\log N - \log\log\frac{N}{P_1} \approx s - (s-1) = 1,$$

aus der sich dann nach leichter Rechnung $q_1 \approx 1 - \frac{1}{e} \approx 0.632$ ergibt. Daraus errechnet sich aber auch der Stellenanteil $q_2 := (\log P_2)/(\log N)$ des zweitgrößten Primfaktors P_2 von N ebenfalls näherungsweise wie folgt:

$$q_2 = \frac{\log P_2}{\log N} = \frac{\log P_2}{\log(N/P_1)}\left(1 - \frac{\log P_1}{\log N}\right) \approx q_1(1-q_1) \approx 0.233.$$

Eine genauere Rechnung unter Verwendung von sog. polylogarithmischen Funktionen (s. [4]) würde zeigen , dass die „echten“ Erwartungswerte, nämlich $q_1 \approx 0.624$ bzw. $q_2 \approx 0.210$, nur geringfügig von den oben berechneten abweichen.

Bei vielen im folgenden betrachteten Faktorisierungsproblemen erweist sich ferner als bedeutsam die Funktion $\psi(x,y)$, welche die Anzahl der y-glatten Zahlen $\leq x$ angibt, wobei hier x und y positive reelle Zahlen mit $y \ll x$ sind. Man kann dabei allgemein zeigen, dass gilt

$$\psi(x,y) = xu^{-u(1+o(1))},$$

wobei $u = (\log x)/(\log y)$. Insbesondere ist also

$$\frac{x}{\psi(x,y)} \approx u^u,$$

wobei diese Größe insofern bedeutsam ist, als sie eine mehr oder weniger gute Näherung für die Anzahl von zufällig ausgewählten ganzen Zahlen „in der Umgebung von x“ angibt, die man betrachten muss, bis man auf eine y-glatte Zahl stößt. In manchen Komplexitätsanalysen werden eigentlich „y-potenzglatte“ Zahlen in der Nähe von x benötigt, für welche allgemeiner alle Teiler in Form einer Primzahlpotenz y nicht übersteigen, doch unterscheidet sich deren Häufigkeit, wie man sich leicht überlegen kann, nur unwesentlich von der für y-glatte Zahlen, sodass obige Formeln dann auch auf sie angewendet werden können.

3 Abspaltung kleiner Primteiler durch Probedivision

Bevor eines der aufwändigeren Faktorisierungsverfahren zur Anwendung kommt, wird man natürlich die vorgegebene natürliche Zahl N daraufhin untersuchen, ob sie „kleine“ Primteiler hat, d.h. Primteiler unterhalb einer gewissen vorgegebenen Schranke B. Dies wurde ja auch schon vor Primzahltests so gemacht, doch darf hier B wegen des im Allgemeinen höheren Aufwands von Faktorisierungsmethoden schon etwas größer sein, also z.B. $B = 10^5$ oder $B = 10^6$.

Die Wahrscheinlichkeit, dass eine große Zufallszahl N überhaupt keine Primteiler $p \leq B$ besitzt, kann unter Benützung eines Satzes von Mertens recht gut durch

$$\prod_{p \leq B} \left(1 - \frac{1}{p}\right) \sim \frac{e^{-\gamma}}{\log B} \approx \frac{0.5615}{\log B}$$

abgeschätzt werden, wobei hier p alle Primzahlen $\leq B$ durchläuft und $\gamma \approx 0.5772$ die Eulersche Konstante bezeichnet. Für $B = 10$ beträgt daher die Wahrscheinlichkeit eines totalen Misserfolgs der Probedivision etwa 4.06% und sie wird natürlich noch kleiner, wenn wir N als zusammengesetzt voraussetzen. Hier wieder ein einfaches Derive-Programm dazu:

```
trialdiv(n, b := 10^6, p_ := 2, t_ := 1) :=
    Loop
        If p_ > b
            RETURN FACTORS(t_)
        If MOD(n, p_) = 0
            Prog
                t_ : ·p_
                n : /p_
                If n = 1
                    b := 1
            p_ :=NEXT_PRIME(p_)

(r :=RANDOM(10^100)) =
        344417073898235039670003368420512313000276010387 95
        861615726705492365757173067203293166269756521 6976

trialdiv(r) = [[2,4],[3,1],[811607,1]]        (13.9 s).
```

In dem angeführten Beispiel werden für eine zufällig generierte 99-stellige Zahl die Primfaktoren $< 10^6$ zusammen mit ihren Vielfachheiten ausgewiesen.

Bei Zahlen spezieller Bauart ist es oft der Fall, dass auf Grund allgemeiner Sätze viele Teiler von vornherein ausgeschlossen werden können. So gilt etwa der folgende

Satz (Legendre). *Sei N von der Form $a^n \pm b^n$ mit* $\mathrm{ggT}(a,b) = 1$*, so erfüllen die primitiven Primteiler p von N, d.h. die Primteiler von N, welche nicht zugleich Primteiler von $a^m \pm b^m$ für einen echten Teiler m von n sind, die Bedingung $p \equiv 1 \bmod n$, bzw. sogar $p \equiv 1 \bmod 2n$, falls p und n beide ungerade sind.*

Obiger Satz kann mit $a = 2$ und $b = 1$ insbesondere auf die schon im ersten Teil dieser Arbeit oft für Beispielzwecke betrachteten Fermatschen Zahlen $F_m := 2^{2^m} + 1$ bzw. Mersenneschen Zahlen $M_p := 2^p - 1$ $(p \in \mathbb{P})$ angewandt werden, wobei in diesen Fällen, wie man leicht zeigen kann, sogar jeder Primteiler primitiv ist. Für eine Fermatsche Zahl F_m folgt daher aus obigem Satz, dass alle ihre Primteiler die Form $k2^{m+1} + 1$ haben müssen, während die Primteiler einer Mersenneschen Zahl M_p von der Form $2kp + 1$ sind, wobei hier allerdings $p \neq 2$ sein muss. Tatsächlich lässt sich diese Aussage nicht nur auf beliebige Teiler der betrachtenen Zahlen ausdehnen, sondern unter Zuhilfenahme von Sätzen über quadratische Reste sogar noch dahingehend verschärfen, dass die Teiler von F_m $(m \geq 2)$ sogar die Form $k2^{m+2} + 1$ haben müssen, während man für das k in der Darstellung $2kp + 1$ eines Teilers einer Mersenneschen Zahl M_p $(p \in \mathbb{P} \setminus \{2\})$ die sich aus der Bedingung $2kp + 1 \equiv \pm 1 \bmod 8$ ergebende einschränkende Aussage $k \equiv 0 \bmod 4$ oder $k \equiv -p \bmod 4$ machen kann.

Die nachfolgende Routine fteiler(m) berechnet den kleinsten Teiler > 1 einer Fermatschen Zahl F_m $(m \geq 2)$. Seine Ausgabe erfolgt dabei in der übersichtlichen Form $k2^{m+2}+1$, die ein Ablesen des Werts von k ermöglicht. Um den nächstgrößeren Teiler zu bekommen, muss dieser Wert von k als zweiter Parameter eingegeben werden, d.h. der Aufruf ist von der Form fteiler(m,k). Optional kann auch noch als dritter Parameter eine obere Schranke s für k angegeben werden.

```
fteiler(m, k := 0, s, t_) :=
    Prog
        m : +2
        t_ := 1 + k · 2^m
        Loop
            k : +1
            t_ : +2^m
            If k > s
                RETURN 1
            If MOD(2^(2^(m−2)), t_) = t_ − 1
                RETURN ′(k ∗ 2^m + 1)
```

fteiler$(12) = 2^{14} \cdot 7 + 1$ (0.04 s)
fteiler$(12,7) = 2^{14} \cdot 1588 + 1$ (7.55 s)
fteiler$(12,1588) = 2^{14} \cdot 3892 + 1$ (13 s)
fteiler$(1945) = 2^{1947} \cdot 5 + 1$ (1.95 s).

Besonders beeindruckend ist hier das letzte Beispiel, wo der 587-stellige Teiler $5 \cdot 2^{1947}+1$ der mit $\approx 3.1867 \cdot 10^{585}$ Stellen (!) wahrhaft gigantischen Zahl F_{1945} von Derive in weniger als 2s gefunden wird.

Nachfolgend das analoge Programm zur Auffindung von Teilern von Mersenneschen Zahlen M_p $(p \in \mathbb{P} \setminus \{2\})$:

```
mteiler(p, k := 0, s, d_, t_) :=
    Prog
        t_ := 1 + 2 · k · p
        d_ := 2 · p
        Loop
            t_ : +d_
            If MODS(t_, 8) = ±1 exit
        If MODS(t_ + d_, 8) = ±3
            d_ := 6 · p
        Loop
            If t_ > s
                RETURN 1
            If MOD(2^p, t_) = 1
```

$$[k := (t\_-1)/(2\cdot p), \text{RETURN}\,'(2\cdot k\cdot p+1)]$$
$$t\_ : +d\_$$
$$d\_ := 8\cdot p - d\_$$

$\text{mteiler}(1187) = 2\cdot 108\cdot 1187+1$ (0.03 s)
$\text{mteiler}(1187,108) = 2\cdot 1187\cdot 47853+1$ (12.4 s)
$\text{mteiler}(3407) = 2\cdot 3407\cdot 20353+1$ (5.82 s)
$\text{mteiler}(67) = 2\cdot 67\cdot 1445580+1$ (319.6 s)
$\text{FACTOR}(2^{67}-1) = 193707721\cdot 761838257287$ (0.11 s).

Auch hier gibt es erhebliche Einsparungen an Rechenzeit, aber, wie man am Beispiel der noch relativ kleinen Mersenneschen Zahl M_{67} sieht, stößt man so bald an Grenzen.

4 Die klassische Faktorisierungsmethode nach Fermat

Dass nicht allzu große Teiler einer Zahl relativ leicht gefunden werden können, wofür wir im letzten Abschnitt einige Beispiele angegeben haben, ist eigentlich plausibel und überrascht daher auch nicht besonders. Erstaunlicher ist es schon, dass dies aufgrund eines gewissen Dualismus auch für Teiler von N gilt, die sehr nahe bei $\sqrt{N}$ liegen und daher eigentlich als groß eingestuft werden müssen. In diesem Fall „greift“ nämlich eine andere Faktorisierungsmethode, welche bereits auf Fermat zurückgeht.

Deren einfache Idee besteht darin, dass man versucht, die zu faktorisierende Zahl N, welche hier als ungerade vorausgesetzt wird, in der Form $N = u^2 - v^2$ mit natürlichen Zahlen u und v darzustellen, woraus dann in trivialer Weise die Faktorisierung $N = (u+v)(u-v)$ folgt. Das erste in Frage kommende u ist dabei natürlich $u = \lceil\sqrt{N}\rceil$ und falls p und q die gleiche Stellenanzahl haben und sich in der ersten Hälfte der Stellen nicht unterscheiden, so klappt es auch bereits mit diesem u und der dann ganzen Zahl $v := \sqrt{u^2-N}$. Ansonsten müsste man u laufend um 1 erhöhen und jeweils überprüfen, ob das so definierte v wirklich ganz ist. Es darf allerdings nicht verschwiegen werden, dass die Erfolgschancen dann für großes N schon sehr gering sind, d.h. es klappt in der Regel mit dem ersten u oder gar nicht! Damit dies aber sichergestellt ist, muss N zwei Faktoren besitzen, die gleich viel Stellen haben und sich in der ersten Hälfte der Stellen nicht unterscheiden.

Der Algorithmus schaut formal so aus:

1. Setze zu Beginn $u \leftarrow \lceil\sqrt{N}\rceil$ und $v \leftarrow u^2 - N$.

2. Im Falle, dass $\sqrt{v}$ ganz ist, so gib die nichttriviale Faktorisierung $N = (u - \sqrt{v})(u + \sqrt{v})$ von N aus, anderfalls setze $v \leftarrow v + 2u + 1$, $u \leftarrow u + 1$.

3. Ist $u > (N+9)/6$, so gib das triviale Teilerpaar $[1, N]$ (oder „N ist Primzahl“) aus, anderfalls setze bei Schritt 2 fort.

Der Worst-Case tritt für ein zusammengesetztes N gerade dann ein, wenn N von der Form $N = 3p$ für eine ungerade Primzahl p ist. Diese Faktorisierung wird erst für $u = (n+9)/6$ entdeckt, was Schritt 3 in obigem Algorithmus erklärt.

Dazu kommt auch noch ein Derive-Programm mit einem Faktorisierungsbeispiel für ein 243-stelliges N, das nebenbei bemerkt in der österreichischen Kriminalgeschichte insofern eine gewisse Rolle gespielt hat, als eine in den Medien als „Briefbombenattentäter“ bezeichnete Person an ein österreichisches Magazin ein großteils mit RSA verschlüsseltes Schreiben geschickt hat, wobei gerade dieses N verwendet wurde. „Bombenhirn schickt Fahnder auf die Suche nach zwei großen Primzahlen“ war damals eine Überschrift in einer großen österreichischen Tageszeitung und der Heeresnachrichtendienst und angeblich sogar die NSA waren eingeschaltet. Tatsächlich aber könnte man diese Aufgabe, wie unten ausgeführt, unter Zuhilfenahme dieser alten Idee von Fermat schon im Informatikunterricht an unseren Mittelschulen ohne weiteres lösen.

```
fermat(n, u_, v_) :=
    Prog
        u_ :=CEILING(< n)
        v_ := u_^2 − n
        Loop
            If INTEGER?(SQRT(v_))
                RETURN [u_−SQRT(v_), u_+SQRT(v_)]
            v_ : +2 · u_ + 1
            u_ : +1
            If u > (n+9)/6
                RETURN [1, n]

n := 630548215070129547156718332495889632234434145411971275888376987603260225252787926135276738944105689100036295535868141424386536403649578707699128189491432138631900590774729214990015369102760964884776344849717811484309528915040117952098061886881
fermat(n) =
    [251107191269013549761909333958671246802408057112768448862509598241562051889494061847352957883875611351675294302430759487 99,
    251107191269013549761909333958671246802408057112768
```

$$844886250959824156205188949406184735295788387561135167529435118429780319] \quad (0.000\ \text{s})$$
$$\text{fermat}(63382643) = [1237, 51239] \quad (5.99\ \text{s})$$
$$\text{fermat}(6! \cdot 63382643) = [204956, 222660] \quad (0.06\text{s}).$$

Am Beispiel der noch recht kleinen Zahl $N = 63382643$ wird sichtbar, dass die Fermatsche wirklich nur dann effizient ist, wenn N zwei nahe beieinander liegende Faktoren besitzt, was in diesem Beispiel nicht der Fall ist. Man könnte aber versuchen, dies dadurch zu erreichen, indem man nicht N selbst, sondern geeignete Vielfache kN von N faktorisiert, wie dies oben am Beispiel $k = 6!$ erfolgreich demonstriert wurde.

Lehmann hat diese Idee konsequent ausgebaut und damit eine heute nach ihm benannte Methode geschaffen, die mit $O(N^{1/3} \log\log N)$ arithmetischen Operationen auskommt (s. [1]). Gegenüber den $O(\sqrt{N})$ Operationen bei einer simplen Probedivision stellte dies historisch gesehen die erste echt qualitative Verbesserung dar.

5 Die ρ-Methode von Pollard-Brent

Sehr einfach und trotzdem bei der Auffindung nicht allzu großer Faktoren recht effizient, ist dabei die sog. ρ-Methode von Pollard-Brent, weshalb sie auch in vielen CAS an erster Stelle verwendet wird. Ihr liegt die folgende einfache Idee zugrunde: ist N die zu faktorisierende Zahl und $f(x)$ ein möglichst einfaches Polynom über $\mathbb{Z}$ mit guten Zufallseigenschaften (in der Praxis haben sich Polynome der Form $x^2 + a$ mit $a \notin \{0, -2\}$ gut bewährt), so bildet man die Folge $x_0, x_1, x_2, \ldots$, welche zu einem vorgegebenen Startwert x_0 rekursiv definiert ist durch

$$x_{i+1} = f(x_i) \bmod N, \qquad i = 0, 1, 2, \ldots$$

Ist nun p ein (zunächst natürlich unbekannter) Primfaktor von N und betrachtet man diese Folge rein gedanklich mod p, so werden sehr bald einmal zwei Folgenglieder mod p gleich sein. Theoretisch könnte dies auch erst nach $p + 1$ Iterationen sein, in der Praxis ist dies aber schon viel früher der Fall. Dieses Phänomen wird nach einer bekannten Einkleidung auch oft als „Geburtstagsparadoxon“ bezeichnet. Wir wählen aber hier ein Urnenmodell und fragen: wie oft muss aus einer Urne, welche m unterscheidbare Objekten enthält, ziehen (und zwar mit Zurücklegung!), bis das Ergebnis mit dem einer früheren Ziehung übereinstimmt. Bezeichnet dazu $W_{k,m}$ die Wahrcheinlichkeit, dass nach k Ziehungen alle Objekte bis dahin noch verschieden waren, so gilt dann

$$\begin{aligned} W_{k,m} &= \left(1 - \frac{1}{m}\right)\left(1 - \frac{2}{m}\right) \cdots \left(1 - \frac{k-1}{m}\right) \\ &\approx e^{-1/m} e^{-2/m} \cdots e^{-(k-1)/m} = e^{-k(k-1)/(2m)}, \end{aligned}$$

wobei hier für die Näherung $k \ll m$ angenommen wurde. $W_{k,m}$ wird mit wachsendem k sehr schnell klein, z.B. gilt $W_{k,m} \leq 0.5$ bereits ab etwa $k \approx \sqrt{2m\log 2} \approx 1.2\sqrt{m}$.

Setzt man noch $W_{0,m} := 1$, so errechnet sich insbesondere der Erwartungswert E_m für die Anzahl der Ziehungen, bis zum ersten Mal eine Koinzidenz auftritt zu

$$\begin{aligned} E_m &= \sum_{k=0}^{\infty} W_{k,m} \\ &= 1+1+\left(1-\frac{1}{m}\right)+\cdots+\left(1-\frac{1}{m}\right)\left(1-\frac{2}{m}\right)\cdots\left(1-\frac{k-1}{m}\right)+\cdots \\ &\approx \sum_{k=0}^{\infty} e^{-k(k-1)/(2m)} \approx \int_0^{\infty} e^{-x^2/(2m)}\,dx = \sqrt{\frac{\pi m}{2}}. \end{aligned}$$

Für unser Ausgangsproblem, wo m die Anzahl der verschiedenen Restklassen mod p bedeutet, die $f(x)$ überhaupt annehmen kann (für ein $f(x)$ der Form $f(x) = x^2 + a$ wäre diese z.B. $m = (p+1)/2$) heißt dies, dass jedenfalls innerhalb der ersten $O(\sqrt{p})$ Glieder der obigen Folge $x_0, x_1, x_2, \ldots$ eine Koinzidenz mod p zu erwarten wäre. Insbesondere bedeutet dies, dass bereits für relativ kleine Indizes i, j mit $i > j$ gilt $x_i \equiv x_j \bmod p$ und folglich $\mathrm{ggT}(x_i - x_j, N) \neq 1$, womit man durch Bildung von ggT – außer in dem sehr unwahrscheinlichen Fall, dass auch $x_i \equiv x_j \bmod N$ gilt – einen nichttrivialen Teiler von N erhält.

Es wäre nun allerdings sehr aufwändig, würde man tatsächlich alle Folgenglieder $x_0, x_1, x_2, \ldots$ in Evidenz halten müssen, um für alle Paare (i, j) mit $i > j$ das Erfülltsein obiger Bedingung $\mathrm{ggT}(x_i - x_j, N) \neq 1$ überprüfen zu können. Dies ist aber auch gar nicht notwendig. So machte es sich schon Pollard in seiner ursprünglichen Version der ρ-Methode zu Nutze, dass es sogar ein derartiges Paar (i, j) mit $i = 2j$ geben muss.

Dies sieht man nach Floyd auf einfache Weise so: zeichnet man zu der Folge $x_0, x_1, x_2, \ldots \bmod p$ den Digraphen, den man erhält, indem man x_k mit x_{k+1} für $k = 0, 1, 2, \ldots$ durch eine gerichtete Kante verbindet, so ist dieser bei geeigneter Anordnung der Knoten in seiner Form ähnlich einem ρ, woher übrigens auch diese Methode ihren Namen hat. Insbesondere gibt es also einen Vorperiodenteil und einen sich daran anschließenden Zyklusteil. Hat letzterer die Länge l, so gilt dann offenbar für das kleinste durch l teilbare j, für welches x_j im Zyklusteil liegt, zum ersten Mal $x_{2j} \equiv x_j \bmod p$.

Damit braucht man also nur parallel zur Folge der x_i eine weitere Folge y_i, $i = 0, 1, 2 \ldots$ mit gleichem Startwert $y_0 = x_0$, aber der doppelt so schnell laufenden Rekursion

$$y_{i+1} = f(f(y_i)), \quad i = 0, 1, 2 \ldots$$

berechnen, womit also $y_i = x_{2i}$ gilt, um dann jeweils nur für jedes i die Bedingung $\mathrm{ggT}(y_i - x_i, N) \neq 1$ zu überprüfen. Ist $\mathrm{ggT}(x_i - x_j, N) = N$, was zwar selten aber

doch vorkommen kann, so empfiehlt es sich, das Polynom $f(x)$ gegen ein anderes auszutauschen. (Man könnte auch einen anderen Startwert x_0 versuchen, doch bringt dies in der Regel nichts.)

Im nachfolgenden Derive-Programm haben wir standardmäßig $f(x) = x^2 + 1$ gesetzt, was sich in der Praxis recht gut bewährt hat. Man beachte jedoch, dass für Zahlen spezieller Bauart u.U. andere Polynome günstiger sein können. Dies gilt insbesondere auch wieder für Mersennesche Zahlen $M_p = 2^p - 1$ $(p \in \mathbb{P})$ und Fermatsche Zahlen $F_m = 2^{2^m} + 1$ $(m \in \mathbb{N})$, für welche Polynome der Bauart $f(x) = x^e + 1$ mit $e = p$ bzw. $e = 2^{m+1}$ gemäß unserer Bemerkungen über die Form der Teiler dieser Zahlen und dem Satz von Legendre deutlich besser sind.

```
rho(n,e := 2,x := 3,y := 3,s := 100,k_,t_ := 1,x_,y_) :=
    Loop
        x_ := x
        y_ := y
        k_ := s
        Loop
            If k_ = 0
                If GCD(t_,n) = 1
                    exit
                    If MOD(t_,n) = 0 AND s > 1
                        [x := x_,y := y_,s := 1,t_ := 1, exit]
                        RETURN GCD(t_,n)
            x :=MOD(x^e,n) + 1
            y :=MOD(y^e,n) + 1
            y :=MOD(y^e,n) + 1
            t_ :=MOD(t_ · (x − y),n)
            k_ : −1
```

$\text{rho}(2^{101} - 1) = 7432339208719$ (163.9 s)
$\text{rho}(2^{101} - 1, 101) = 7432339208719$ (84.9 s)
$\text{rho}(2^{2^8} + 1, 2^{10}) = 1238926361552897$ (558.5 s)
$\text{rho}(2^{2^{12}} + 1) = 114689$ (0.901 s)
$\text{rho}(2^{2^{12}} + 1, 2^{14}) = 190276431449381650433$ (4.57 s)
$\text{FACTOR}(190276431449381650433) =$
$114689 \cdot 26017793 \cdot 63766529$ (0.031 s).

Man kann aber, worauf R. Brent als erster hingewiesen hat, auch nur mit der ursprünglichen Folge $x_0, x_1, x_2, \ldots$ allein auskommen, wenn man die Überprüfung der Bedingung $\text{ggT}(x_i - x_j, N) \neq 1$ nur für jene Paare (i, j) vornimmt, für welche j von der speziellen Form $j = 2^k - 1$ ist und i nur jeweils die Werte $i = j + 2^{k-1} + r$, $r = 1, \ldots, 2^{k-1}$ durchläuft. Dass dies ausreicht, sieht man mit einer ähnlichen

Überlegung wie oben, indem man diesmal den kleinsten Index j von der Form $2^j - 1$ betrachtet, sodass einerseits x_j bereits im Zyklus liegt, andererseits aber $2^k \geq l$ ist, wobei l wieder die Zykluslänge bezeichnet. Gegenüber der ursprünglichen ρ-Methode von Pollard ergibt dies immerhin eine Beschleunigung um ca. 25%, doch verzichten wir hier aus Platzgründen auf eine Implementierung in Derive.

Wie bereits oben ausgeführt, sind für beide Algorithmen $O(\sqrt{p})$ Iterationen zu erwarten, wobei p der kleinste Primfaktor von N ist. In jedem Iterationsschritt wird nur eine konstante Anzahl von arithmetischen Operationen mit Zahlen von der gleichen Größenordnung wie N durchgeführt, deren Aufwand durch $O((\log N)^2)$ abgeschätzt werden kann. Der Gesamtaufwand wäre demnach $O(\sqrt{p}(\log N)^2)$ und hängt damit sehr stark von der Größe des kleinsten Primfaktors p von N ab. Der ungünstigste Fall bei Anwendung dieser Methode liegt dann vor, wenn N das Produkt etwa zwei gleich großer Primzahlen ist, womit dann für unser p gilt $p \approx \sqrt{N}$, d.h. in diesem Fall beträgt der Aufwand $O(N^{1/4}(\log N)^2)$. Dies ist aber immer noch erheblich günstiger als der entsprechende Aufwand bei der Probedivision in diesem Fall, welcher $O(\sqrt{N}(\log N)^2)$beträgt.

6 Die $(p-1)$-Methode und $(p+1)$-Methode

Fast bei allen bisher besprochenen Faktorisierungsmethoden waren die Erfolgschancen auf eine nichtriviale Faktorisierung von N ganz entscheidend verknüpft mit der Größe des kleinsten Primfaktors p von N. Im Gegensatz dazu kommt es bei den nun zu besprechenden Methoden auf andere Eigenschaften an, die nur indirekt mit der Größe von p gekoppelt sind.

Bei der sog. $(p-1)$-Methode von Pollard versucht man mit einem zur Testzahl N teilerfremden a eine Potenz a^r mod N so zu bilden, dass für einen (vorderhand noch unbekannten) Primfaktor p von N gilt, dass $p-1$ ein Teiler von r ist. Für jedes solche r folgt nämlich aus dem „Kleinen Fermatschen Satz“ sofort

$$a^r = (a^{p-1})^{\frac{r}{p-1}} \equiv 1 \bmod p,$$

womit durch Bildung von $\mathrm{ggT}(a^r - 1, N)$ sofort einen nichttrivialer Teiler von N finden könnte, außer in dem höchst unwahrscheinlichen Fall, dass auch $a^r \equiv 1 \bmod N$ gilt.

Die Hauptschwierigkeit ist dabei klarerweise das Auffinden eines geeigneten r. Unter der (wie wir allerdings schon gesehen haben selten gegebenen) Voraussetzung, dass $p-1$ für wenigstens einen Primteiler p von N keine „großen“ Primzahlpotenzen enthält, also S-potenzglatt für eine nicht allzu große Schranke S ist, wären dann u.a. alle r geeignet, die sämtliche Primzahlpotenzen $\leq S$ als Faktoren enthalten, da für sie dann $p-1$ ein Teiler von r wäre.

Um so ein r zu konstruieren, geht man nach folgendem 2-Stufenplan vor: ist $p_1, p_2, \ldots, p_s$ die Folge der Primzahlen in ihrer natürlichen Reihenfolge und $q_i = p_i^{e_i}$, dass für eine fest gewählte Schranke S_1 gilt $q_i \le S_i$ aber $p_i q_i > S_1$, d.h. also

$$e_i = \lfloor \log S_1 / \log p_i \rfloor, \quad i = 1, 2, \ldots, s,$$

so berechnet man für eine fest gewählte Basis a in der 1. Stufe der Reihe nach die Zahlen

$$b_1 = a^{q_i} \bmod N \quad \text{und} \quad b_i = b_{i-1}^{q_i} \bmod N \quad \text{für } i > 1$$

sowie

$$u_1 = b_1 - 1 \quad \text{und} \quad u_i = (b_i - 1) u_{i-1} \bmod N \quad \text{für } i > 1$$

und überprüft periodisch, ob $\mathrm{ggT}(u_i, N) > 1$ ist, womit man dann (außer in dem sehr unwahrscheinlichen Fall $\mathrm{ggT}(u_i, N) = 1$) einen nichttrivialen Teiler von N gefunden hätte.

Gilt stets $\mathrm{ggT}(u_i, N) = 1$ für $i = 1, 2, \ldots, s$, so war die 1. Stufe der Pollardschen $(p-1)$-Methode erfolglos und man kann eine 2. Stufe in folgender Weise anschließen:

Ist S_2 eine weitere fest gewählte Schranke, welche in der Praxis etwa 10–100 mal so groß wie S_1 ist und seien die Primzahlen q mit $S_1 < q \le S_2$ fortlaufend mit $q_{s+1}, q_{s+2}, \ldots, q_t$ benannt, so setzt man

$$c_1 = b_s^{q_{s+1}} \bmod N \quad \text{und} \quad c_i = c_{i-1} b_s^{q_{s+i} - q_{s+i-1}} \bmod N \quad \text{für } i > 1.$$

Ferner wird wieder eine Folge $u_1, u_2, u_3, \ldots$ in analoger Weise wie oben, aber mit den c_i an Stelle der b_i definiert und es wird wieder periodisch überprüft, ob $\mathrm{ggT}(u_i, N) > 1$ ist. Wie man sich leicht überlegt, führt diese 2. Stufe sicher dann zum Erfolg, wenn N einen Primfaktor p besitzt, sodass für einen Primfaktor q von $p-1$ mit $S_1 < q \le S_2$ gilt, dass $(p-1)/q$ potenzglatt ist bezüglich S_1. (q ist also für $p-1$ gewissermaßen ein nicht zu großer „Ausreißer“ im Bezug auf die S_1-Potenzglattheit.)

Im nachfolgenden Derive-Programm haben die einzugebenden Parameter folgende Bedeutung: n ist die zu faktorisierende Zahl, a die Ausgangsbasis für die Potenzbildungen, s und t sind die oben näher beschriebenen Schranken S_1 und S_2 für die erste und zweite Stufe. Ferner gibt es noch den Parameter u, welcher den Defaultwert 100 besitzt und für die 2. Stufe festlegt, nach wieviel Schritten jeweils eine Überprüfung von $\mathrm{ggT}(u_i, N) > 1$ vorgenommen wird. (Für die erste und weniger zeitkritische Stufe wurde der entsprechende Wert intern auf 1 gesetzt.)

```
pminus1(n, a, s, t, u := 100, a_, b_ := 1, k_ := 0, p_ := 2, q_) :=
    Prog
        Loop
            a :=MOD(a^p_^FLOOR(LOG(s, p_)), n)
```

```
    If GCD(a − 1, n) > 1
      RETURN GCD(a − 1, n)
    p_ :=NEXT_PRIME(p_)
    If p_^2 > s exit
  Loop
    a :=MOD(a^p_, n)
    If GCD(a − 1, n) > 1
      RETURN GCD(a − 1, n)
    p_ :=NEXT_PRIME(p_)
    If p_ > s exit
  a_ :=MOD(a^p_, n)
  q_ :=NEXT_PRIME(p_)
  Loop
    b_ :=MOD((a_ − 1) · b_, n)
    If k_ = 0
      If GCD(b_, n) > 1
        RETURN GCD(b_, n)
        k_ := u
    If p_ > t
      RETURN GCD(b_, n)
    a_ :=MOD(a_ · MOD(a^(q_ − p_), n), n)
    p_ := q_
    q_ :=NEXT_PRIME(q_)
    k_ : −1
```

$$\text{pminus1}(2^{257}-1, 3, 120000, 1200000) = 115568539524661918267303 3. \qquad (32.3\text{ s})$$

Als eindrucksvolles Beispiel für die Wirksamkeit dieser Methode ist die Auffindung des 25-stelligen Primteilers 1155685395246619182673033 von $2^{257}-1$ in nur 32.3s (!) angegeben. Die eingebaute Faktorisierungsmethode, welche sich u.a. ebenfalls der $(p-1)$-Methode in modifizierter Form bedient, liefert übrigens die vollständige Faktorisierung

$$535006138814359 \cdot 1155685395246619182673033 \cdot 37455059850181093658177663009631318139 3$$

in 191.7s, was immer noch beeindruckend schnell ist. (Der Zeitunterschied erklärt sich aus der vorherigen erfolglosen Anwendung von anderen Methoden, insbesondere der ρ-Methode.)

Dieses „Kunststück“ war übrigens nur deshalb möglich, weil der zweitgrößte Primfaktor p durch die besondere Primteilerstruktur von $p-1$ eine Angriffsfläche bot:

$$\text{FACTOR}(115568539524661918267303 3-1) = \\ 2\cdot 3\cdot 19\cdot 47\cdot 67\cdot 257\cdot 439\cdot 119173\cdot 1050151$$

Im Nachhinein wird damit auch klar, warum die besondere Wahl der Schranken in diesem Beispiel zum Erfolg führte: $S_1 = 120\,000$ „deckt“ alle Primzahlpotenzen von $p-1$ mit Ausnahme der Primzahl 1050151 ab, wobei diese aber unterhalb von $S_2 = 1\,200\,000$ liegt.

Das „Gegenstück“ zur $(p-1)$-Methode von Pollard, bei welcher die Rechnungen in der primen Restklassengruppe mod p (mit der Ordnung $p-1$) durchgeführt werden, ist die $(p+1)$-Methode von Williams, wo in der (eindeutig bestimmten) Untergruppe G der Ordnung $p+1$ der multiplikativen Gruppe des Körpers $\mathbf{F}_{p^2}$ gerechnet wird.

Man kann dabei wieder auf gewisse Eigenschaften der bereits im 1. Teil dieses Artikels eingeführten Lucasfolgen zurückgreifen. Wählt man nämlich $Q = 1$ und P so, dass für die Diskriminante $D = P^2 - 1$ gilt $(D/p) = -1$, so folgt aus

$$\alpha^{p+1} = \alpha\alpha^p = \alpha\beta = Q = 1 \quad \text{und analog} \quad \beta^{p+1} = 1,$$

dass α und β tatsächlich in G liegen und damit nach Definition der U- bzw. V-Lucasfolgen deren sämtliche Glieder. Insbesondere gilt, wenn $p+1$ Teiler von r ist, dass

$$\alpha^r = \beta^r = 1$$

und daher auch

$$V_r = \alpha^r + \beta^r \equiv 2 \bmod p.$$

Die Teilerbeziehung

$$p | \text{ggT}(V_r - 2, N)$$

kann aber nun nach schon bewährten Vorbildern zur Auffindung von nichttrivialen Faktoren von N herangezogen werden. Bei der praktischen Durchführung der $(p+1)$-Methode macht man dabei Gebrauch von

$$V_{kl}(P,1) = V_k(V_l(P,1),1),$$

womit man dann V_i in einer ähnlichen Weise sukzessive berechnen kann wie oben die b_i für die $(p-1)$-Methode.

Auch die $(p+1)$-Methode, welche auch oft nach ihren Entdecker Williams benannt wird, kommt in Derive als eine der vielen „Faktorisierungsstrategien“ zur Anwendung. In der einfachsten Version (entsprechend der ersten Stufe bei der $(p-1)$-Methode) geht man diesmal davon aus, dass N einen Primfaktor p besitzt, sodass $p+1$ nur durch Primzahlpotenzen $\leq S$ für eine relativ kleine Schranke S teilbar ist. Leider braucht man, da man ja p nicht kennt, auch etwas „Glück“, damit bei der konkreten Wahl von P, Q auch wirklich $(D/p) = -1$ ist: hat man

Pech und ist $(D/p) = 1$, so wird die $(p+1)$-Methode nämlich zu einer langsamen $(p-1)$-Methode. In der Praxis läuft dies auf mehrere Versuche hinaus. Aus Platzgründen wollen wir uns diesmal mit einem einfachen Beispiel, nämlich der vollständigen Faktorisierung der 103-stelligen Zahl begnügen. Wegen

$$10^{102}+1 = (10^{34}+1)(10^{68}-10^{34}+1)$$

und der von Derive selbst leicht gefundenen Faktorisierung

$$\begin{aligned}&\text{FACTOR}(10^{34}+1) = \\ &\quad 101\cdot 28559389\cdot 1491383821\cdot 2324557465671829 \qquad (0.49\text{ s})\end{aligned}$$

genügt es, die Faktorisierung des Kofaktors

$$n := 10^{68}-10^{34}+1$$

zu finden. Mit Hilfe von

$$\begin{aligned}&\text{GCD}(\text{V\_MOD}(\text{LCM}([2,\ldots,10000]),5,1,n)-2,n) = \\ &\quad 377313498335611636061436653011201 \qquad (7.19\text{ s}) \\ &\text{FACTOR}(377313498335611636061436653011201) = \\ &\quad 409\cdot 3061\cdot 9901\cdot 134703241\cdot 225974065503889\end{aligned}$$

erhalten wir eine Reihe von weiteren Faktoren. Insbesondere wurde der 15-stellige Primfaktor 225974065503889 wegen

$$\text{FACTOR}(225974065503889+1) = 2\cdot 5\cdot 11\cdot 79\cdot 401\cdot 7867\cdot 8243$$

so rasch gefunden. Die Auffindung der beiden restlichen Faktoren kann man dann getrost wieder Derive überlassen:

$$\begin{aligned}&\text{FACTOR}(n/377313498335611636061436653011201) = \\ &\quad 5969449\cdot 443980004790079975697517642 49 \qquad (0.08\text{ s}).\end{aligned}$$

7 Arithmetik auf Elliptischen Kurven

H. Lenstra hat als erster in seiner bahnbrechenden Arbeit [7] darauf hingewiesen, dass man die Ideen des vorangegangenen Abschnitts mit großem Erfolg auch auf eine andere wichtige Klasse von endlichen abelschen Gruppen anwenden kann, nämlich solchen, welche den sog. Elliptischen Kurven auf endlichen Körpern in natürlicher Weise zugeordnet sind.

Ist K irgendein Körper, so versteht man allgemein unter einer elliptischen Kurve E über K die Menge der Punkte $(x,y) \in K\times K$, welche einer Gleichung der Form

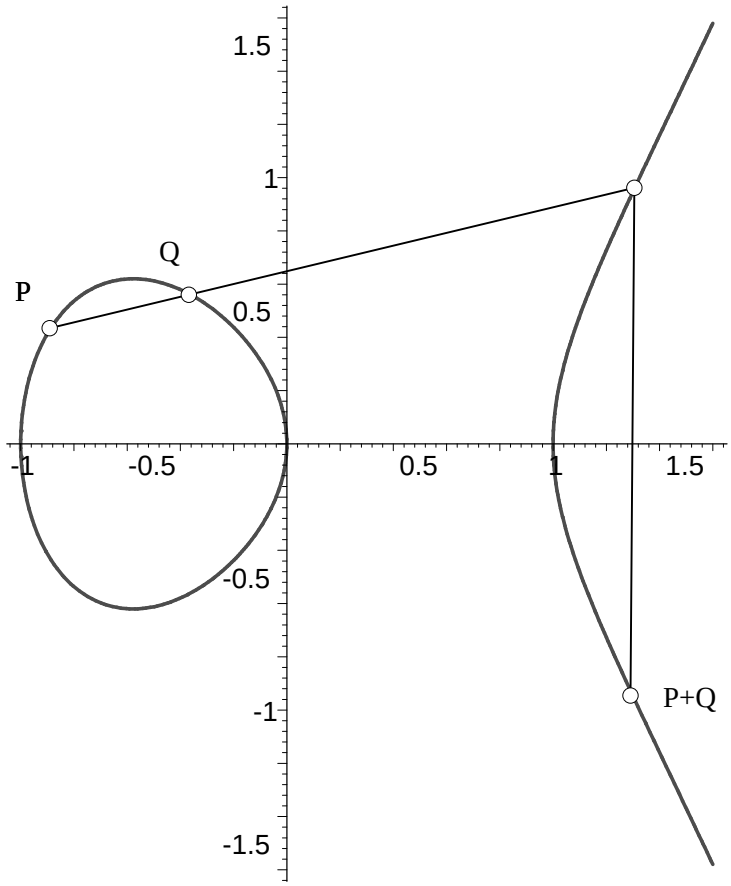
$$y^2+a_4xy+a_3y = x^3+a_2x^2+a_1x+a_0 \quad (a_i \in K,\ i = 0,1,2,3,4)$$

genügen, zusammen mit dem sogenannten „unendlich fernen“ Punkt O. Ferner wird noch vorausgesetzt, dass es keine singulären Punkte gibt. (Bringt man obige Kurvengleichung auf die Form $F(x,y)=0$, so bedeutet dies, dass für keinen Punkt (x,y) im algebraischen Abschluß beide partiellen Ableitungen $F_x(x,y)$ und $F_y(x,y)$ gleichzeitig verschwinden.)

Speziell für $\mathrm{char}(K) \neq 2,3$ kann man nach einer ev. linearen Transformation der Koordinaten x,y stets davon ausgehen, dass obige Gleichung die Form

$$y^2 = x^3 + ax + b \quad (a,b \in K)$$

hat, was wir im folgenden der Einfachheit halber stets annehmen wollen. Die Bedingung der Nichtexistenz von singulären Punkten bedeutet dann, dass das rechtsstehende Polynom keine mehrfachen Nullstellen hat, was wiederum zur einfachen Bedingung $4a^3+27b^2 \neq 0$, d.h. zum Nichtverschwinden der Diskriminante des kubischen Polynoms gleichwertig ist. Sie garantiert im Fall $K=\mathbb{R}$, dass die durch sie definierte algebraische Kurve E keine Spitzen und Überkreuzungen hat und daher (ohne die Geraden) z.B. so wie in der untenstehenden Abbildung aussehen könnte:



Die eingezeichneten Hilfsgeraden sollen dabei andeuten, wie für zwei Punkte P und Q von E die Summe $P+Q$ definiert ist, sodass dann $(E,+)$ zu einer abelschen Gruppe wird. Man unterscheidet dazu folgende Fälle:

1. Ist $P = O$ bzw. $Q = O$, so ist $P+Q = Q$ bzw. $P+Q = P$, d.h. O spielt die Rolle eines neutralen Elements bez. $+$.

2. Liegen P und Q spiegelbildlich bezüglich der x-Achse, so sei $P+Q = O$. Insbesondere sind in diesem Fall wegen 1. die Punkte P und Q zueinander invers.

3. Liegt weder der Fall 1. noch der Fall 2. vor, so sei $P+Q$ wie aus der vorstehenden Skizze ersichtlich definiert, d.h. man bestimmt den eindeutig definierten Schnittpunkt der Sekante durch P und Q (bzw. im Fall $P = Q$ der Tangente durch P) mit der Kurve und definiert $P+Q$ als seinen Spiegelpunkt bez. der x-Achse.

Den Fall 3. wollen wir uns nun noch genauer ansehen. Sei dazu $P = (x_1, y_1)$ und $Q = (x_2, y_2)$, so ist die Steigung k der Sekante durch P und Q (bzw. im Fall $P = Q$ Tangente durch P) gegeben durch

$$k = \begin{cases} \dfrac{y_2 - y_1}{x_2 - x_1}, & \text{falls } x_1 \neq x_2, \\ \dfrac{3x_1^2 + a}{2y_1}, & \text{falls } x_1 = x_2,\ y_1 \neq 0. \end{cases}$$

Für die Koordinaten (x_3, y_3) von $P+Q$ ergibt sich daher nach einfacher Rechnung

$$x_3 = k^2 - x_1 - x_2, \quad y_3 = -y_1 + k(x_1 - x_3).$$

Für die hier nun betrachteten Anwendungen besonders wichtig ist der Fall $K = \mathbb{Z}_p$, wo p eine Primzahl ist. Nachfolgend ist eine Derive-Implementierung einer Routine für die Addition von zwei Punkten U und V auf einer elliptischen Kurve mod p (mit $[p,p]$ als Darstellung für den Punkt O) angegeben.

```
add(u,v,a,p,k_) :=
    PROG(
        IF(u = [p,p] OR v = [p,p],
            RETURN u+v-[p,p]),
        IF(u SUB 1 = v SUB 1 AND MOD(u SUB 2+v SUB 2,p) = 0,
            RETURN [p,p]),
        IF(u = v,
            k_ :=MOD((3·u SUB 1 ^2+a)·
                INVERSE_MOD(2·u SUB 2,p),p),
```

```
    k_ := MOD((v SUB 2 − u SUB 2)·
        INVERSE_MOD(v SUB 1 − u SUB 1, p), p)),
  IF(k_ = ?,
    RETURN IF(u = v, GCD(2 · u SUB 2, p),
        GCD(v SUB 1 − u SUB 1, p))),
  a := MOD(k_^2 − u SUB 1 − v SUB 1, p),
  [a, MOD(−u SUB 2 + k_ · (u SUB 1 − a), p)]).
```

Im Hinblick auf spätere Anwendungen wurde dabei auch der allgemeinere Fall berücksichtigt, dass p keine Primzahl ist. Dann ist aber die Berechnung von k gemäß obiger Formeln nicht immer möglich, da ja dann die dazu benötigten Inversen von $x_2 - x_1$ bzw. $2y_1$ mod p nicht mehr notwendigerweise existieren. Trifft dieser Fall zu, so werden die Teiler $\mathrm{ggT}(x_2 - x_1, p)$ bzw. $\mathrm{ggT}(2y_1, p)$ von p ausgegeben.

Im Folgenden wird auch häufig die Berechnung von Vielfachen nU eines Punktes für ein $n \geq 0$ benötigt. Diese geschieht am einfachsten mit Hilfe der sog. „Square and Multiply"-Methode, welche auch schon die alten Ägypter zur Berechnung von Produkten von natürlichen Zahlen verwendeten, indem sie Produkte als additive Potenzen interpretierten. (Auch die im ersten Teil dieser Arbeit im Zusammenhang mit dem Fermattest und dessen Verallgemeinerungen auftretenden modularen Potenzen werden auf diese Weise berechnet, was diese Tests erst praktikabel macht.)

Nachfolgend wieder eine Derive-Routine zur Berechnung von nU für den Punkt U auf der elliptischen Kurve mod p. (Man beachte, dass nur a explizit angegeben werden muss, da sich der Wert von b dann aus a und dem Punkt $U \in E$ ergibt.)

```
multiple(u, n, a, p, b_) :=
  PROG(
    b_ := [p, p],
    LOOP(
      IF(n = 0, RETURN b_),
      IF(ODD?(n),
        PROG(
          b_ := add(u, b_, a, p),
          IF(NUMBER?(b_), RETURN b_))),
      u := add(u, u, a, p),
      IF(NUMBER?(u), RETURN u),
      n := FLOOR(n, 2))).
```

Für praktische Anwendungen sehr wichtig wäre noch eine effiziente Routine NOP(a,b,p), welche die Anzahl der Punkte („**n**umber **o**f **p**oints") auf einer elliptischen Kurve $E : y^2 = x^3 + ax + b$ mod p berechnet. R. Schoof hat dazu in

[8] einen heute nach ihm benannten Algorithmus der Komplexität $O((\log p)^8)$ angegeben, was inzwischen durch Beiträge von Elkies, Atkin und Morain (s. [1]) noch weiter auf $O((\log p)^6)$ verbessert werden konnte. Wir begnügen uns hier aus Platzgründen mit der folgenden allereinfachsten Version, welche jedoch ausreichen sollte, um einfache Beispiele damit rechnen zu können.

$$\begin{aligned}\mathrm{NOP}(a,b,p) &:= p+1 \\ &\quad + \mathrm{SUM}(\mathrm{JACOBI}(x\_^3 + a\cdot x\_ + b, p), x\_, 0, p-1)\end{aligned}$$

Insbesondere zeigt der rechts stehende Ausdruck, wenn man die darin enthaltene Summe von Jacobisymbolen, die ja nur Werte in $\{-1,0,1\}$ annehmen können, als „Random Walk“ auf der Zahlengerade in 0 beginnend deutet, dass die Anzahl der Punkte auf E mod p statistisch gesehen um höchstens $O(\log p)$ von $p+1$ abweichen sollte. Genauer gilt nach einem Satz von Hasse, dass diese Abweichung (nach oben oder unten) maximal $2\sqrt{p}$ beträgt. (Interessanterweise werden für ein vorgegebenes p durch Variation der Elliptischen Kurven auch alle ganzen Werte in dem sog. Hasse-Intervall $(p+1-2\sqrt{p}, p+1+2\sqrt{p})$ tatsächlich angenommen.)

Nachstehend möchte ich versuchen, an einigen Beispielen wenigstens anzudeuten, inwiefern Elliptische Kurven im Hinblick auf unser generelles Thema von Nutzen sein können. An erster Stelle wäre hier zu erwähnen der versprochene Nachtrag zu den deterministischen Primzahltests, nämlich der Goldwasser-Kilian-Test. Die theoretische Grundlage dafür bildet der

Satz. *Sei $N>1$ eine natürliche Zahl mit $\mathrm{ggT}(6,N)=1$ und sei E die Menge der Punkte (x,y), welche eine Gleichung der Form $y^2 = x^3+ax+b \bmod N$ mit gewissen ganzen Zahlen a,b erfüllen. Gibt es dann ein $m\in\mathbb{N}$ mit einem Primteiler $q>(N^{1/4}+1)^2$ und einen Punkt P von E, sodass (mit der wie oben definierten Addition über $\mathbb{Z}_N$)*

$$mP = O, \quad \textit{aber} \quad \frac{m}{q}P \neq O$$

gilt, so ist N prim.

Und hier ein kleines Beispiel dazu, in dem wir unter Benutzung des obigen Satzes beweisen, dass $N=11311$ prim ist. Wir verwenden dazu die elliptische Kurve $y^2 = x^3+x-1$ und den Punkt $P=(1,1)$.

$$\begin{aligned}&n := 11311\\ &\mathrm{nop}(1,-1,n) = 11394\\ &\mathrm{FACTOR}(11394) = 2\cdot 3^3\cdot 211\\ &\mathrm{SOLVE}(211 > (n^{1/4}+1)^2) = \mathrm{true}\\ &\mathrm{multiple}([1,1],11394,1,n) = [11311,11311]\\ &\mathrm{multiple}([1,1],11394/211,1,n) = [8987,9105].\end{aligned}$$

Prinzipiell ist noch zu sagen, dass dieser Test natürlich erst zur Anwendung kommt, wenn N schon eine Reihe von einfachen probalistischen Primzahltests

bestanden hat, sodass also mit hoher Wahrscheinlichkeit $\mathbb{Z}_N$ wirklich ein Körper ist und man auf einer „echten“ elliptischen Kurve rechnet. Sollte dies doch nicht der Fall sein, so würden eventuell daraus resultierende Probleme gerade die Zusammengesetztheit von N beweisen!

So wie in dem Beispiel, verwendet man für das m im Satz in der Regel die Anzahl der Punkte auf der elliptischen Kurve, deren Bestimmung sicher die Hauptschwierigkeit darstellt. Der oben dafür angegebene Aufwand, nämlich $O((\log N)^6)$, ist zugleich der Erwartungswert für den Gesamtaufwand. Eine weitere Hürde ist ferner die Auffindung eines Primteilers $q > (N^{1/4}+1)^2$ von m, falls ein solcher existiert. Dabei wird man sich in der Regel zunächst damit begnügen, dass q eine wahrscheinliche Primzahl ist und erst nach bestandenen Test sich der Frage der Primalität von q erneut zuwenden, indem man zeigt, dass auch q den Goldwasser-Kilian-Test besteht. (Dies natürlich wieder unter der Voraussetzung, dass das dabei verwendete q wirklich prim ist usw. Da die Folge der so erhaltenen q exponentiell kleiner wird, kommt man so bald an ein Ende.) Die Gesamtheit aller Parameter, welche für die Tests verwendet wurden, bildet dann ein sog. Primzahlzertifikat, das eine eventuelle Wiederholung oder Überprüfung des Tests sehr einfach macht. Dies ist ein weiterer nicht zu unterschätzender Vorteil gegenüber dem früher oft verwendeten APRCL-Test (s. [5]).

Elliptische Kurven können aber, wie eingangs schon erwähnt, auch zum Faktorisieren benutzt werden und sie werden auch in Derive intern zu diesem Zweck angewendet, wenn alle anderen Faktorisierungsmethoden bereits versagt haben. Die von H. Lenstra 1985 zu diesem Zweck eingeführte ECM (=Elliptic Curve Method) ist jedoch in ihren Grundzügen der $(p-1)$-Methode des vorigen Abschnitts so ähnlich, dass wir uns hier sehr kurz fassen können.

Ähnlich wie beim Goldwasser-Kilian-Test geht man wieder aus von einer festen elliptischen Kurve $E : y^2 = x^3 + ax + b$ über $\mathbb{Z}_N$ und einem festen Punkt P auf E. Im Unterschied zu vorhin weiß man jetzt durch einen vorangegangenen Primalitätstest, dass N zusammengesetzt ist und versucht ein Vielfaches von rP zu finden, welches undefiniert ist, womit man dann gleichzeitig einen nichttrivialen Teiler von N gefunden hätte. Dies ist jedenfalls sicher dann der Fall, wenn N einen Primfaktor p besitzt, sodass bei Durchführung aller Rechnungen mod p statt mod N (was natürlich nur gedanklich möglich ist!) $rP = O$ gilt, d.h. es erweist sich auch hier wieder als aussichtsreich, alle Primzahlpotenzen bis zu einer Schranke S in r zu „akkumulieren“. Die algorithmische Durchführung ist ansonsten gleich wie für die $(p-1)$-Methode, der einzige Unterschied besteht in der additiven Schreibweise. Insbesondere gibt es auch hier wieder in ganz analoger Weise eine zweite Stufe.

Als Beispiel wollen wir eine vereinfachte Form der ECM auf die Fermatzahlen F_7 und F_8 anwenden, was den jeweils kleineren der beiden Primfaktoren eindrucksvoll schnell liefert:

$$\text{multiple}([1,1], \text{LCM}([2,\ldots,4000]), 501, 2^{2^7}+1) =$$
$$59649589127497217 \qquad (12.6\text{ s})$$
$$\text{multiple}([1,1], \text{LCM}([2,\ldots,7000]), 134, 2^{2^8}+1) =$$
$$1238926361552897 \qquad (29.5\text{ s}).$$

Natürlich darf dabei nicht verschwiegen werden, dass in der Regel viele elliptische Kurven „durchprobiert“ werden müssen, bevor man auf eine passende stößt. Die Zeit für diese Fehlversuche muss also noch addiert werden. Insgesamt ist der Rechenaufwand zur Auffindung eines Primfaktors p von N bei der ECM „subexponentiell“, genauer von der Größenordnung

$$O\left(\exp\left(\sqrt{(2+o(1))\log p \log\log p}\right)\right),$$

was, bezogen auf N selbst, im ungünstigsten Fall $p \approx \sqrt{N}$ einen Aufwand

$$O\left(\exp\left(\sqrt{(1+o(1))\log N \log\log N}\right)\right)$$

ergibt. In der Praxis können mit der ECM Primfaktoren von N mit bis etwa 40 Stellen gefunden werden, in Einzelfällen auch noch darüber.

8 Faktorisierungsmethoen, basierend auf der Legendreschen Kongruenz

Für die Faktorisierung wirklich großer Zahlen, wie z.B. die berühmten Zahlen RSA-129 und RSA-155, kämen allerdings alle bisher angeführten Faktorisierungsmethoden nicht in Frage. Tatsächlich wurden zu ihrer Faktorisierung das sog. Quadratische Sieb bzw. das Zahlkörpersieb verwendet (siehe [1]). Leider würde eine ausführliche Besprechung dieser Methoden den Rahmen dieser Arbeit bei weitem sprengen, doch seien wenigstens einige grundsätzliche Dinge noch angemerkt.

Ist N wieder die zu faktorisierende Zahl, so geht es bei beiden Methoden um das Auffinden von nichttrivialen Lösungen der sog. Legendreschen Kongruenz $x^2 \equiv y^2 \bmod N$, d.h. von Lösungen, für die gilt $x \equiv \pm y \bmod N$. N ist dann nämlich Teiler von $(x+y)(x-y)$, aber nicht auch Teiler von $x+y$ bzw. $x-y$, woraus folgt, dass man durch Berechnung von $\text{ggT}(x+y,N)$ bzw. $\text{ggT}(x-y,N)$ jeweils nichttriviale Faktoren von N erhält.

Beide Methoden verwenden ferner zur Erreichung dieses Ziels sog. Faktorbasen. In seiner einfachsten Form ist eine Faktorbasis $B = \{p_1, p_2, \ldots, p_m\}$ eine der Größe nach geordnete Menge von Primzahlen (mit der der eventuellen Ausnahme $p_1 = -1$). Nennt man dann b eine B-Zahl, wenn der kleinste nichtnegative

Rest (bzw. im Falle $p_1 = -1$ der kleinste Absoluttrest) $a = b^2 \bmod N$ als ein Produkt von (nicht notwendig verschiedenen) Zahlen aus B dargestellt werden kann, so gilt der grundlegende

Satz. *Sind bezüglich der Faktorbasis $B = \{p_1, p_2, \ldots, p_m\}$ B-Zahlen, für welche gilt*

$$b_i^2 \equiv p_1^{e_{i1}} p_2^{e_{i2}} \cdots p_m^{e_{im}} \bmod N, \quad i = 1, \ldots, n$$

und ist für sie die Summe der Vektoren

$$\mathbf{e}_i := (e_{i1} \bmod 2, e_{i2} \bmod 2, \ldots, e_{im} \bmod 2), \quad i = 1, 2, \ldots, n,$$

gleich $\mathbf{0}$ *im Vektorraum $\mathbb{Z}_2^m$, so sind dann*

$$x = b_1 b_2 \cdots b_n,\ y = p_1^{f_1} p_2^{f_2} \cdots p_m^{f_m} \quad \textit{mit} \quad f_j = \frac{1}{2} \sum_{i=1}^{n} e_{ij}, \quad j = 1, \ldots, m$$

Lösungen der Kongruenz $x^2 \equiv y^2 \bmod N$, welche für ein zusammengesetztes N mit einer Wahrscheinlichkeit von höchstens 50% trivial sind.

Nachfolgend als einfaches Beispiel für die Anwendung dieses Satzes die Faktorisierung von $N = 20569$ unter Verwendung der Faktorbasis $B = \{-1, 2, 3, 5\}$. Bei der Suche nach B-Zahlen ist es aussichtsreich, in der Nähe von $\lfloor\sqrt{N}\rfloor$ (oder allgemeiner $\lfloor\sqrt{kN}\rfloor$ für $k = 1, 2, 3, \ldots$) zu suchen, da die Quadrate dieser Zahlen mod N relativ klein sind. Um festzustellen, ob eine Zahl n über einer Faktorbasis B faktorisierbar ist bedienen wir uns dabei der eigens dafür geschriebenen Routine smooth(n, b).

$N := 20569$
$m :=$ FLOOR(SQRT(N)) $= 143$

smooth$(n, b) :=$
  PROG(
    IF($n < 0$ AND FIRST$(b) > 0$, RETURN false),
    $b :=$ PRODUCT(b),
    $n :=$ ITERATE($n_/$GCD$(n_, b), n_$, ABS(n)),
    SOLVE$(n = 1)$)

SELECT(smooth(MODS$(x^2, N), [-1, 2, 3, 5]), x, m - 10, m + 10) =$
  $[133, 137, 142, 143]$
TABLE(FACTOR(MODS$(x^2, N)), x, [133, 137, 142, 143]) =$
  $[[133, -2 \cdot 3 \cdot 5], [137, -2 \cdot 3 \cdot 5], [142, -3 \cdot 5], [143, -2 \cdot 3 \cdot 5]]$.

Nach obiger Rechnung sind also 133, 137, 142, 143 B-Zahlen für unsere Faktorbasis. Diesen sind folgende Exponentenvektoren zugeordnet:

$133 \to (1,6,2,1)$ (bzw. $(1,0,0,1)$ mod 2)
$137 \to (1,3,2,2)$ (bzw. $(1,1,0,0)$ mod 2)
$142 \to (1,0,4,1)$ (bzw. $(1,0,0,1)$ mod 2)
$143 \to (1,3,1,1)$ (bzw. $(1,1,1,1)$ mod 2).

Um eine nichttriviale Linearkombination dieser Vektoren zu finden, welche den Nullvektor mod 2 liefert, hätte man allgemein im Körper $\mathbb{Z}_2$ das folgende lineare Gleichungssystem zu lösen:

$$x_1(1,0,0,1)+x_2(1,1,0,0)+x_3(1,0,0,1)+x_4(1,1,1,1)=(0,0,0,0).$$

In diesem Fall sieht man auch so sehr schnell, dass sich z.B. die Vektoren für 133 und 142 mod 2 auf den Nullvektor ergänzen. Tatsächlich erhält man dann unter Anwendung des obigen Satzes mit $x = 133 \cdot 142 = 18886$ und $y = 2 \cdot 3 \cdot 5 = 1080$ die Faktorisierung $N = 67 \cdot 307$ von N:

$$[\mathrm{GCD}(x+y,n),\, \mathrm{GCD}(x-y,n)] = [67,307]$$

Bei der Generierung von B-Zahlen bedient man sich beim quadratischen Sieb allgemeiner quadratischer Polynome der Bauart $Q(x) := Ax^2+2Bx+C$, wobei wegen

$$A(Ax^2+2Bx+C) = (Ax^2+B)^2+(AC-B)^2$$

die Bedingung $N|AC-B^2$ sicherstellt, dass $AQ(x)$ als Werte stets Quadrate mod N liefert. (Tatsächlich haben auch wir in obigem Beispiel bei genauerem Hinsehen das Polynom $Q(x) = x^2 - N$ verwendet!) Für jede festgewählte Primzahl p in der Faktorbasis gilt dann mit $p|Q(x)$ auch $p|Q(x+kp)$ für jedes ganze k. Da ferner die Kongruenz $Q(x) \equiv 0$ mod p zwei Lösungen hat, liegen also alle x-Werte mit $p|Q(x)$ in zwei arithmetischen Folgen. Man benötigt also nur die Anfangsglieder dieser arithmetischen Folgen im Suchintervall, um dann gezielt und ohne Fehlversuche aus allen $Q(x)$ den Primfaktor p „auszusieben“.

Leider kann ich hier auf weitere Details nicht mehr eingehen. Es sei nur noch erwähnt, dass der Rechenaufwand beim Quadratischen Sieb durch

$$O\left(\exp\left(\sqrt{(1+o(1))\log N \log\log N}\right)\right)$$

begrenzt ist, während er beim Zahlenkörpersieb sogar nur

$$O\left(\exp\left((c+o(1))(\log N)^{1/3}(\log\log N)^{2/3}\right)\right)$$

für ein $c < 2$ beträgt. In der Praxis beginnt aber erst irgendwo im Bereich von 100–120 Stellen das vom „Overhead“ her wesentlich aufwändigere Zahlkörpersieb das Quadratische Sieb zu überholen und es stellt damit für wirklich große Zahlen die zur Zeit beste bekannte Faktorisierungsmethode auf klassischen Computern dar

(siehe [2]). Sollten letztere einmal durch Quantencomputer abgelöst werden, so wäre dann natürlich der heute schon dafür existierende Polynomialzeitalgorithmus von P. Shor (s. [6]) die Lösung des Faktorisierungsproblems schlechthin. Ob es aber je dazu kommen wird, vermag heute noch niemand zu sagen.

Literatur

1. R. Crandall and C. Pomerance, *Prime Numbers: a computational perspective*, Springer, 2000.

2. C. Pomerance, *A tale of two sieves*, Notices Amer. Math. Soc. **43** (1996), 1473–1485.

3. P. Ribenboim, *The New Book of Prime Number records*, 2nd ed., Springer, New York, 1995.

4. H. Riesel, *Prime Numbers and Computer Methods for Factorization*, 2nd ed., Birkhäuser, Boston, 1994.

5. J. Wiesenbauer, *Primzahltests und Faktorisierungsalgorithmen I*, Int. Math. Nachrichten **186** (2001), 9–23.

6. C. P. Williams and A. C. Clearwater, *Explorations in Quantum Computing*, TELOS-Reihe, Springer, New York, 1997.

7. H. Lenstra Jr., *Factoring integers with elliptic curves*, Ann. Math. **2** (1987), 649–673.

8. R. Schoof, *Elliptic curves over finite fields and the computation of square roots mod p*, Math. Comp. **44** (1985), 483–494.

Der Autor ist Dozent an der Technischen Universität Wien und hält dort seit vielen Jahren Vorlesungen über Computeranwendungen in Algebra und Zahlentheorie und Analyse von Algorithmen. Er ist Autor der Zahlentheorie-Bibliothek NUMBER.MTH von Derive 5 und war anlässlich eines Gastaufenthaltes bei Software House in Hawaii im Sommer 1999 auch maßgeblich an der Neugestaltung der internen Routinen von Derive 5, welche Primzahltests und Faktorisierungsalgorithmen von ganzen Zahlen betreffen, beteiligt.

Internat. Math. Nachrichten
Nr. 190 (2002), 37–42

Best Current Practices. Recommendations on Electronic Information Communication*

Committee on Electronic Information Communication

International Mathematical Union

Communication of mathematical research and scholarship is undergoing profound change as new technology creates new ways to disseminate and access the literature. More than technology is changing, however; the culture and practices of those who create, disseminate, and archive the mathematical literature are changing as well. For the sake of present and future mathematicians, we should shape those changes to make them suit the needs of the discipline.

For this reason, we have identified a number of *best practices* for those involved with the mathematical literature–mathematicians, librarians, and publishers. Many of these are practices that apply to other academic disciplines as well. Although we focus primarily on mathematics, we recognize that we can learn from each other as we move forward, and that no single discipline should act in isolation.

Our advice is meant to guide practice as it changes rather than to set forth a collection of firm rules and admonitions. The recommendations concern all forms of scholarly publishing and do not promote any particular form. Indeed, the authors of this document hold many differing views on the future of scholarly publishing. The common principle used to formulate our recommendations is that those who write, disseminate, and store mathematical literature should act in ways that serve the interests of mathematics, first and foremost.

This is advice that is meant to ease the transition in scholarly communication for present mathematicians. Most importantly, however, it is advice aimed at protecting mathematicians in the future.

*Endorsed by the IMU Executive Committee on April 13, 2002 in its 69^{th} *session in Paris, France* and printed with kind permission of Peter Michor.

ISSN 0020-7926

For Mathematicians

1. Structure and Format Logically structured documents correctly reflect the content of a mathematician's work, setting forth results, arguments, and explanations to make them understandable to readers. But a logical structure also makes it possible to retrieve and eventually to update the document. Identifying the constituent parts of an electronic document is essential in order to move from one format to another without human intervention. Authoring documents should be more than setting down mathematical research in a pleasing format.

Authors are encouraged to provide the structure necessary to use their documents now and in the future. The aim is to create a master file from which the various other formats can be derived. [In mathematics, LaTeX is a congenial and accessible way to give documents some structure without adding unreasonable burdens on the author.]

2. Linking and Enrichment. An electronic publication can offer much more than a print publication. Electronic publication gives the user the ability to move effortlessly among the various parts of a paper or even from one paper to another. In order to make this possible, however, someone must add the necessary information to establish links in the electronic version.

Adding links is easier when authors provide the information necessary to establish them. [Correct cross-referencing and citation in LaTeX transforms readily into hyperlinks, yielding enriched electronic versions of one's work. Hyperlinks may be used in PDF files as well.]

Moreover, electronic publication is not restricted by the constraints of the traditional print medium. This provides an opportunity to detail material that might otherwise be dismissed as "well known" and to add explanatory appendices. A little less easily, whenever appropriate, one may include graphic enhancements, animations, extensive data, tools to analyze that data, or even active examples that may be varied by the reader.

3. Versions. Online publication can lead to severe problems in citation, because the posted paper can be updated continuously until it bears little resemblance to the original, as an author corrects, adds, and deletes material without indicating that changes were made. As the mathematical literature grows, references to nonexistent papers and results will eventually jeopardize its coherence.

To avoid this problem, papers that have achieved a sufficiently final state should be stored in an immutable form. This includes any paper to which others may make reference, whether published in refereed journals or posted as a preprint. If revisions subsequently are necessary, each released version should be clearly labeled with its own version number and old versions should remain available.

4. Personal Homepages. Mathematical communication is more than merely posting or publishing papers. Information about the mathematical community and its activities is valuable to all mathematicians, and it is now easier than ever to circulate and to find such material.

Mathematicians are encouraged to have their own homepage. Ideally, basic data on such a page (or on a "secondary" homepage) should be presented in standard form to allow ready automatic compilation into databases.

[Material found at *http://www.math-net.org/Math-Net_Page_Help.html* describes the Math-Net project, which provides standardized homepages for departments and institutes.]

5. Personal Collected Works. Mathematics ages slowly. Access to older literature is important for most mathematicians, and yet much of the older literature is likely to remain unavailable in electronic form in the immediate future. Mathematicians can change that by taking collective action.

Whenever legally and technically possible, mathematicians are encouraged to scan their old (pre-TEX) papers and post them on their homepages, making their "collected work" readily available to all. This relatively small effort on the part of every mathematician will provide enormous benefit to the entire community.

The *Call to Mathematicians* found at *http://www.mathunion.org* provides further information.

6. Preprints and archives. Mathematical writing is ineffective if it is not communicated. A generation ago, the photocopier made it easy to send preprints to one's peers. Today, as a substitute, we have departmental servers, homepages, and public archives. [The arXiv (*http://www.arxiv.org/*) is one prominent example.]

It is a good practice to place one's preprints both on a homepage and in an appropriate archive. Either copy serves to communicate the mathematics to one's peers, but the public archive will make it more likely that others can reference your work in the future.

7. Copyright. While copyright is a complex subject that is far removed from mathematics, copyright law and policy can profoundly affect the ways in which mathematics is disseminated and used. Copyright is important for mathematicians.

Authors should be aware of the basic principles of copyright law and custom. Decisions about copyright for one's own work should be made thoughtfully.

The material found at *http://www.ceic.math.ca/* serves as a good reference.

For Librarians and Mathematicians

8. Journal Price and Policy. Libraries have limited budgets, which often grow more slowly than the prices of journals, forcing libraries to cancel subscriptions. The cumulative effect of cancellations goes beyond individual institutions because it shifts costs to an ever smaller number of subscribers, accelerating the process of price increase and cancellation. Journal prices matter to all mathematicians.

When deciding where to submit a paper an author may choose to be aware of a journal's standing and impact, but an author also should take account of a journal's price (as well as its general policies, including archiving). In addition, one might consider a journal's price and policies when considering whether to referee or serve on an editorial board.

9. Validation. Publication and peer review processes are increasingly detached. The emergence of overlay journals, archival preprint servers, and other new structures of publication raise new and pressing questions about the appropriate forms of validation. These are important issues for all scholarship, but even more important for mathematics since it is essential to know which parts of the mathematical literature are valid.

Both mathematicians and decision makers need to be alert to the distinction between posting and providing validation. Editorial boards should be explicit about the form and the level of validation they provide for papers and make this information plain to all users.

10. Statistics. Electronic delivery of information has changed the nature of statistics available to assess the usage and the 'value' of academic literature. Gathering statistics from the Internet is notoriously complicated, and even those who are knowledgeable about the pitfalls can be inadvertently or intentionally misled. As librarians and other decision makers increasingly rely on web statistics (such as the number of hits, page accesses or downloads) it is important to be informed about the nature of such measurements and the difficulty in gathering and interpreting them. Moreover, the value of a particular resource is often not best measured by simply counting the number of times it is currently used in some way. This is especially true in a field like mathematics in which current research continues to play such a significant role far into the future.

Given that statistics, while subject to misuse, are valuable and will be used, it is important that mathematics researchers and research librarians are alert to these rapidly changing issues and are prepared to make appropriate arguments for mathematics.

For Publishers and Mathematicians

11. Partial Access. Many journals restrict access to (paying) subscribers. As the web of mathematical literature grows, however, it will be increasingly important for all mathematicians to navigate that web, whether or not they have access to complete articles. This allows mathematicians to learn basic information about an article, even when they do not belong to institutions that have the financial resources to support the journal. It is especially advantageous to mathematicians from the developing world.

Journals should provide unrestricted access to tables of contents, abstracts of papers, and other data, such as keywords. Where practical, journals should also provide unrestricted access to reference lists with links, allowing all mathematicians to navigate the web of literature, even when they don't have access to the full-text of some parts of that web.

12. Eventual Free Access. The scholarly enterprise rests on the free exchange of ideas, and scholars need to have easy access to those ideas. Many journals, however, rely on subscriptions to recover costs and to provide an incentive to publish, forcing them to limit access to subscribers. Access should be a balance between those two needs, of scholars and of publishers.

Limiting access to subscribers for a fixed period of time after publication may be necessary for many journals. In order to ensure appropriate accessibility for the electronic literature, we encourage all journals to grant free access after that fixed period of time.

13. Archiving format. Ensuring the success of long-term archiving is more than storing the electronic data on reliable media in multiple locations. As software and formats change in the future, the data will require modification and updating. Not all electronic formats are suitable for these purposes.

In general, electronic documents should be stored in their most primitive format, that is, the format used to derive subsequent formats. Any format in which material is stored should follow an "open standard" that has a detailed public specification. This will increase the likelihood that scholars working decades or centuries from now will be able to use the material.

14. Archiving responsibility. Traditionally, maintaining the older literature has been the responsibility of librarians rather than publishers. Even in the electronic age, scholars and the librarians who represent them have the greatest motivation among all of the affected parties to ensure the preservation of older material.

We recommend that electronic archives of the mathematical literature should ultimately be under the control of the academic community.

15. Licensing and Bundling. Some licensing and bundling arrangements for journals accelerate the transfer of control of our literature away from mathemati-

cians and research librarians. When institutions are forced to accept or reject large collections of scholarly literature covering many different disciplines, the decisions are less likely to be made by scholars. As a consequence, the normal processes that promote the highest quality journals become less effective.

The best protection, as always, comes through staying well informed and alert to these issues. In general, decisions about journal adoptions and cancellations should be made by academics and librarians.

Postscript on Developing Countries. Today, active mathematicians depend on access to electronic information–online journals, databases of reviews, and preprint servers. More than access, research mathematicians need the tools to create and edit documents in standard formats [such as LaTeX Postscript, and PDF]. This is true for mathematicians everywhere, including those in developing countries. Implementing many of the recommendations in the preceding document makes little sense if mathematicians are not connected to the Internet or have no tools to create electronic documents.

National mathematical societies and academies in developing countries need to impress on their governments the need to establish the infrastructure necessary to provide high speed connectivity among academic institutions.

The entire mathematics community should encourage and support specific actions designed to help in this effort, which include:

1. Establishing "mirror" services that provide quick access to users of electronic services within each region.

2. Establishing local help and service centers that spread expertise on the use of common standards [for example, LaTeX].

3. Creating small groups who tour the region and demonstrate the use of technology for research and study.

Because scholarly communication is changing rapidly, there is great urgency to begin these efforts.

Remark: The above recommendations have been stated in very general form. Whenever reference to existing formats [e.g. LaTeX, PDF], to archiving systems [e.g. arXiv], or to information and communication systems [e.g. Math-Net] has been made this is meant for illustration and not to promote these formats and systems. The IMU EC has asked CEIC to enhance, whenever appropriate and useful, individual recommendations by adding links to web pages that explain some of the technical issues involved, provide additional information, or contain (possibly controversial) discussions of the topics addressed. These links will be under the responsibility of CEIC and are not subject of the IMU EC recommendations.

Internat. Math. Nachrichten
Nr. 190 (2002), 43–46

Das Kompetenzzentrum Industriemathematik (IMCC) in Linz

Andreas Binder

MathConsult GmbH

Mit 1. Jänner 2002 hat das Kompetenzzentrum Industriemathematik (Industrial Mathematics Competence Center – IMCC) in Linz seinen Vollbetrieb aufgenommen. Das IMCC ist ein Kompetenzzentrum in der Aktionslinie Kind des Bundesministeriums für Wirtschaft und Arbeit (BMWA) und wird aus Mitteln des BMWA, des Landes Oberösterreich und aus Geld- und Sachleistungen der Partnerunternehmen finanziert. Rechtsträger des IMCC ist die seit 1996 bestehende MathConsult GmbH, Linz.

Die Bedeutung der mathematischen Modellierung, Simulation und Optimierung hat in den letzten Jahrzehnten stetig zugenommen. Dies auch deshalb, weil es durch die rasante Entwicklung auf dem Gebiet der Hardware möglich geworden ist, technische Prozesse wesentlich realistischer als früher zu modellieren und zu simulieren, insbesondere auch ohne Dimensionsreduktion, d.h. z.B. voll dreidimensional und/oder transient und nicht nur, wie früher, in vereinfachten Geometrien (etwa rotationssymmetrisch) und unter Vernachlässigung des zeitlichen Ablaufs. Diese neuen Hardwaremöglichkeiten haben zu einer ebenso rasanten Zunahme der Forschung auf dem Gebiet der Entwicklung entsprechender schneller und robuster Algorithmen geführt. Auch auf dem Gebiet der Modellierung und Simulation wirtschaftlicher Prozesse hat es in den letzten Jahren wesentliche Fortschritte gegeben.

Das Ziel des IMCC ist es, die in den Partnerunternehmen des IMCC, beim Rechtsträger des IMCC und bei den akademischen Partnern des IMCC vorhandene Kompetenz im Bereich der industriellen Forschung auf dem Gebiet der Industriemathematik zu fokussieren. Insbesondere konzentriert sich das IMCC auf die Arbeit an mathematischen Verfahren für Aufgabenstellungen, die durch Anwendungsprobleme der Partnerunternehmen motiviert sind.

ISSN 0020-7926

Die Förderung des IMCC als K_{ind}-Kompetenzzentrum verstärkt die gute Positionierung von Linz im Bereich der Industriemathematik weiter und stellt natürlich auch große Herausforderungen an die Beteiligten.

Die Partner des IMCC

Als Rechtsträger des IMCC fungiert die MathConsult GmbH, die 1996 als ein Spin-Off des Linzer Instituts für Industriemathematik gegründet wurde und seither an Aufgabenstellungen der numerischen Simulation arbeitet (sowohl für technische Aufgabenstellungen als auch für Aufgabenstellungen im Bereich der Bewertung von Finanzderivaten).

Die Partnerunternehmen des IMCC sind:

- AVL List GmbH, Graz: Die AVL ist das weltweit größte unabhängige Unternehmen im Bereich der Forschung und Entwicklung von Verbrennungskraftmaschinen und Antriebssträngen.
- GE Medical Systems Kretztechnik GmbH & Co OHG, Zipf: Die GE Medical Systems Kretztechnik ist ein führender Anbieter von 3D- und 4D-Ultraschallgeräten für die medizinische Diagnostik.
- Henkel KGaA, Düsseldorf: Die Henkel KGaA ist ein führender europäischer Markenartikelhersteller.
- VOEST-Alpine Industrieanlagenbau GmbH & Co, Linz: Die VAI ist ein big player im Anlagenbau, insbesondere im Bereich der Eisenhütten und Stahlwerke.

Wissenschaftliche Leitung:

- o.Univ.Prof. Dr. Heinz Engl (Institut für Industriemathematik, Universität Linz) ist der wissenschaftliche Gesamtleiter des IMCC und gleichzeitig Leiter des Bereichs „Numerische Simulation und Optimierung“
- o.Univ.Prof. Dr. Manfred Deistler (Institut für Ökonometrie, Operations Research und Systemtheorie, TU Wien) leitet den Bereich „Statistik, Ökonometrie und Systemtheorie“
- Univ.Prof. Dr. Otmar Scherzer (Institut für Informatik, Universität Innsbruck) leitet den Bereich „Mathematische Methoden in der Bildverarbeitung“.

Das IMCC hat zur Zeit 15 wissenschaftliche Mitarbeiter, zum größten Teil Mathematiker/innen, zum Teil mit Doktorat.

Das Arbeitsprogramm des IMCC

Die inhaltliche Arbeit am IMCC wird in Methodenprojekten und in Umsetzungsprojekten organisiert:

Methodenprojekte dienen der Erforschung und Vertiefung mathematischer Methoden insbesondere in folgenden Forschungsfeldern:

- Numerische Methoden für stark nichtlineare partielle und gewöhnliche Differentialgleichungen (auch Algebrodifferentialgleichungen) und für komplexe Systeme von Differentialgleichungen.
- Optimale Steuerung, Optimierung und Parameteridentifikation von Systemen, die durch (Systeme von) partielle(n) Differentialgleichungen beschrieben werden.
- Numerische Methoden in der Bildverarbeitung.
- Identifikation von dynamischen Systemen, Zeitreihenanalyse.

Zwischen diesen Methodenprojekten bestehen inhaltliche Querverbindungen. Typisch ist auch, dass die mathematischen Modelle (also etwa: sehr große Systeme steifer Differentialgleichungen) für Aufgabenstellungen mehrerer Partnerunternehmen von Bedeutung sind.

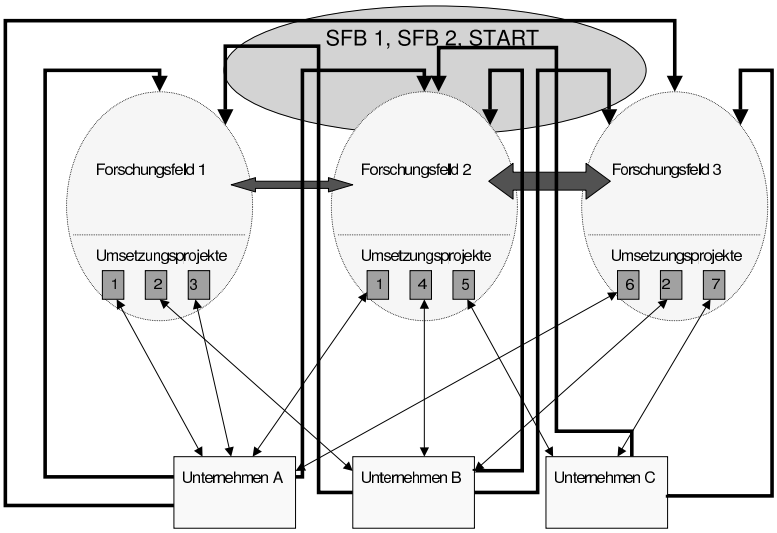
Die Anwendbarkeit der so entwickelten oder vertieften Methoden und Algorithmen soll dann in Umsetzungsprojekten prototypisch demonstriert werden, beispielsweise in:

- Numerische Simulation und Optimierung in Mechanik und Mehrkörperdynamik für die Motorensimulation.
- Kinetisches Modell zur Hochofenkontrolle.
- Segmentierung von Hi/Low Contrast Objekten in 3D/4D.
- Ökonometrische Analysen im Bereich Marketing.

Es handelt sich hier um einen mehrstufigen Prozess: von der Methodenentwicklung über den ersten Umsetzungs-Prototyp bis hin zur Vertiefung der Methodenentwicklung.

Die Grafik auf der folgenden Seite soll die grundsätzliche Organisation veranschaulichen:

Im Hintergrund des IMCC steht die starke Verankerung der wissenschaftlichen Bereichsleiter in der Grundlagenforschung (Deistler und Engl in SFBs, Scherzer ist START-Preisträger). Kennzeichnend ist weiters, dass Aufgabenstellungen



der Unternehmen in die Formulierungen der Methodenprojekte für mehrere Forschungsfelder einfließen und dass Umsetzungsprojekte die Ergebnisse mehrerer Methodenprojekte benötigen.

Transferprojekte

Im Rahmen des IMCC ist es geplant und erwünscht, Methoden, die in Methodenprojekten entwickelt wurden, einem weiteren Nutzerkreis als den Partnerunternehmen des IMCC, insbesondere auch kleinen und mittleren Unternehmen, zugänglich zu machen und Transferprojekte durchzuführen.

Der Autor Dr. Andreas Binder ist Geschäftsführer der MathConsult GmbH, Altenbergerstr. 74, 4040 Linz.
binder@mathconsult.co.at *http://imcc.indmath.uni-linz.ac.at*

Internat. Math. Nachrichten
Nr. 190 (2002), 47–55

Känguru der Mathematik 2002

Michael Hofer

Technische Universität Wien

Seit 10 Jahren gibt es den Internationalen Wettbewerb *Känguru der Mathematik*, und seit 5 Jahren ist auch Österreich daran beteiligt. Jedes Jahr am dritten Donnerstag im März lösen über 2 Millionen Schülerinnen und Schüler im Alter von 8–18 Jahren in mehr als 30 Staaten Europas und darüber hinaus in den 5 Kategorien *Écolier, Benjamin, Kadett, Junior* und *Student* die Wettbewerbsbeispiele. Diese haben denksportartigen Charakter und sollen den Teilnehmerinnen und Teilnehmern vor allem Freude an der Mathematik vermitteln. In den Kategorien Écolier und Benjamin sind 24 multiple choice-Aufgaben in 60 Minuten zu lösen, in den Kategorien Kadett, Junior und Student 30 Aufgaben in 75 Minuten. Die jeweils 8 (in den ersten beiden Kategorien) und 10 (in den restlichen drei) 3-, 4- und 5-Punkte-Aufgaben entstammen verschiedensten mathematischen Gebieten – von der Geometrie über die Analysis bis zur Zahlentheorie. Mit 24 (30) Basispunkten können also 120 (150) Punkte erreicht werden. Für genauere Informationen zum Ablauf des Wettbewerbs sei auf [1] verwiesen.

Die *Australian Kangaroo Nugget*-Goldmünze 2002.

Das *Känguru der Mathematik* als Mathematikwettbewerb in den Schulen hat will die Begeisterung an der Mathematik bei möglichst vielen Kindern und Jugendlichen wecken. Ein Nebeneffekt ist, dass immer wieder Schülerinnen und Schüler durch die Teilnahme am *Känguru der Mathematik* Lust auf weitere mathematische Wettbewerbe haben und so z.B. auch zur Mathematik-Olympiade kommen können.

ISSN 0020-7926

Am 21. März 2002 haben in Österreich 100.000 Kinder und Jugendliche am internationalen Wettbewerb *Känguru der Mathematik* teilgenommen. Die erbrachten Leistungen wurden in Form von Schul- und Landessiegerehrungen gewürdigt. Die besten jeder Kategorie sind am 21. Juni 2002 im Bundesministerium für Bildung, Wissenschaft und Kultur geehrt worden. Dort haben sie als Preis unter anderem eine australische Känguru-Goldmünze erhalten, eine symbolische Verbindung zur Australian Mathematics Competition, von welcher die Idee für einen europäischen Wettbewerb dieser Art stammt. Von den Wettbewerbsbeispielen des Jahres 2002 stellen wir hier exemplarisch die *Gruppe Student* (11. und 12. Schulstufe) vor. Die österreichischen Wettbewerbsbeispiele des Jahres 2002 der restlichen Kategorien finden Sie auf der Webseite *http://www.geometrie.tuwien.ac.at/kaenguru/*. Wettbewerbsbeispiele früherer Jahre und Musterlösungen dazu finden Sie im Downloadbereich Mathematik der Webseite *http://arge.stvg.at/*. Das *Känguru der Mathematik* 2003 findet am 20. März 2003 in allen teilnehmenden Schulen statt.

Bundessiegerinnen und Bundessieger der Schulstufen 3 bis 12 beim Empfang im Bundesministerium am 21. Juni 2002. Von links nach rechts: Karl Rupp, Markus Legner, Markus Riegler, Markus Rothschädl, Iris Murer, David Kreuzwiesner, Bundesministerin Elisabeth Gehrer, Josef Baumgartner, Birgit Vera Schmidt, Johannes Eder, Markus Weger.

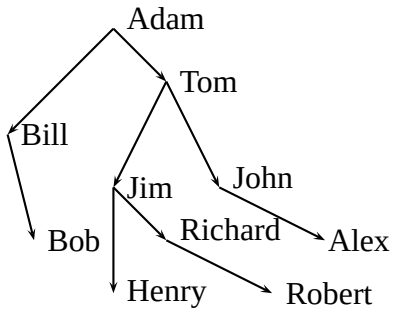
Die Wettbewerbsbeispiele der Kategorie „Student“

3 Punkte-Probleme

1. Ein Känguru springt von Bukarest nach Paris (2500 km), wobei es mit jedem Sprung doppelt so weit springt wie mit dem Sprung davor. Sein erster Sprung ist 1m lang. Nach wie viel Sprüngen ist es Paris am nächsten?

(**A**) 11 (**B**) 12 (**C**) 22 (**D**) 20 (**E**) 21

2. Robert betrachtet seinen Stammbaum, in dem nur männliche Ahnen eingetragen sind. Die Pfeile zeigen jeweils von Vätern zu ihren Söhnen. Wie heißt der Sohn des Bruders des Großvaters des Bruders von Roberts Vater?



(**A**) Jon (**B**) Alex
(**C**) Tom (**D**) Bob
(**E**) Ein anderer Name

3. Eine Seitenfläche eines Polyeders ist ein Fünfeck. Was ist die kleinste Zahl der Seitenflächen, die das Polyeder haben kann?

(**A**) 5 (**B**) 6 (**C**) 7 (**D**) 8 (**E**) 10

4. Ein Hotel ist in den drei Sommermonaten zu 88% ausgelastet und in den restlichen Monaten zu 44%. Wie hoch ist die Auslastung des Hotels über das ganze Jahr?

(**A**) 132% (**B**) 66% (**C**) 55%
(**D**) 44% (**E**) Eine andere Zahl

5. Wenn a und b positive ganze Zahlen mit dem größten gemeinsamen Teiler 3 sind und $\frac{a}{b} = 0,4$ gilt, wie groß ist dann ab?

(**A**) 18 (**B**) 10 (**C**) 36 (**D**) 30 (**E**) 90

6. Ein Prisma hat 2002 Eckpunkte. Wie viele Kanten hat das Prisma?

(**A**) 3003 (**B**) 1001 (**C**) 2002 (**D**) 4002 (**E**) 2001

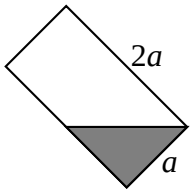
7. Wenn Wasser friert, nimmt sein Volumen um $\frac{1}{11}$ zu. Um welchen Bruchteil nimmt sein Volumen ab, wenn es wieder schmilzt?

(**A**) $\frac{1}{10}$ (**B**) $\frac{1}{11}$ (**C**) $\frac{1}{12}$ (**D**) $\frac{1}{13}$ (**E**) $\frac{1}{14}$

8. Ordne $\sin 1$, $\sin 2$, $\sin 3$ von der kleinsten zur größten Zahl. (Die Winkel sind in Bogenmaß angegeben.)

(**A**) $\sin 1 < \sin 2 < \sin 3$ (**B**) $\sin 3 < \sin 2 < \sin 1$ (**C**) $\sin 1 < \sin 3 < \sin 2$
(**D**) $\sin 2 < \sin 1 < \sin 3$ (**E**) $\sin 3 < \sin 1 < \sin 2$

9. Ein zylindrisches Trinkglas wird teilweise mit Wasser gefüllt und wie in der Zeichnung mit 45° geneigt gehalten. Welcher Prozentanteil des Glases ist gefüllt?



(**A**) Weniger als 25% (**B**) 25%
(**C**) 33% (**D**) 33 $\frac{1}{3}$%
(**E**) Mehr als 33 $\frac{1}{3}$%

10. Der Äquator ist etwa 40 000 km lang. Die Länge des Breitenkreises bei 60° im Norden ist

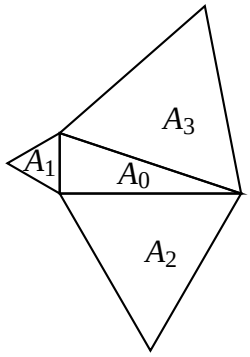
(**A**) 34 600 km (**B**) 23 500 km (**C**) 26 700 km
(**D**) 30 000 km (**E**) Eine andere Zahl

4 Punkte-Probleme

11. Das Alphabet der Sprache des Polabau-Volkes ist aus nur 6 Buchstaben zusammengesetzt, nämlich A, B, E, L, R und S (in dieser Reihenfolge). Die Wörter der Polabauer sind genau die geordneten Sequenzen dieser Buchstaben, wobei jeder Buchstabe in jedem Wort genau einmal vorkommt. Welches Wort kommt in ihrem amtlichen Wörterbuch an der 537. Stelle vor?

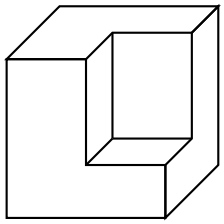
(**A**) REBLAS (**B**) SBERLA (**C**) LERBAS
(**D**) RABLES (**E**) ARBELS

12. In diesem Bild sehen wir 4 Dreiecke mit den Flächen A_i $(i = 0,1,2,3)$. Das Dreieck mit der Fläche A_0 ist rechtwinklig und die übrigen sind gleichseitig. Dann gilt



(**A**) $A_1 + A_2 = A_3$
(**B**) $(A_1)^2 + (A_2)^2 = (A_3)^2$
(**C**) $A_1 + A_2 + A_3 = 3A_0$
(**D**) $A_1 + A_2 = \sqrt{2}A_3$
(**E**) etwas Anderes

13. Die abgebildete abstrakte Statue wurde aus einem würfelförmigen Stein gehauen. Das Volumen dieses ursprünglichen Steins war $512dm^3$. Wie groß ist die Oberfläche der Statue?



(**A**) $320dm^2$ (**B**) $336dm^2$
(**C**) $384dm^2$ (**D**) $468dm^2$
(**E**) Man kann dieses Problem nicht ohne zusätzliche Information lösen

14. Peter und sein Sohn und Johann und sein Sohn waren fischen. Peter hat gleich viele Fische wie sein Sohn gefangen. Johann hat dreimal so viele Fische wie sein Sohn gefangen. Zusammen haben sie 35 Fische gefangen. Peters Sohn ist Lukas. Wie heißt Johanns Sohn?

(**A**) Diese Situation ist unmöglich (**B**) Johann
(**C**) Peter (**D**) Lukas
(**E**) Es ist nicht genug Information angegeben, um das zu wissen

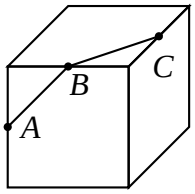
15. Zehn Mannschaften bestreiten ein Tischtennisturnier, in dem jede Mannschaft gegen jede andere genau einmal spielt. In jeder Partie erhält die Siegermannschaft 3 Punkte und die unterlegene 0 Punkte. Im Fall eines Unentschieden erhalten beide Mannschaften je einen Punkt. Im Turnier werden an alle Mannschaften insgesamt 130 Punkte vergeben. Wie viele Partien endeten unentschieden?

(**A**) 1 (**B**) 2 (**C**) 3 (**D**) 4 (**E**) 5

16. Durch die Einführung einer Innovation kann ein Betrieb seine Unkosten um 50% senken. Durch eine zweite senken sich die Unkosten um 40% und durch eine dritte um 10%. Um wie viel senken sich die Unkosten bei gleichzeitiger Einführung aller drei Innovationen, (die voneinander unabhängig sind)?

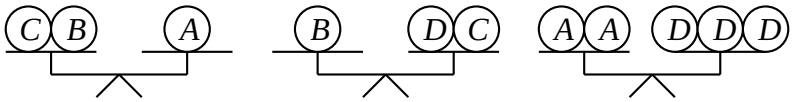
(**A**) 100% (**B**) 73% (**C**) 92% (**D**) 87% (**E**) 67%

17. Bestimme den Winkel, den die Strecken AB und BC miteinander einschließen, wobei A, B und C die Mittelpunkte der jeweiligen Würfelkanten sind.



(**A**) 90° (**B**) 100° (**C**) 110° (**D**) 120° (**E**) 135°

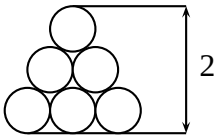
18. Wie viele Gewichte C balancieren ein Gewicht B?



.

(**A**) 2 (**B**) 3 (**C**) 5 (**D**) 6 (**E**) 7

19. Das 'Dreieck' in der Abbildung besteht aus berührenden Kreisen mit demselben Radius r. Die Höhe des 'Dreiecks' ist 2. Wie groß ist r?



(**A**) $\frac{1}{1+\sqrt{3}}$ (**B**) $\frac{2}{1+\sqrt{3}}$ (**C**) $\frac{2}{2+\sqrt{3}}$

(**D**) $\frac{1}{2+\sqrt{3}}$ (**E**) Ein anderer Wert

20. Achilles läuft los, um die vor ihm gestartete Schildkröte zu überholen. Zu Beginn beträgt der Abstand zwischen den beiden 990 m. Achilles läuft mit der Geschwindigkeit von 10 Meter pro Sekunde und die Schildkröte mit der Geschwindigkeit von 1 Meter pro 10 Sekunden. Wann überholt Achilles die Schildkröte?

(**A**) in 1 min 40 sec (**B**) in 990 sec (**C**) in 1 min 39 sec

(**D**) in 1 min 50 sec (**E**) nie

5 Punkte-Probleme

21. In einer Folge positiver Zahlen ist jedes Folgenglied außer den ersten beiden die Summe aller Vorgänger. Das elfte Glied der Folge ist 1000 und das erste Glied ist 1. Was ist das zweite Glied?

(**A**) 2 (**B**) $\frac{93}{32}$ (**C**) $\frac{250}{64}$

(**D**) $\frac{109}{16}$ (**E**) Eine andere Zahl

22. Es seien 10 Punkte in der Ebene gegeben. Fünf davon liegen auf einer gemeinsamen Gerade und keine andere Gerade geht durch mehr als zwei der Punkte. Wie viele Dreiecke gibt es, deren Eckpunkte alle zu diesen 10 Punkten gehören?

(**A**) 20 (**B**) 50 (**C**) 70 (**D**) 100 (**E**) 110

23. Gegeben sei die Zahl $2002! = 1 \cdot 2 \cdot 3 \cdots 2002$. Offensichtlich ist 2001 ein Teiler von 2002!, weil $2002! = 2000! \cdot 2001 \cdot 2002$ gilt. Das größte k, für das 2001^k die Zahl 2002! teilt, ist

(**A**) 101 (**B**) 71 (**C**) 69 (**D**) 2 (**E**) 1

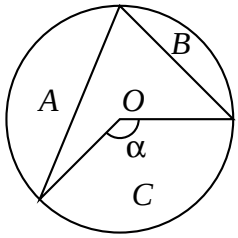
24. In zwei Gruppen sind zusammen mehr als 27 Personen. Die Anzahl der Personen in der ersten Gruppe ist mehr als doppelt so groß wie die Anzahl in der zweiten Gruppe, vermindert um 12. Die Anzahl in der zweiten Gruppe ist mehr als 9 Mal so groß wie die Anzahl in der ersten, vermindert um 10. Wie viele Personen sind in jeder Gruppe?

(**A**) 12 und 18 (**B**) 11 und 17 (**C**) 10 und 20
(**D**) 13 und 15 (**E**) Man kann das nicht feststellen

25. Wie viele nicht-kongruente Dreiecke haben ihre Eckpunkte in den Eckpunkten eines regelmäßigen Zehnecks?

(**A**) 6 (**B**) 7 (**C**) 8
(**D**) 9 (**E**) Eine andere Anzahl

26. Der Kreis im Bild hat seinen Mittelpunkt in O und den Radius 1. Der Winkel α ist kleiner als π. Die Fläche der Region A ist gleich $\frac{5\pi}{12} - \frac{1}{4}$ und die Fläche der Region B ist $\frac{\pi}{4} - \frac{1}{2}$. Die Fläche der Region C ist dann gleich



(**A**) $\frac{\pi}{4}$ (**B**) $\frac{\pi}{3}$ (**C**) $\frac{2\pi}{3}$ (**D**) $\frac{\pi}{6}$ (**E**) $\frac{5\pi}{12}$

27. Wie viele Zahlen von 1 bis 10^{2002} haben die Ziffernsumme 2?

(**A**) 2007006 (**B**) 2005003 (**C**) 2003001
(**D**) 2005002 (**E**) Eine andere Anzahl

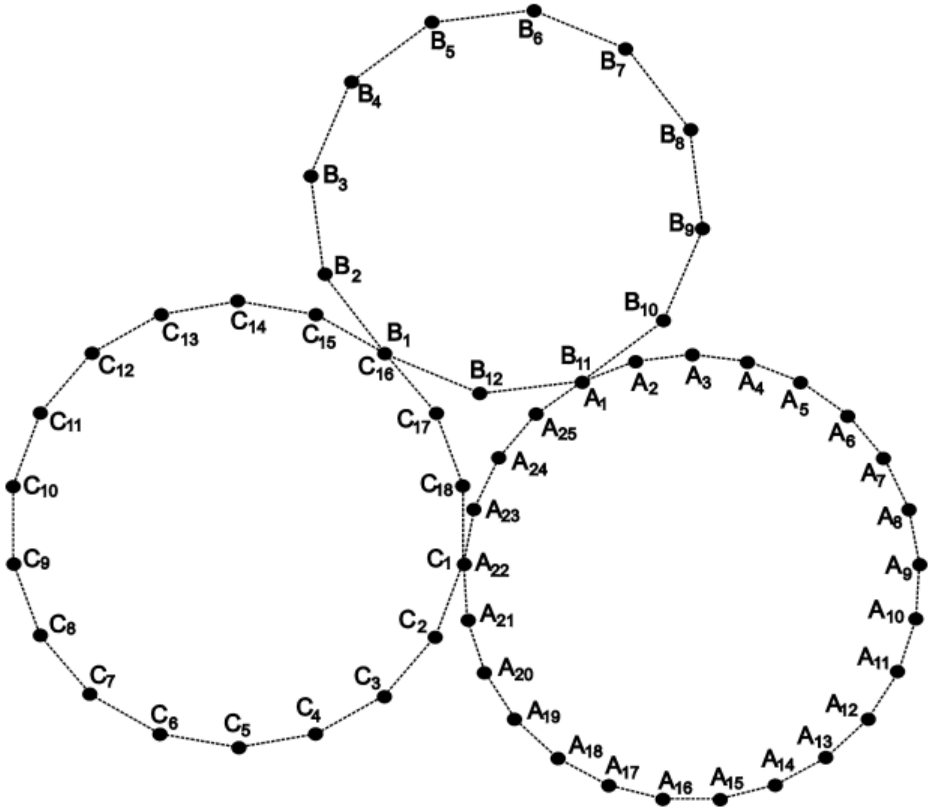
28. In einem Behälter befinden sich 21 Liter einer 18%-igen Alkohollösung. Wie viel Liter müssen durch eine 90%-ige Alkohollösung ersetzt werden, damit man eine 42%-ige Lösung erhält?

(**A**) 3 (**B**) 5 (**C**) 7 (**D**) 9 (**E**) 11

29. Es sei $a+b+c=7$, $\frac{1}{a+b} + \frac{1}{b+c} + \frac{1}{c+a} = \frac{7}{10}$. Dann gilt $\frac{a}{b+c} + \frac{b}{c+a} + \frac{c}{a+b} =$

(**A**) $\frac{19}{10}$ (**B**) $\frac{17}{10}$ (**C**) $\frac{9}{7}$ (**D**) $\frac{3}{2}$ (**E**) $\frac{10}{7}$

30. In diesem Bild sehen wir ein Brettspiel mit nummerierten Feldern A_1 bis A_{25}, B_1 bis B_{12} und C_1 bis C_{18}. Eine Spielfigur beginnt auf A_1 und bewegt sich nach folgender Regel: mit jedem Zug kann die Spielfigur auf das übernächste Feld in jeder Richtung auf dem selben Kreis ziehen. Erlaubt ist z.B. die Zugfolge $C_5 \to C_3 \to C_1 = A_{22} \to A_{20} \to A_{18} \to A_{20}$, aber man darf nicht direkt von C_2 zu A_{23} ziehen. Wie viele Felder gibt es, die man im Spiel überhaupt nicht erreichen kann?



(**A**) 0 (**B**) 6 (**C**) 15 (**D**) 27 (**E**) 30

Lösungen

1.E	2.D	3.B	4.C	5.E	6.A	7.C	8.E	9.B	10.E
11.A	12.A	13.C	14.C	15.E	16.B	17.D	18.C	19.A	20.A
21.B	22.E	23.B	24.B	25.C	26.B	27.B	28.C	29.A	30.B

Literatur

1. M. Hofer, R. Geretschläger, Internationaler Wettbewerb Känguru der Mathematik, Internat. Math. Nachrichten Nr. 187 (2001), 49-56

2. *http://www.geometrie.tuwien.ac.at/kaenguru/*

2. *http://arge.stvg.at/*

3. *http://www.mathkang.org/*

Buchbesprechungen

Allgemeines und Geschichte — General and History — Généralités, histoire

J. Arndt, Ch. Haenel: Pi — Unleashed. Translated from the German by C. and D. Lischka. With CD-ROM. Springer, Berlin u.a. 2001, XII+270 S. ISBN 3-540-66572-2 P/b DM 59,–.

Es liegt nun die zweite, wesentlich überarbeitete und erweiterte Auflage der deutschen Erstfassung vor (Pi. Algorithmen, Computer, Arithmetik, 1998), wieder mit beigefügter CD-ROM. Der Leser findet die unterschiedlichen Zugangsversuche der Menschen, sowohl der Mathematiker als auch der Anwender, zur Zahl π in den vergangenen 4000 Jahren. Die mathematischen Modelle der jeweiligen Ideen können von der CD-ROM abgerufen und visualisiert werden.

Folgende Zugänge zu π zeigen den umfassenden Charakter dieses Lehrbuches: Statistische Fragestellungen; Approximation von π durch stetige Funktionen, insbesondere durch die Arcustangensfunktion; Ansätze von Gauss, Ramanujan, Peter und Jonathan Borwein zu π; unterschiedliche arithmetische Aussagen über π; sehr rasche Algorithmen zur Berechnung sehr vieler Stellen von π; Internetadressen zu π-Projekten; Formelsammlungen von π und Angabe der Stellen von π in unterschiedlichen Zahlenformaten; und natürlich die historischen Versuche zur Charakterisierung von π, vermischt mit den bekannten (und zum Teil weniger bekannten) bunten Aussagen im Umfeld von π.

Sicherlich liegt hier ein sehr empfehlenswertes Lehrbuch für den Lehr- und Lernbetrieb im Bereich der Anfangssemester des Mathematikstudiums an Universitäten vor.

P. Paukowitsch (Wien)

Ch. Godsil, G. Royle: Algebraic Graph Theory. With 120 Illustrations. (Graduate Texts in Mathematics 207.) Springer, New York u.a. 2001, XIX+439 S. ISBN 0-387-95220-9 P/b DM 89,-, ISBN 0-387-95241-1 H/b DM 149,–*.

Zwischen Graphentheorie und Algebra (sowohl Linearer Algebra wie Strukturalgebra) gibt es viele Beziehungen, und zwar durchaus in beiden Richtungen. Diese gegenseitigen Anwendungen sind in umfassender und tiefgehender Form der Gegenstand dieser hervorragenden Monographie, die sich an (sehr) fortgeschrittene Studierende und Forscher wendet. Dabei werden jedoch stets alle wesentlichen Vorkenntnisse und Methoden bereitgestellt. Das Werk kann thematisch in drei große Teile gegliedert werden. Im ersten Teil werden neben den graphentheoretischen Grundlagen die Beziehungen zur Gruppentheorie behandelt: Automorphismen, Homomorphismen, knoten-transitive Graphen (und ihr Zusammenhang), kanten-transitive Graphen, spezielle Graphen und ihre Gruppen, Moore-Graphen, verallgemeinerte Polygone, Kneser-Graphen (fractional colourings, Erdős-Ko-Rado theorem). Der zweite Teil studiert die Anwendungen von Methoden der Linearen Algebra in der Graphentheorie: Matrizen und Eigenvektoren, Methode des "Interlacing" von Eigenwerten, Fullerene, stark reguläre Graphen, two-graphs (Geraden, wo der Winkel zwischen je zweien derselbe ist), kleinster Eigenwert, line graphs, Laplace-Matrix, Schnitte und Flüsse. Der dritte Teil stellt die Anwendungen der Graphentheorie mittels Rangpolynom und Jones-Polynom insbesondere in der Knotentheorie dar: Matroide, Anwendungen des Rang-Polynoms, Jones-Polynom als Knoteninvariante, Knoten und Eulersche Graphen. Jedes Kapitel enthält zahlreiche Aufgaben und Probleme (zum Teil sehr anspruchsvoll), Hinweise und (knappe) Literaturangaben. Den Autoren gelingt es vorzüglich, den besonderen Reiz des Zusammenwirkens von zunächst sehr unterschiedlichen und getrennt erscheinenden Teilgebieten der Mathematik herauszuarbeiten. Es wird eine riesige Fülle an Material, Details und Beispielen präsentiert, die oft aus der aktuellen Forschung stammen. Ein Buch, das viele Überraschungen birgt und für sehr lange Zeit faszinierenden Lesestoff bietet.

W. Dörfler (Klagenfurt)

W. D. Wallis: Magic Graphs. Birkhäuser Verlag, Boston, Basel, Berlin, 2001, XIV+146 S. ISBN 0-8176-4252-8, 3-7643-4252-8 P/b sFr 78,00.

Beginnend mit Arbeiten von Sedlacek, Kotzig und Rosa sind magische Graphen seit gut vierzig Jahren Gegenstand vielfältiger Untersuchungen. Dabei werden die wohlbekannten Konzepte magischer Quadrate und Rechtecke auf Graphen verallgemeinert. Man unterscheidet zwischen kantenmagischen, knotenmagischen und vollständig magischen Graphen. So ist ein Graph $G(V,E)$ mit $|V| = n$, $|E| = m$

kantenmagisch, wenn es eine ganzzahlige Konstante $k > 0$ und eine bijektive Abbildung f, $f : (V \cup E) \to \{1, 2, \ldots, n+m\}$, so gibt, dass für jede Kante uv die Beziehung $f(u) + f(uv) + f(v) = k$ erfüllt ist. Knotenmagisch ist ein Graph dann, wenn es eine ganzzahlige Konstante $h > 0$ so gibt, dass für jeden Knoten v die Beziehung $f(v) + \sum f(vu) = h$ erfüllt ist, wobei über alle zu v adjazenten Knoten u summiert wird. Ist ein Graph sowohl kanten- als auch knotenmagisch, so nennt man ihn vollständig magisch.

In drei getrennten Kapiteln werden Graphen, die diese Bedingungen erfüllen, untersucht. Die Darstellungen der Ergebnisse und Beweise sind elementar gehalten und somit auch für den Nichtspezialisten leicht nachvollziehbar. Da dieses Buch aus Vorlesungsunterlagen des Autors entstanden ist, enthält es auch eine Fülle von — im Anhang gelösten — Übungsaufgaben. Neben diesen Übungsaufgaben werden zu jedem Kapitel auch einige offene Probleme angegeben. Das Buch ist also durchaus auch geeignet, das Interesse an kombinatorischen Problemstellungen beim interessierten, fortgeschrittenen Studenten zu fördern.

N. Seifter (Leoben)

Geometrie, Topologie — Geometry, Topology — Géométrie, Topologie

F. J. Almgren, Jr: Plateau's Problem. An Invitation to Varifold Geometry. Revised Edition. With new illustrations by K. J. Brakke and J. M. Sullivan. (Student Mathematical Library, Vol. 13.) American Mathematical Society, Providence, Rhode Island, 2001, XVI+78 S. ISBN 0-8218-2747-2 P/b $ 19,00.

Die Neuauflage dieses Standardwerkes aus dem Jahr 1966 für jenen Teil der Differentialgeometrie, der sich um die nach Plateau benannte Fragestellung rankt und auf die Geometrie der Variationsrechnung stützt, gewinnt vor allem durch die mit einer geeigneten Grafiksoftware angefertigten Visualisierungen von Minimalflächen zu gegebenen Randkurven. Der entscheidende mathematische Lösungsansatz des Autors verwendet die Begriffsbildung *varifold*, allerdings in einer anderen Bedeutung als in der aktuellen Literatur. Diese Neuauflage stellt einen wirklichen Gewinn für Spezialisten der geometrischen Sicht der Differentialformen, Grassmannmannigfaltigkeiten, der Variationsrechnung auf Mannigfaltigkeiten und, nicht zuletzt, des Plateauschen Problems dar.

P. Paukowitsch (Wien)

J. N. Cederberg: A Course in Modern Geometries. Second Edition. With 151 Illustrations. (Undergraduate Texts in Mathematics.) Springer, New York u.a. 2001, XIX+442 S. ISBN 0-387-98972-2 H/b DM 138,99.

This is the second edition of a textbook which originally appeared in 1989. In the light of changing demands and new tasks of undergraduate education in Mathematics this book has undergone a revision. Some new parts have been added. Chapter 1 starts with 'Axiomatic Systems and Finite Geometries'. This is the equipment preparing the reader for the second part named 'Noneuclidean Geometry'. The next topic is 'Geometric Transformations in the Euclidean Plane' . In chapter 4 'Projective Geometry' is on the agenda, whilst an 'Introduction to Fractal Geometry' is the content of chapter 5.

Six appendices containing some standard axiomatic systems (Euclid, Hilbert, Birkhoff,...) are at the reader's disposal. Each of the chapters sets off with an introductory section called 'Gaining perspectives'. It delivers some information about the historical background and the scientific environment, where the particular topic is being positioned. There are also some clues to additional software (Cabri Geometry II) and links to helpful support via the World Wide Web.

The layout of the book is handsome in its partition into theorems, proofs, definitions, corollaries and some joining text. The figures are right to the point. The understanding of Euclidean geometry might be fostered though — or dare I say because — the reader comes to it the other way round: Walking through Non-Euclidean fields opens the eye for geometric structures. The ravishing beauty of projective geometry evolving from seemingly minuscule objects like perspectivities comes to the fore as well as the beauty of fractals (which strikes quite a different chord).

The axiomatic approach to undergraduate mathematics is carried out in a pretty self-assured way. This book somehow narrows the gap between sober axiomatic theory and the engineer's approach. At least it successfully works out that the theoretical point of view has its own merits and can reveal things which otherwise most likely would not be recognized.

This book is capable of widening the view of many of its readers and boosting their interest in geometry. I can recommend it to students in mathematics as well as to mathematicians of any kind.

J. Lang (Graz)

L. Conlon: Differentiable Manifolds. (Birkhäuser Advanced Texts, Basler Lehrbücher.) Birkhäuser, Boston, Basel, Berlin, 2001, XIII+418 S. ISBN 0-8176-4134-3, 3-7643-4134-3 H/b $ 59,95.

Gegenüber der ersten Auflage aus 1993 ist eine präzise Teilung des Bandes in einen *Grundkurs* und eine *fortsetzende umfassende Darstellung* der Theorie differenzierbarer Mannigfaltigkeiten erkennbar. Vom Leser wird insgesamt natürlich

eine solide Kenntnis der Analysis zur Linearisierung nichtlinearer Probleme, der Linearen Algebra zur Lösung dieser Linearisierungen und schließlich der Theorie der Differentialgleichungen zur Rückübersetzung dieser Lösungen auf die Ebene der ursprüngliche Fragestellung verlangt (Zitat). Sachgemäß und problemabhängig wird zwischen dem globalen — koordinatenfreien — und dem lokalen — Koordinatenumgebungen verwendenden — Standpunkt gewechselt. Dafür ist ein sehr gutes Vertrautsein mit Inhalten und Methoden der Topologie und der algebraischen Topologie erforderlich.

Eine zentrale Rolle in der globalen Theorie diffenzierbarer Mannigfaltigkeiten spielt das Konzept der differenzierbaren Vektor- und Tensorbündel. Ohne wirklich wesentliche Einschränkung wird stets beliebig oftmalige Differenzierbarkeit vorausgesetzt, die Anpassung an endliche Differentiationsklassen bzw. an die reelle Analytizität ist bekanntlich manchmal recht mühsam. Der sogenannte *Grundkurs* umfaßt das gesamte einschlägige Gebiet der differenzierbaren Mannigfaltigkeiten. Bemerkenswert ist die Darstellung einiger Themen, die sonst zumeist nur als Abrundung der Theorie oder als Ausblick behandelt werden. So findet sich eine umfassende Einführung in die Morsetheorie samt Anwendungen, der Einbettungssatz von Whitney, im Zusammenhang mit Liegruppen die Behandlung abgeschlossener Untergruppen von Liegruppen sowie homogene Räume, die de Rhamsche Theorie und die Poincarésche Dualität und schließlich ein umfassender Exkurs über homogene und symmetrische Riemannsche Räume.

In vier Anhängen werden die für eine sachgemäße Behandlung der Theorie differenzierbarer Mannigfaltigkeiten erforderlichen Aussagen, Beweise und Methoden zur Konstruktion universeller Überlagerungen, inverser Funktionen, Differentialgleichungen sowie der Kohomologiesatz von de Rham behandelt.

Ein sehr empfehlenswertes Lehrbuch, sicherlich an der Spitze der aktuellen Forschung!

P. Paukowitsch (Wien)

A. Juhl: Cohomological Theory of Dynamical Zeta Functions. (Progress in Mathematics, Vol. 194.) Birkhäuser, Basel, Boston, Berlin, 2001, X+709 S. ISBN 3-7643-6405-X H/b sfr 198,–.

Dieses Buch gibt den derzeitigen Stand der Forschung bei der Untersuchung der Eigenschaften dynamischer Zetafunktionen wieder. Die periodischen Orbits des geodätischen Flusses auf einer kompakten lokal symmetrischen Mannigfaltigkeit konstanter negativer Gaußscher Krümmung werden zur Definition einer Zetafunktion verwendet, die eine meromorphe Fortsetzung in die ganze komplexe Ebene besitzt. In dieses allgemeine Konzept fallen die (verallgemeinerte) Selbergsche und die Ruellesche Zetafunktion. Ein wesentlicher Aspekt des in der Einleitung des Buches formulierten Programms ist die Erklärung der Nullstellen und Pole dieser Funktionen durch kohomologische Daten der Mannigfaltigkeit. Darüber

hinaus führt diese Betrachtungsweise zu einer neuen Interpretation der Funktionalgleichung. Ein wichtiges Hilfsmittel dabei ist eine Verallgemeinerung der Fixpunktformel von Lefschetz für den hier betrachteten kontinuierlichen Fall.

P. Grabner (Graz)

J. M. Lee: Introduction to Topological Manifolds. With 138 Illustrations. (Graduate Texts in Mathematics 202.) Springer, New York u.a. 2000, XVII+385 S. ISBN 0-387-98759-2 H/b, ISBN 0-387-95026-5 P/b DM 69,–.

The title of this book may be a bit misleading, since it is not specialized to topological manifolds as opposed to smooth or PL manifolds. Rather than that, it offers a detailed and gentle introduction to several aspects of general and algebraic topology that are needed in the study of manifolds in analysis or differential geometry. Starting from the introductory chapter 1, which is devoted to the questions "What is a manifold?" and "Why study manifolds?", a lot of motivation and many examples are presented. The book is written in a very user friendly way, and a number of exercises and (slightly more difficult) problems help the reader to see whether he or she has digested the material.

The contents roughly split into five parts. The first part (three chapters) studies aspects of general topology. Starting from generalities on topological spaces, the author discusses subspaces, products, and quotient topologies, including for example a discussion of group actions. Next, basic facts on compactness and connectedness are proved, including a discussion of locally compact spaces and the Baire category theorem. The second part (two chapters) is devoted to simplicial complexes and manifolds of dimension one and two, including a discussion of polygonal presentation of surfaces and their classification, as well as triangulability theorems in dimensions one and two. The third part (three chapters) is devoted to the fundamental group and the Seifert-van Kampen theorem. The next two chapters discuss coverings and their relations to the fundamental group, and in a final chapter the basics of singular and simplicial homology theory as well as a bit of cohomology theory are discussed.

The prerequisites are kept rather low, rigorous introductory courses in analysis and linear algebra should be sufficient to follow the presentation. Moreover, some of the background material on set theory, metric spaces, and group theory is reviewed in an appendix. While all the material presented in the book is of course standard, one would certainly have to consult several sources for the different subjects covered. In view of the nice and concise presentation and the unusual collection of material, the book is certainly a valuable addition to the introductory literature available in the field.

A. Cap (Wien)

A. M. Mathai: An Introduction to Geometrical Probability. Distributional Aspects with Applications. (Statistical Distributions and Models with Applications, Vol. 1.) Gordon and Breach Science Publishers, Australia u.a. 1999, XXII+554 S. ISBN 90-5699-681-9 H/b $ 120,–.

Dieses umfangreiche Buch vermittelt eine ausführliche und systematische Einführung in das Gebiet der geometrischen Wahrscheinlichkeit. Während es vom Leser eine gründliche Vertrautheit mit der höherdimensionalen Analysis (insbesondere alternierenden Differentialformen) voraussetzt, sind die erforderlichen Kenntnisse aus der Geometrie und mehr noch der Wahrscheinlichkeitstheorie als eher bescheiden anzusehen. Diese Voraussetzungen, insbesondere der Verzicht auf eine maßtheoretische Grundlegung, bringen es mit sich, daß oft heuristische, nicht immer ganz einfache Argumente herangezogen werden, sodaß in solchen Fällen eine in jeder Hinsicht strenge Ableitung unterbleiben muß (der Verfasser selbst spricht von ‘semi-rigorous level’). Diese Vorgangsweise erspart freilich die Entwicklung eines umfangreichen technischen Apparats, und der Verfasser gelangt von Anfang an zum eigentlichen Gegenstand.

Das Werk gliedert sich in 4 Kapitel: Kap. 1 behandelt Grundlagen, wie das Buffonsche Nadelproblem mit Variationen, geometrische Objekte wie Polyeder, die Theorie der Zufallsauswahl von Punkten, Geraden und Ebenen im Sinne der Konstruktion bewegungsinvarianter Maße auf Mengen solcher Gebilde, Croftonsche Sätze über konvexe Figuren der Ebene u. dgl. Kap. 2 widmet sich zufälligen Punkten und Abständen, wobei die Punkte aus Gleichverteilungen oder aus Poisson-Prozessen stammen. Mit den hier entwickelten Methoden lassen sich nicht nur bekannte Paradoxien, wie die Bertrandsche, oder rein geometrische Fragestellungen behandeln, sondern auch interessante naturwissenschaftlich-technische Probleme, u.a. Stereologie. Kap. 3 und 4 behandeln Flächen und Volumina zufälliger, auch höherdimensionaler Mengen, wie konvexe Hüllen zufälliger Punkte oder zufällige Simplices, wobei das letze Kapitel vornehmlich Fragen der Verteilung solcher Größen (Dichte, Momente) gewidmet ist. Dabei kommen übrigens auch Ergebnisse der Wiener Schule zur Sprache.

Das Buch beeindruckt durch viele Vorzüge: die systematische, übersichtliche Darstellung, die zahlreichen konkreten Falluntersuchungen, überaus umfangreiche Literaturangaben und zahlreiche Übungsaufgaben. Mancherlei Druckfehler, bisweilen etwas umständliche oder unklare Argumente und unschöne Bezeichnungen sowie mäßig gelungene Abbildungen (z.B. zeigt Fig. 1.1.6 anstatt einer Sinuskurve einen Halbkreis) kommen vor; bisweilen könnte auch der Wechsel zwischen ausführlichen Erklärungen einfacher, elementarer Dinge und schwierigen analytischen Argumenten überraschen. Dies vermag jedoch nicht den ausgezeichneten Eindruck dieses Werkes zu trüben, das als gründliche Einführung bestens empfohlen werden kann. Es läßt sich aber auch als Fundgrube für eine Fülle von interessanten Detailfragen und Literaturhinweisen verwenden.

W. Wertz (Wien)

M. M. Postnikov: Geometry VI. Riemannian Geometry. (Encyclopaedia of Mathematical Sciences, Vol. 91.) Springer, Berlin u.a. 2001, XVIII+503 S. ISBN 3-540-41108-9 H/b DM 199,-.

Gegenüber der russischen Originalausgabe aus dem Jahr 1998 ist als wesentliche Änderung zur inhaltlichen Abrundung dieses umfassenden Lehrbuchs der Riemannschen Geometrie die Ergänzung der notwendigen Grundlagen zur Theorie differenzierbarer Mannigfaltigkeiten erfolgt: Auf etwa einem Viertel des Umfanges dieser Monographie werden die differenzierbare Struktur von Mannigfaltigkeiten, Vektor- und Tensorfelder, Differentialformen, Zusammenhänge auf Vektorbündeln und die mit der Parallelverschiebung verknüpften Inhalte vorgestellt, und zwar wegen der erforderlichen Kürze jeweils ohne Beweis (Kapitel 30 bis 36).

Der gesamte Band ist sehr stark in Kapitel und Unterabschnitte gegliedert. Diese Struktur ist aus der Absicht des Autors entstanden, eine Vorlage für Lehrveranstaltungen zu gestalten. Kapitel 1 bringt eine Einführung in Affinzusammenhänge und Geodätische, Kapitel 2 ist der kovarianten Differentiation, dem Torsions- und dem Krümmungstensor gewidmet. Im 3. Kapitel wird die Geometrie von Teilmannigfaltigkeiten eines Raumes mit Affinzusammenhang vorgestellt. Kapitel 4 beschreibt die Cartanschen Strukturgleichungen unter Verwendung von Polarkoordinaten. Symmetrische affinzusammenhängende Räume werden durch lokale Eigenschaften vorbereitet, die globale Struktur kommt in Kapitel 6. Die Kopplung zwischen Liegruppen und Liealgebren wird in Kapitel 7 behandelt. Die Kapitel 8 und 9 bereiten diese Inhalte auf symmetrische Räume auf, im Kapitel 10 werden endlichdimensionale Liealgebren auf Vektorfeldern betrachtet.

Die Kapitel 11 und 12 führen zu Riemannschen Zusammenhängen, Geodätischen und ihren Extremaleigenschaften; Riemannnsche Koordinaten, das Lemma von Gauss, die innere Metrik und der Satz von Hopf-Rinow finden sich hier ebenfalls. Auch sehr nahe zur klassischen Differentialgeometrie zweidimensionaler Flächen sind die Kapitel 13 bis 16 angelegt: Minimalflächen, Krümmungstensor, Satz von Gauss-Bonnet. Kapitel 17 bespricht dimensionsmäßige Verallgemeinerungen, den Riccitensor und Einsteinräume. Die konforme Struktur von Räumen, insbesondere die konforme Transformation von Metriken, wird im Kapitel 18 diskutiert. Die Kapitel 19 und 20 enthalten einen weiteren Überbau zur klassischen Differentialgeometrie: Abbildungen Riemannscher Räume, Isometriegruppe, Riemannsche Zusammenhänge auf Teilmannigfaltigkeiten, Formeln von Gauss, Weingarten und Codazzi.

Das Kapitel 20 ist lokal symmetrischen bzw. kompakten Teilmannigfaltigkeiten, nur aus Nabelpunkten bestehenden Hyperflächen sowie der Starrheit von Sphären gewidmet. Hyperflächen zu gegebener erster und zweiter Fundamentalform werden im Kapitel 21 behandelt. In den Kapiteln 22 und 23 werden Räume konstanter Krümmung besprochen, im Kapitel 24 insbesondere 4-dimensionale Mannigfal-

tigkeiten. Invariante Metriken auf einer Liegruppe werden in den Kapiteln 25 und 26 diskutiert. Jacobifelder, konjugierte Punkte, zweite Variation und das 'Jacobi theorem' werden in Kapitel 27 vorgestellt. In den folgenden Kapiteln 28 und 29 — den letzten der russischen Erstauflage — werden diese Ergebnisse angewendet: Schnittpunktort, Räume streng positiver Ricci- oder Schnittkrümmung, Räume nichtpositiver Schnittkrümmung, Sätze von Cartan-Hadamard und von Cartan-Killing, 'Bochner theorem', Isometriegruppe kompakter Räume.

Die anschließenden sieben Kapitel stellen, wie bereits erwähnt, eine vom bisherigen Hauptteil unabhängige, sehr kompakte und für sich sehr brauchbare Einführung in die Theorie differenzierbarer Mannigfaltigkeiten dar. Insgesamt liegt ein sehr empfehlenswertes Lehrbuch einerseits zur Riemannschen Geometrie und andererseits zur Theorie differenzierbarer Mannigfaltigkeiten vor, wegen der strukturierten Breite der Darstellung sehr gut geeignet sowohl zum Selbststudium für Studierende mathematischer Disziplinen als auch für Dozenten als Grundlage einschlägiger Lehrveranstaltungen.

P. Paukowitsch (Wien)

H. Pottmann, J. Wallner: Computational Line Geometry. With 264 Figures, 17 in Color. (Mathematics + Visualization). Springer, Berlin u.a. 2001, IX+563 S. ISBN 3-540-42058-4 EUR 74,95.

This textbook treats the field of line geometry from various points of view. It starts with some prerequisites on projective geometry, projective differential geometry, algebraic geometry and the geometric design of curves and surfaces. In the second chapter it presents models of line space. This vantage point puts the reader in the position to follow the subsequent chapter on linear complexes. The link to null polarities and the helical motions of the Euclidean space is described as well as some emerging applications in kinematics and statics. Approximation in line space is the topic of chapter 4. Of course, an elaborate chapter on ruled surfaces — viewed from the projective, algebraic, Euclidean and numerical points of view — is also part of the book. The last three chapters are dedicated to developable surfaces, line congruences and complexes in general and to linear and kinematic mappings. There are 247 neat figures and 17 colour plates which are a sight for sore eyes.

The depth of the presentation is one of the striking things about this work. It does not only scratch the surface of the numerous fields but delves into the matter meticulously. But all the same there is enough room left for applications which keep the book exciting, not only for students and mathematicians but also for ambitious engineers. Some of them might ask themselves beforehand: *'How on earth can anybody write so much about mere straight lines?'* Maybe after reading it they will have changed their mind completely and ask: *'How come I haven't stumbled across this interesting field until now?'*

I can well imagine that this book will render a tremendous service to many of its readers. I wholeheartedly recommend this outstanding monograph.

J. Lang (Graz)

Analysis — Analysis — Analyse

H. Amann, J. Escher: Analysis III. (Grundstudium Mathematik.) Birkhäuser Verlag, Basel, Boston, Berlin, 2001, XII+480 S. ISBN 3-7643-6614-1 H/b, ISBN 3-7643-6613-3 P/b sFr 42,00.

Wie in der Besprechung der Analysis II (IMN 185, 2000, p. 32) angemerkt, handelt es sich nicht um eine Einführung in die Analysis, sondern vielmehr um einen umfassenden „Cours d'analyse". Die vorliegende Analysis III behandelt auf 240 Seiten die Lebesguesche Maß- und Integrationstheorie (für Funktionen mit Werten in Banachräumen), sowie auf weiteren 150 Seiten Mannigfaltigkeiten und Differentialformen. Im Kapitel XII kulminiert die Darstellung mit der „Integration auf Mannigfaltigkeiten", wobei der „Stokessche Satz für Singularitäten" bewiesen wird. Ebenso wie im Band II ist die Darstellung elegant und präzise. Daher ist dem Klappentext vollinhaltlich zuzustimmen: „. . . machen dieses Lehrbuch zu einem verläßlichen Begleiter durch das gesamte Studium."

N. Ortner (Innsbruck)

V. V. Beletsky: Essays on the Motion of Celestial Bodies. Translated from the Russian by A. Iacob. Birkhäuser Verlag, Basel, Boston, Berlin, 2001, XVIII+ 372 S. ISBN 3-7643-5866-1 H/b sFr 228,–.

Die Himmelsmechanik, wohl eine der ersten und ältesten exakten Wissenschaften, zu der viele bedeutende Mathematiker, wie Lagrange, Laplace, Gauß, Hamilton, Jacobi oder Lyapunov beigetragen haben, hat immer wieder zu wichtigen mathematischen Entwicklungen Anstoß gegeben. Als Beispiel sei nur die 1889 vom schwedischen und norwegischen König Oskar II. gestellte Preisfrage nach der Stabilität des Sonnensystems erwähnt, die vom Preisträger Poincaré nur unvollständig beantwortet wurde, aber den Anstoß zur KAM-Theorie gab, die weit über die ursprüngliche Fragestellung hinausgeht.

Eine starke Wiederbelebung des Interesses an der Himmelsmechanik ergab sich in der zweiten Hälfte des 20. Jahrhunderts durch neue Probleme und Fragestellungen aus der Raumfahrt. Während sich die Fragestellungen der klassischen Himmelsmechanik durch einfache Modelle, die jedoch, wie das Beispiel des Dreikörperproblems zeigt, dennoch eine sehr komplexe Dynamik besitzen können, charakterisieren ließen, erforderte die praktisch relevante Behandlung der Bewegung

künstlicher Satelliten kompliziertere Modelle und genauere Untersuchungsmethoden. Dies hatte natürlich die Konsequenz, dass dadurch manchmal die Eleganz der klasssischen Theorie verloren geht, aber andererseits neue Gesichtspunkte, Theorien und Ansätze eingebracht werden. Diese neue und moderne Entwicklung aufzuzeigen ist gerade das Anliegen des Autors, der selbst maßgebend in der zweiten Hälfte des vorigen Jahrhunderts an Bahnberechnungen sowjetischer künstlicher Himmelskörper mitgewirkt hat.

Das Wort Essay im Titel des Buches deutet darauf hin, dass es sich nicht um ein Lehrbuch handelt, sondern der Autor eine Reihe ihm wichtig erscheinender Probleme herausgegriffen hat, die, wie er im Vorwort andeutet, zwar von unterschiedlicher praktischer Bedeutung sind, aber alle ein sehr interessantes Phänomen behandeln. Beispiele sind das schon erwähnte Stabilitätsproblem des Sonnensystems, die Frage optimaler interplanetarer Trajektorien oder das komplexe Phänomen von Ebbe und Flut.

Besonders atraktiv an dem Buch ist sein Stil, denn jedes behandelte Problem wird detailiert analysiert und dem Leser werden einige wichtige mathematische Methoden vorgestellt.

Die russische Ausgabe hat einen Preis der Russischen Akademie der Wissenschaften erhalten. Dies zeigt, dass der hervorragende Eindruck von Inhalt und Stil des Buches, den auch der Referent gewonnen hat, keine einzelne Meinung darstellt. Für jeden akademischen Lehrer, der zu einer Vorlesung über gewöhnliche Differentialgleichungen eine Reihe interessanter, physikalisch motivierter Anwendungsbeispiele sucht, ist das vorliegende Buch eine ideale Quelle.

H. Troger (Wien)

J. B. Conway: A Course in Operator Theory. (Graduate Studies in Mathematics, Vol. 21.) American Mathematical Society, Providence, Rhode Island, 2000, XV+372 S. ISBN 0-8218-2065-6 H/b $ 49,–.

Das Buch entstand aus einer mehrjährigen Vorlesung des Autors. Vorausgesetzt werden grundlegende Kenntnisse der Funktionalanalysis, wie sie zum Beispiel im Buch desselben Autors *A Course in Functional Analysis*, Springer Verlag, New York 1990, dargelegt sind, das auch als Referenzgrundlage dient.

Operatorentheorie ist hier im engeren Sinne zu sehen als Theorie der Operatoren auf dem Hilbertraum. Letztere ist nicht von der Theorie der C^*- und von Neumann-Algebren zu trennen, worauf in diesem Text besonders Wert gelegt wird. So startet dieses Buch mit einführenden Kapitel über C^*-Algebren, beginnend mit den abstrakten C^*-Axiomen und endend mit der GNS-Konstruktion, womit die Brücke zur konkreten Operatortheorie geschlossen wird.

Dieses Kapitel zusammen mit dem zweiten, das die Spektraltheorie von normalen Operatoren, Funktionenkalkül auf der Grundlage der kommutativen C^*-Algebren

behandelt, bietet einen guten Ansatz- und Überschneidungspunkt mit den allgemeineren einführenden Funktionalanalysislehrbüchern.

In den folgenden Kapiteln werden dann die zentralen Themen der gegenwärtigen Operatorentheorie eingeführt. Dabei wird auf Gründlichkeit Wert gelegt und eine repräsentative Auswahl gegeben. Im Hinblick auf den Zweck des Buches als Lehrbuch wird zugunsten der Einfachheit manchmal auf die größte Allgemeinheit der Resultate verzichtet.

Im dritten Kapitel geht es um kompakte Operatoren, zunächst vom C^*-algebraischen Standpunkt gesehen bis hin zu Hilbert-Schmidt- und Spurklassenoperatoren und Dualitätsaussagen für diese Operatorenräume.

Das vierte Kapitel ist einigen Klassen und konkreten Beispielen von nichtnormalen Operatoren gewidmet, von Isometrien, Shift bis hin zu essentiell normalen Operatoren.

In Kapitel 5 wird die weitergehende Theorie der C^*-Algebren behandelt, insbesondere vollständig positive Operatoren, und als Anwendung wird der Dilationssatz von Sz.-Nagy bewiesen.

Kapitel 6 ist kompakten Perturbationen gewidmet; die grundlegenden Sätze von Weyl und von Neumann bzw. Voiculescu werden bewiesen.

Das Buch schließt ab mit einem einführenden Kapitel über von Neumann-Algebren und einem Kapitel über Reflexivität (im Sinne von Unterraumverbänden).

Der Autor präsentiert unter Voraussetzung minimaler Vorkenntnisse ein breites Spektrum von aktuellen und klassischen Themen. Das Buch kann als Einführung ins Fach wärmstens empfohlen werden.

F. Lehner (Graz)

R. Estrada, R. P. Kanwal: Singular Integral Equations. Birkhäuser Verlag, Boston, Basel, Berlin, 2000, XII+427 S. ISBN 0-8176-4085-1, 3-7643-4085-1 H/b öS 1008,–.

Rechnerisch-formal werden in den Kapiteln 2, 3, 4 (ca. 1/3 des Buchumfangs) Abelsche, Cauchysche und Carlemanintegralgleichungen behandelt — mit Mitteln der Differential- und Integralrechnung in einer Dimension sowie der Funktionentheorie. Daher ist dieser Teil als Übungsbuch für Studierende ab dem 4. Semester gut geeignet — zur Vertiefung der klassischen Analysis in einer Dimension.

Mit Mitteln der Distributionentheorie in einer Variablen werden dann "Distributional Solutions" dieser Integralgleichungen untersucht.

Das Buch enthält eine Vielzahl von Übungsaufgaben und eine Menge Details. Als störend empfinde ich ein gewisses Fehlen mathematischer Strenge. Um ein Beispiel zu geben: Auf Seite 183 wird gesagt, die für $\alpha, \beta > -1$ gültige Faltungsrelation $x_+^\alpha * x_+^\beta = c x_+^{\alpha+\beta+1}$ bleibe mit analytischer Fortsetzung für alle kom-

plexen α, β gültig, solange sie nicht negativ ganz sind. Was fehlt, ist ein Satz über die Holomorphie der Faltung — oder zumindest ein Zitat. Die Definition der distributionellen Hilberttransformation erfolgt mittels einer von den Autoren 1985 eingeführten Dualitätsmethode — auf die schon 1956 von L. Schwartz-Lévy (Théorie quantique des champs) gegebene Definition wird nicht eingegangen, auch nicht auf die allgemeine Faltungsdefinition für Distributionen, die — bei Schwartz — die spezielle für die Hilberttransformation verallgemeinert. Das ist wohl auch der Grund, warum die Arbeiten zur distributionellen Hilberttransformation von C. Carton-Lebrun nicht erwähnt werden.

Das Werk endet mit Abschnitten über Wiener-Hopf-Integralgleichungen (vgl. das Buch von Noble, 1958) und dualen sowie Tripelintegralgleichungen (vgl. das Buch von Sneddon, 1966), die zur Lösung von gemischten Randwertproblemen der mathematischen Physik benötigt werden.

N. Ortner (Innsbruck)

K. Königsberger: Analysis 1. Fünfte, neu bearbeitete Auflage. Mit 161 Abbildungen und 250 Aufgaben samt ausgearbeiteten Lösungen. (Springer-Lehrbuch.) Springer, Berlin u.a. 2001, XIII+412 S. ISBN 3-540-41282-4 P/b DM 39,90.

Den anerkennenden und begeisterten Besprechungen der 1. und 3. Auflage (IMN 162, 1993, p. 56; 173, 1996, p. 29) bzw. der 4. (IMN 185, 2000, p. 55) braucht nichts hinzugefügt zu werden. Inhaltlich wurde die Darstellung der harmonischen Analysis ergänzt durch Herleitung der Poissonschen Summationsformel für stetige Funktionen, die ebenso wie ihre Fouriertransformierte $O(|x|^{-1-\varepsilon})$, $\varepsilon > 0$, im Unendlichen sind (vgl. E. Stein, G. Weiß: Fourier Analysis on Euclidean Spaces, Princeton, N.J., 1971, p. 252, Cor. 2.6.).

N. Ortner (Innsbruck)

R. B. Paris, D. Kaminski: Asymptotics and Mellin-Barnes Integrals. (Encyclopedia of Mathematics and Its Applications 85.) Cambridge University Press, 2001, XVI+422 S. ISBN 0-521-79001-8 H/b £ 65,00.

Das vorliegende Buch gibt einen umfangreichen Einblick in die Theorie und Anwendung der Mellin-Transformation und der Mellin-Barnes-Integrale. Ausgehend von fundamentalen Eigenschaften der Γ-Funktion werden zunächst einige wichtige Konvergenzaussagen für Mellin-Barnes-Integrale hergeleitet. Die nächsten Kapitel beschäftigen sich detailliert mit Eigenschaften und Anwendungen der Mellin-Transformation, wobei Beispiele aus der Zahlentheorie, der Lösung von Differentialgleichungen, Integralgleichungen und Differenzengleichungen vorgestellt werden. Ein eigenes Kapitel behandelt asymptotische Entwicklungen. Es folgen Abschnitte über das Stokes-Phänomen und über die asymptotische Auswertung von Mehrfachintegralen sowie ein abschließendes Kapitel über Anwendungen auf das Studium einiger Klassen spezieller Funktionen. Mellin-Integrale

besitzen ein weites Anwendungsfeld von Analysis über (analytische) Zahlentheorie bis zur Analyse von Algorithmen — das Buch liefert eine vorzügliche Darstellung der entsprechenden Techniken und kann allen in diesen Gebieten Tätigen uneingeschränkt empfohlen werden.

P. Kirschenhofer (Leoben)

V. P. Pikulin, St. I. Pohozaev: Equations in Mathematical Physics. A practical course. Translated from the Russian by A. Iacob. Birkhäuser Verlag, Basel, Boston, Berlin, 2001, VIII+207 S. ISBN 3-7643-6501-3 H/b sFr 148,00.

Dieses Buch behandelt exakte Lösungen elliptischer, hyperbolischer und parabolischer Gleichungen. Demgemäß sind die Bereiche dieser Randwertprobleme einfach: Scheiben, Ringe, Rechtecke, Zylinder oder Kugeln. Die wichtigste der hier verwendeten Methoden ist die Überlagerungsmethode, die ein Analogon zur Methode partikulärer Lösungen bei gewöhnlichen Differentialgleichungen darstellt. Im Gegensatz zu letzterer ist aber bei linearen partiellen Differentialgleichungen der Satz von „Lösungsatomen“ nicht endlich, sondern unendlich (diskret oder ein Kontinuum bildend). Weiters wird die Methode konformer Abbildungen diskutiert, sowie Integraltransformationsmethoden (Fourier, Laplace und Hankel) für nichtstationäre Probleme, die ebenfalls auf der linearen Überlagerungsmethode beruhen.

J. Hertling (Wien)

H. Sohr: The Navier-Stokes Equations. An Elementary Functional Analytic Approach. (Birkhäuser Advanced Texts, Basler Lehrbücher.) Birkhäuser Verlag, Basel, Boston, Berlin, 2001, X+367 S. ISBN 3-7643-6545-5 H/b sFr 158,00.

Eine elementare und ‘self-contained’ Behandlung der mathematischen Theorie einer viskösen inkompressiblen Flüssigkeit in einem Gebiet des $\mathbb{R}^n$, wie sie durch die Navier-Stokes-Gleichungen beschrieben wird, fehlte bisher in der Literatur. Beiträge dazu sind sehr weit gestreut. In diesem Buch werden sowohl die stationären Navier-Stokes-Gleichungen, die linearisierte nichtstationäre Theorie, wie auch die vollen nichtlinearen Navier-Stokes-Gleichungen behandelt. Die Theorie wird für ganz allgemeine, nicht beschränkte, nicht glatte Gebiete formuliert. Im nichtlinearen Fall muß man sich dabei auf Räume der Dimension zwei und drei beschränken, die ja auch vom physikalischen Gesichtspunkt die wichtigsten sind. Die linearisierte Theorie wird allgemein für Dimensionen $n \geq 2$ entwickelt.

J. Hertling (Wien)

Funktionentheorie — Complex Analysis — Théorie des fonctions des variables complexes

E. Freitag, R. Busam: Funktionentheorie 1. Dritte, neu bearbeitete und erweiterte Auflage. Mit 125 Abbildungen und Lösungshinweisen zu 420 Übungsaufgaben. (Springer Lehrbuch.) Springer, Berlin, Heidelberg, New York, 2000, XX+539 S. ISBN 3-540-67641-4 P/b DM 54,–.

Wir haben es nunmehr mit der dritten Auflage dieses hervorragenden und bewährten Lehrbuches über Funktionentheorie zu tun. Abgesehen von Druckfehlerkorrekturen wurde der Text nur an wenigen Stellen geglättet, es wurden einige Übungsbeispiele ausgetauscht und ein Symbolverzeichnis hinzugefügt.

Kurz zum Inhalt: Dieser zerfällt relativ kanonisch in zwei Teile, wobei in den ersten vier Kapiteln der klassische Aufbau der Funktionentheorie elegant und anschaulich behandelt wird und in den Beweisen des kleinen Riemannschen Abbildungssatzes, des Weierstraßschen Produktsatzes und der Partialbruchzerlegung nach Mittag-Leffler gipfelt. Die Kapitel V–VII verwenden die erarbeiteten Grundlagen, um die Theorie der elliptischen Funktionen und Modulformen aufzubauen und deren Verbindung zur analytischen Zahlentheorie zu beleuchten.

Das Buch eignet sich nicht zuletzt auch durch seine Vielzahl an interessanten Übungsaufgaben (samt Lösungshinweisen) hervorragend zum Selbststudium und zu Lehrzwecken und kann uneingeschränkt empfohlen werden.

M. Lamberger (Graz)

St. G. Krantz: Handbook of Complex Variables. With 102 Figures. Birkhäuser, Boston, Basel, Berlin, 1999 XXIV+290 S. ISBN 0-8176-4011-8, 3-7643-4011-8 H/b sFr 128,–.

Hunderte von Büchern über Funktionentheorie existieren. Wozu ein weiteres, ein Handbuch? Verstehen wir als eine Aufgabe von Wissenschaft auch die Erhaltung des Wissens, so hat dieses Handbuch einen Sinn: Es „erhält Wissen“ — beispielsweise über viele konkrete, konforme Abbildungen und Anwendungen in der mathematischen Physik — klassisch gesammelt und dargestellt in M. R. Spiegel (Complex Variables, Schaum, New York, 1964, 103 Aufgaben) oder N. M. Günter, R. O. Kusmin (Aufgabensammlung zur höheren Mathematik II, Deutscher Verlag der Wissenschaften, Berlin, 1973, 55 Aufgaben). Auch das Standardwissen über die Anwendung des Residuensatzes zur Berechnung bestimmter Integrale wird didaktisch gut dargestellt. Weit darüber hinaus gehen allerdings die Darstellungen von H. G. Garnir, J. Gobert (Fonctions d’une variable complexe, Dunod, Paris, 1965), D. S. Mitrinović, J. D. Kečkić (The Cauchy Method of Residues, D. Reidel, Dordrecht, 1984) oder H. Cartan (Elementare Theorie der analytischen Funktionen einer oder mehrerer komplexen Veränderlichen, BI,

Mannheim, 1966) und M. Ya. Antimirov, A. A. Kolyshkin, R. Vaillancourt (Complex Variables, Academic Press, San Diego, 1998).

Die Kapitel über spezielle Funktionen und Transformationstheorie sind in anderen Lehrbüchern besser dargestellt, z.B. in M. Lavrentiev, B. Chabat (Méthodes de la théorie des fonctions d'une variable complexe, Mir, Moscou, 1967).

Hervorzuheben sind Abschnitte über rationale Approximationstheorie (Runge's theorem und Mergelyan's theorem) sowie über schlichte Funktionen und die Bieberbachsche Vermutung. Beweise der vielen Sätze fehlen — dafür existiert ein ausführliches Glossarium zu Termini aus der Funktionentheorie. Daneben vermitteln auch Tabellen einen handbuchartigen Eindruck.

N. Ortner (Innsbruck)

Angewandte und numerische Mathematik — Applied Mathematics, Numerical Analysis — Mathématiques appliquées, analyse numérique

D. Alpay: The Schur Algorithm, Reproducing Kernel Spaces and System Theory. (SMF/AMS Texts and Monographs, Vol. 5.) American Mathematical Society, Providence, Rhode Island — Société Mathématique de France, 2001, VIII+150 S. ISBN 0-8218-2155-5 P/b $ 49,00.

Das Buch beschäftigt sich in der Art eines Übersichtsartikels mit den Anwendungen der klassischen komplexen Analysis auf die Systemtheorie. Dabei spielen die Selbstabbildungen des Einheitskreises, die Schur-Funktionen, die Hardy-Räume, die Dirichlet-Räume bis hin zu den Pontrjagin-Räumen im Lichte der Operatoren auf Hilberträumen mit reproduzierendem Kern die tragende Rolle für eine adäquate Behandlung vor allem der zeitinvarianten dissipativen linearen Systeme und des inversen Streuungsproblems.

Das Buch ist bemerkenswert und wertvoll in vieler Hinsicht: Es kann dem routinierten Leser als Einführung dienen, es stellt viele Zusammenhänge wesentlich dar. Und es enthält 360 Zitate von den klassischen Werken des ausgehenden 19. Jahrhunderts bis zum Ende des 20. Jahrhunderts, wobei der Autor ausdrücklich keinen Anspruch auf Vollständigkeit erhebt. Stephen S. Wilson besorgte die ausgezeichnete Übersetzung aus dem Französischen. Das Buch bereichert den Leser und macht Freude!

P. Zinterhof (Salzburg)

W. Cheney: Analysis for Applied Mathematics. With 27 Illustrations. (Graduate Texts in Mathematics 208.) Springer, New York u.a. 2001, VIII+444 S. ISBN 0-387-95279-9 H/b DM 117,59.

Das vorliegende Buch ist einer zweisemestrigen Vorlesung nachgestaltet, die jahrelang an der University of Texas at Austin gehalten wurde. Sowohl die Auswahl als auch die Abfolge des dargebotenen Stoffes haben sich also „in der Praxis“ schon bewährt. Folgende Themen werden in 8 Kapiteln behandelt:

Normed Linear Spaces; Hilbert Spaces; Calculus in Banach Spaces; Basic Approximate Methods of Analysis; Distributions; The Fourier Transform; Additional Topics (z.B. Fixed-Point Theorems, Separation Theorems, Fredholm Theory, Topological Spaces); Measure and Integration.

Das Buch ist gut geschrieben! Eine große Anzahl von Beispielen, die sich organisch in den Text einfügen, bringt zusätzliche Einblicke in das gerade behandelte Thema; “Problems” beschließen jeden Abschnitt. Eine ausgedehnte Bibliographie, ein Stichwortverzeichnis und ein Verzeichnis der im Buch verwendeten Notationen finden sich am Ende des Werkes.

Das Buch ist für Studierende in höheren Semestern gedacht. Es soll ihnen — so betont es der Verlag — das analytische Handwerkszeug, aber auch die Konzepte und Sichtweisen der Analysis, die für eine Beschäftigung mit angewandter Mathematik nötig sind, vermitteln. Diese Aufgabe erfüllt das Buch in ausgezeichneter Weise — es sollte in keiner einschlägigen Bibliothek fehlen!

P. Dörfler (Leoben)

D. J. Daley, J. Gani: Epidemic Modelling: An Introduction. (Cambridge Studies in Mathematical Biology 15.) Cambridge University Press, 1999, XII+213 S., ISBN 0-521-64079-2 H/b £ 30,–.

Man kann sich die Frage stellen, weshalb ein zusätzliches Buch über epidemische Modelle gerechtfertigt sein sollte. Findet man nicht schon alles bei Anderson und May (1991)[1] oder sogar schon bei Bailey (1975)[2]? Bei der Lektüre des vorliegenden Buches wird die Antwort aber schnell klar: es ist die Auswahl und die Darstellungsweise, welche diesen Text hervorhebt und lesenswert gestaltet. Es handelt sich um eine didaktisch geschickte Einführung in ein zunehmend wichtiges Gebiet (HIV, Malaria; aber auch Verbreitung von Informationen mit Anwendungen z.B. im Marketing etc.), wobei bewusst Einschränkungen in Kauf genommen werden. Die oben angeführten Bücher sind zwar umfassend, aber eher als Nachschlagewerke geeignet, während der “Daley-Gani” als einführende Darstellung überlegen

[1] Anderson, R.M. and R.M. May (1991), Infectious Diseases of Humans. Dynamics and Control. Oxford University Press, Oxford.

[2] Bailey, N.T.J. (1975), The Mathematical Theory of Infectious Diseases and its Applications. Charles Griffin,London.

scheint. Nach dessen Studium sollte der Leser in der Lage sein, die reichhaltige Literatur im Gebiet epidemischer Modellierung erfolgreich zu bewältigen.

Kap. 1 startet mit historischen Bemerkungen und einer Einführung in grundlegende Begriffe. Kap. 2 bietet eine Einführung in deterministische Modelle, sowohl diskret als auch kontinuierlich in die Zeit. Kap. 3 enthält stochastische Modelle in stetiger Zeit, während in Kap. 4 zeit-diskrete Zufallsmodelle behandelt werden. Kap. 5 analysiert die Verbreitung von Gerüchten. Kap. 6 bringt eine Einführung in die statistische Analyse über Validierung epidemischer Modelle anhand empirischer Daten. Kap. 7 beschäftigt sich mit einigen Methoden zur Kontrolle von Epidemien.

Naturgemäß kann man die Abwesenheit einer ganzen Reihe wichtiger Modellbildungen bedauern, so etwa der McKendrickschen PDE u.a.m. Andererseits ist es bewerkenswert, wie viel wichtiges Material die Autoren — in typisch angelsächsischer Manier der Literatur über stochastische Prozesse — auf knapp 200 Textseiten aufbereiten. Und dies in einem schönen Aufbau und klarer Darstellung. Ein Buch, dessen Lektüre nicht nur den Spezialisten warm empfohlen werden kann!

G. Feichtinger (Wien)

D. Gardy, A. Mokkadem (eds.): Mathematics and Computer Science. Algorithms, Trees, Combinatorics and Probabilities. (Trends in Mathematics.) Birkhäuser, Basel, Boston, Berlin, 2000, XI+341 S. ISBN 3-7643-6430-0 H/b sfr 128,–.

Das vorliegende Buch ist aus den Proceedings einer Konferenz gleichen Titels an der Universität von Versailles St. Quentin entstanden. Die enthaltenen Artikel stammen aus dem reichen Grenzgebiet zwischen Mathematik und Computerwissenschaften und sind thematisch in Kapiteln zusammengefaßt:

I. *Trees and Analysis of Algorithms*: *A. Antos, L. Devroye*: Rawa trees, *P. Chassaing, J. F. Marckert, M. Yor*: The height and width of simple trees, *M. Dekking, S. de Graaf, L. E. Mester*: On the node structure of binary search trees, *M. Drmota*: The saturation level in binary search tree, *J. A. Fill, S. Janson*: Smoothness and decay properties of the limiting quicksort density function, *B. Gittenberger*: The number of descendants in simply generated random trees, *P. Jacquet, W. Szpankowski, I. Apostol*: An universal predictor based on pattern matching, preliminary results.

II. *Combinatorics and Random Generation*: *M. Bousquet, C. Chauve, G. Labelle, P. Leroux*: A bijective proof of the arborescent form of the multivariate Lagrange's inversion formula, *M. Bousquet-Mélou, G. Schaeffer*: Counting paths on the slit plane *A. Denise, O. Rocques, M. Termier*: Random generation of words of context-free languages according to the frequencies of letters, *D. Merlini, R. Sprugnoli, M. C. Verri*: An algebra of generating trees, *E. Pergola, R. Pinzani, S. Rinaldi*: A set of well-defined operations on succession rules.

III. *Algorithms and Optimization*: *J. Bérard, A. Bienvenüe*: Convergence of a genetic algorithm with finite percolation, *M. Dror, D. Fortin, C. Roucairol*: Complexity issues for a redistribution problem, *C. Mazza, D. Piau*: On the rate of escape of a mutation-selection algorithm, *Y. Metivier, N. Saheb, A. Zemmari*: Randomized rendezvous.

IV. *Performance Evaluation*: *M. Ben Mamoun, N. Pekergin*: Computing closed-form stochastic bounds on the stationary distribution of Markov chains, *T. Dayar*: Effects of reordering and lumping in the analysis of discrete-time SANs, *F. Delcoigne, A. De La Fortelle*: Large deviations in polling systems, *G. Fayolle, J. M. Lasgouttes*: A nonlinear integral operator encountered in the bandwidth sharing of a star-shaped network.

V. *Other Topics*: *J. Geiger*: A new proof of Yaglom's exponential limit law, *Q. Liu*: The branching measure, Hausdorff and packing measures on the Galton-Watson tree, *E. Löcherbach*: Likelihood ratio processes and asymptotic statistics for systems of interacting diffusions with branching and immigration, *G. Louchard, O. Rocques*: Probabilistic analysis of a Schröder walk generation algorithm, *V. Malyshev*: Gibbs families, *R. Pemantle*: Generating functions with high-order poles are nearly polynomial, *J. H. Spencer*: Ultrahigh moments for a Brownian excursion, *B. Ycart, M. C. Rousset*: A zero-one law for random sentences in description logic.

P. Grabner (Graz)

V. Y. Pan: Structured Matrices and Polynomials. Unified Superfast Algorithms. Birkhäuser Boston — Springer, New York, 2001, XXV+278 S. ISBN 0-8176-4240-4, 3-7643-4240-4 H/b sFr 108,00.

Matrizen und Polynome haben viel gemeinsam. Dies gilt insbesondere für Matrizen mit gewissen Strukturen, wo etwa die Zeilen durch Verschiebung in der Diagonal- oder Gegendiagonalrichtung entstehen. Dazu gehören etwa Toeplitzmatrizen, Hankelmatrizen, Vandermondematrizen und Cauchymatrizen. Diese Matrizen können durch eine kleine Anzahl von Parametern dargestellt werden und mit Vektoren besonders schnell multipliziert werden. Die enge algorithmische Beziehung zu Polynomen und rationalen Funktionen spiegelt sich in ihrer Multiplikation, Division, Interpolation und Mehrpunktentwicklung wieder. Anwendungen strukturierter Matrizen ergeben sich etwa bei bekannten Problemen der rationalen Interpolation und Approximation. Ebenso kann für strukturierte Matrizen die Anzahl der Operationen, etwa bei der Lösung eines linearen Gleichungssystems durch Gaußelimination, dramatisch gesenkt, und es können „superschnelle" Algorithmen entwickelt werden. Es sollen vielleicht noch einige Schlagworte angeführt werden, die im Rahmen dieses Buches behandelt werden: Nevanlinna-Pick-Interpolationsprobleme, das Matrix-Nehari-Problem, dünnbesetzte mehrdimensionale Polynominterpolation, diskrete Sinus- und Cosinustransformationen, der "Teile und Herrsche"-Algorithmus sowie Newton-strukturierte numerische

und algebraische Iteration. Wer sich mit der Entwicklung moderner Algorithmen beschäftigt, wird wohl dieses Buch nicht umgehen können.

J. Hertling (Wien)

A. Quarteroni, R. Sacco, F. Saleri: Numerische Mathematik 1. Übersetzt von L. Tobiska. (Springer-Lehrbuch.) Springer, Berlin u.a. 2002, XIV+367 S. ISBN 3-540-67878-6 P/b DM 49,90.

Im ersten Teil werden zunächst Grundlagen der linearen Algebra, wie etwa Rang und Kern einer Matrix, die Singulärwertzerlegung und Matrixnormen behandelt. Weiters werden Fragen der Kondition und Stabilität sowie die Gleitkommaarithmetik betrachtet. Der zweite Teil ist der numerischen linearen Algebra gewidmet. Hier werden zunächst direkte Methoden und verschiedene Faktorisierungen besprochen; es wird auch auf Blocksysteme und schwachbesetzte Systeme eingegangen. Die nächsten Kapitel behandeln iterative Methoden zur Lösung linearer Gleichungssysteme, wobei etwa Methoden behandelt werden, die auf Krylov-Teilraumiterationen basieren, und die Approximation von Eigenwerten und Eigenvektoren mit Formen der QR-Iteration. Der dritte Teil ist nichtlinearen Gleichungen und der Optimierung gewidmet. Bei der Bestimmung der Wurzeln nichtlinearer Gleichungen tauchen Fixpunkt-Verfahren auf, sowie Methoden zur Bestimmung der Nullstellen algebraischer Gleichungen. Das letzte Kapitel über nichtlineare Systeme und numerische Optimierung behandelt zunächst die Lösung nichtlinearer Gleichungssysteme, sodann nichtrestringierte Optimierung und schließlich Optimierung unter Nebenbedingungen.

J. Hertling (Wien)

Optimierung, Kontrolltheorie — Optimization, Optimal Control — Théorie de l'optimisation et du réglage

D. Alevras, M. W. Padberg: Linear Optimization and Extensions. Problems and Solutions. With 67 Figures. (Universitext.) Springer, Berlin u.a. 2001, IX+449 S. ISBN 3-540-41744-3 P/b DM 79,00.

Das Buch ist eine Ergänzung zu Padbergs Lehrbuch 'Linear Optimization and extensions' (Springer 1995, Besprechung IMN Heft 172, 1996).

Die in diesem Werk enthaltenen Übungsaufgaben wurden überarbeitet, ergänzt, und werden im vorliegenden Text samt Lösungen und geraffter Zusammenfassung der notwendigen theoretischen Resultate präsentiert.

Der Schwierigkeitsgrad der Aufgaben ist dabei sehr unterschiedlich, von einfachen Rechenübungen bis zu umfangreicheren kleinen Projektarbeiten. Bemerkenswert ist weiters, daß auch Programmieraufgaben gestellt und gelöst werden.

Dabei wird einerseits kommerzielle Software (*Cplex*) verwendet, andererseits sind auch etliche Algorithmen in *Matlab*-source-codes angegeben. (Ich konnte allerdings keinen Verweis im Buch finden, ob diese source-codes auch über das Internet erhältlich wären.) Schließlich ist zum Inhaltlichen noch anzumerken, daß neben einer ausführlichen Behandlung der Simplexmethode weiters auf Innere-Punkte-Methoden und die Ellipsoidmethode detailliert eingegangen wird.

Insgesamt ist das Buch sowohl als Quelle für Übungsaufgaben zu Vorlesungen über Lineare Optimierung als auch zum Selbststudium sehr gut geeignet.

F. Rendl (Klagenfurt)

A. Locatelli: Optimal Control. An Introduction. Birkhäuser, Basel, Boston, Berlin, 2001, IX+294 S. ISBN 3-7643-6408-4 H/b.

Dieses Lehrbuch verfolgt zwei Ziele: Einmal soll die Bedeutung und Eignung der Theorie optimaler Steuerungen für die Lösung von Aufgaben der Anwendungen gezeigt werden, zum anderen die wesentlichen Grundelemente dieser Theorie mathematisch sauber und — auch für Anwender — gut verständlich dargestellt werden. Beides ist dem Autor in hervorragender Weise gelungen, was nicht zuletzt den zahlreichen gut gewählten Beispielen und bereitgestellten Algorithmen zu verdanken ist. Hervorzuheben ist die Tatsache, daß der Autor stets auch auf die Frage der Modellierung eingeht, d.h. auf die Wahl eines für das konkrete Problem (Beispiel) geeigneten Gütefunktionals. Inhaltlich ist der Band in zwei große Abschnitte und die wichtigsten Grundlagen der Systemtheorie und der linearen Algebra zusammenfassende Anhänge gegliedert. Im ersten Teil werden auf Grundlage der Hamilton-Jacobi-Theorie globale Methoden vorgestellt und bewiesen, wobei insbesondere auf die für die Praxis wichtigen LQ- und LQG-Probleme ausführlich eingegangen wird und die wichtigen Eigenschaften der Riccati-Differentialgleichung sowie der algebraischen Riccati-Gleichung dargestellt werden. Im zweiten Teil werden Variationsmethoden behandelt, d.h. die notwendige und hinreichende Bedingungen des Maximumprinzips für verschiedene Aufgabenarten formuliert, Beweise skizziert, die Aussagen hinsichtlich ihrer Bedeutung für die Anwendung ausführlich diskutiert und durch zahlreiche Beispiele illustriert. Vorausgesetzt werden vom Autor jene mathematischen Kenntnisse der Analysis, die an Universitäten üblicherweise im ersten Studienabschnitt sowohl Mathematikern als auch Physikern und Ingenieuren üblicherweise vermittelt werden. Darüber hinaus sind Grundkenntnisse der Systemtheorie (Begriffe wie ‘steuerbar’, ‘stabiliserbar’ usw. werden benötigt) hilfreich. Insgesamt ein empfehlenswerter Band für Lehrende und Studierende.

I. Troch (Wien)

S. E. Lyshevski: Control Systems Theory with Engineering Applications. With 169 Figures and a CD-ROM. (Control Engineering.) Birkhäuser Verlag, Boston, Basel, Berlin, 2001, XI+416 S. ISBN 0-8176-4203-X, 3-7643-4203-X H/b sFr 148,00.

Das Hauptziel der Autors des vorliegenden Lehrbuches ist es, Studenten höherer Semester an einer Technischen Universität und im Beruf stehenden Ingenieuren eine lesbare, gutverständliche Darstellung anspruchsvoller mathematischer Konzepte der Regelungstechnik zur Verfügung zu stellen. Mehr als die Hälfte des Buches beschäftigt sich mit Analyse, Identifikation und Regelung nichtlinearer dynamischer Systeme. Die vorgestellten Methoden und Konzepte entsprechen dem Standard vergleichbarer Lehrbücher.

Eine wesentliche Neuerung und damit auch ein gegenüber vergleichbaren Büchern sehr interessanter Aspekt des Buches, der es besonders attraktiv erscheinen läßt, liegt darin, dass der Simulation breiter Raum gewidmet wird. Dazu wird die *Matlab*-Umgebung eingeführt, die eine Reihe von Toolboxen wie *Simulink, Real-Time Workshop, Control System, Nonlinear Control Design, Optimization, Signal Processing, System Identification* und noch einige andere zur Verfügung stellt. Die starke Betonung der Simulation wird nicht nur computerbegeisterte Studenten ansprechen, sondern vor allem auch praktisch tätige Ingenieure, für die Simulation bereits zu einem unverzichtbaren Hilfsmittel in der Entwicklung, Analyse und Optimierung geregelter Prozesse geworden ist. Die vielen *Matlab*-Files und *Simulink*-Modelle, die im Buch präsentiert werden, können ohne Schwierigkeiten für Probleme aus der Ingenieurspraxis modifiziert werden.

Das Buch wird einerseits durch seine moderne rechentechnisch orientierte Ausrichtung und andererseits durch seine ausführliche Darstellung, die sehr um Verständlichkeit bemüht ist, bei der interessierten Leserschaft zweifelsohne sehr gut ankommen.

H. Troger (Wien)

Finanzmathematik — Financial Mathematics — Mathématiques financières

N. Bouleau: Glück und Strategie auf Finanzmärkten. Aus dem Französischen von P. Hiltner. Birkhäuser, Basel, Boston, Berlin, 2000, 207 S. ISBN 3-7643-6085-2 H/b sFr 52,–.

Im vorliegenden Buch unternimmt der Autor den prinzipiell sehr lobenswerten Versuch, die Konzepte und Methoden, die faszinierenden Resultate und Konsequenzen der modernen Finanzmathematik einem breiteren Leserkreis nahe zu bringen. Aus meiner Sicht ist dieses Vorhaben dem Autor in diesem Buch nicht

wirklich gelungen: Das Buch ist zwar in einzelnen Passagen durchaus interessant und gut zu lesen (die Übersetzung lässt allerdings sowohl stilistisch als auch fachlich durchwegs sehr zu wünschen übrig), es bildet aber keine durchgehende Einheit und lässt einen stringenten Ablauf vermissen. Für einen Laien auf dem Gebiet der Finanzmathematik fehlt somit eine schlüssige Schritt-für-Schritt-Einführung in dieses Gebiet. Banalitäten werden zuweilen ausführlich dargestellt, während wesentliche oder schwierige Konzepte (z.B. das Itô-Integral) dem Leser ohne viele Bedenken relativ selbstverständlich vorgesetzt werden. Ein Laie wird also keinen wirklichen Nutzen aus diesem Buch ziehen können.

Für den fachlich vorgebildeten Leser sind, wie bereits erwähnt, einzelne Passagen sehr wohl von Interesse, doch werden Ungenauigkeiten in manchen Bereichen durchaus als störend empfunden.

Zusammenfassend ist vielleicht folgendes Resümee zu ziehen: Der Autor wollte mit diesem Buch auf wenigen Seiten zu viel. So hat sich ein nicht ausgegorenes und nicht konsistentes Misch-Masch aus einzelnen, für sich durchaus interessanten Ansätzen ergeben.

G. Larcher (Linz)

M. Kohlmann, Shanjian Tang: Mathematical Finance. Workshop of the Mathematical Finance Research Project, Konstanz, Germany, October 5–7, 2000. (Trends in Mathematics.) Birkhäuser Verlag, Basel, Boston, Berlin, 2001, 374 S. ISBN 3-7643-6553-6 H/b sFr 148,00.

100 Jahre nach der Veröffentlichung von Bacheliers Dissertation “Théorie de la Spéculation” fand in Konstanz vom 5.–7. 10. 2000 der “Workshop of the Mathematical Finance Research Project” statt. Das vorliegende Buch enthält 35 Arbeiten aus verschiedenen Teilgebieten der Finanzmathematik, wie etwa unvollständige Marktmodelle, Portfolio-Selektion, Hedging von Claims, Value-at-Risk oder Interest-Rate-Theorie. Hervorzuheben sind besonders Beiträge, welche die fraktionelle Brownsche Bewegung zur Beschreibung von Markt-Modellen verwenden. Es konnte eine Reihe bekannter Autoren, wie etwa E. Benth, R.J. Elliott, S. Pliska, E. Platen, W. Schachermayer oder R. Wojakowski gewonnen werden. Durch die Vielfalt vermitteln die Artikel in diesem Tagungsband einen sehr guten Eindruck vom aktuellen Stand der Forschung auf dem Gebiet der Finanzmathematik.

M. Predota (Graz)

Wahrscheinlichkeistheorie und Statistik — Probability Theory and Statictics — Théorie des probabilités, statistique

A. B. Cruzeiro, J.-C. Zambrini (eds.): Stochastic Analysis and Mathematical Physics. (Progress in Probability, Vol. 50.) Birkhäuser Verlag, Boston, Basel, Berlin, 2001, 158 S. ISBN 0-8176-4246-3, 3-7643-4246-3 H/b sFr 158,00.

The proceedings under review comprise nine papers which are, according to the preface, related to a meeting organized in Lisbon by the Group of Mathematical Physics. Six of the papers are full-length papers with proofs. Two papers (by Airault and Malliavin, and by Léandre) are devoted to analysis on manifolds. Motivated by potential applications to fractional Brownian motion, Coutin and Decrausefond study a stochastic version of the Volterra equation. Markov and martingale uniqueness of Nelson diffusions on infinite dimensional spaces is studied by Wu, while the paper by Oberguggenberger and Russo deals with stochastic nonlinear wave equations. Üstünel's contribution contains results on measure preserving shifts on the Wiener space. Two papers (by P. Lescot and Léonard) are only short surveys of their authors' recent results which are published in detail elsewhere. Robelledo gives a short introduction to quantum dynamical semigroups and quantum flows.

The papers are of high quality. However, the topics are loosely tied together, which should be taken into consideration before spending more than 100 Euros.

E. Hausenblas (Salzburg)

R. M. Dudley: Uniform Central Limit Theorems. (Cambridge Studies in Advanced Mathematics 63.) Cambridge University Press, Cambridge, 1999, XIV+436 S. ISBN 0-521-46102-2 H/b £ 55,–.

Der klassische n-dimensionale Zentrale Grenzwertsatz (ZGS) gilt bekanntlich gleichmäßig für alle Halbräume; diese Gleichmäßigkeit geht aber verloren, wenn stattdessen „große“ Mengenfamilien, wie z. B. alle Borelmengen, zugrundegelegt werden. Diese Monographie widmet sich der Untersuchung von in diesem Sinne gleichmäßigen ZGSen. Dabei spielen Donsker-Klassen — das sind, sehr vereinfachend gesagt, Klassen (von Funktionen), für die der ZGS gleichmäßig gilt — eine entscheidende Rolle.

Das vorliegende Buch hat seinen Ursprung in Vorlesungen des Verfassers bei der St. Flour-Sommerschule 1982; es ist aber derart erweitert, daß die Entwicklungen der 80er und 90er Jahre voll berücksichtigt sind, sodaß es dem gegenwärtigen Entwicklungsstand der Forschung entspricht. Demzufolge ist technischen Einzelheiten maßtheoretischer, geometrischer (Konvexität!), topologischer und funktionalanalytischer Natur breiter Raum gewidmet; der Leser kann somit viele derartige Techniken finden, die übrigens auch in völlig anderen Gebieten anwendbar

sind. Es erweist sich als notwendig, eine Reihe herkömmlicher Definitionen und Begriffe so zu verallgemeinern, daß sie der gegenständlichen Problemstellung angemessen und hilfreich sind (z. B. Konvergenztheorie für nicht notwendigerweise meßbare Funktionen).

Das Buch stützt sich im wesentlichen auf das Werk "Real Analysis and Probability" des Verfassers. Jedem der 12 Kapitel sind ausführliche Kommentare und Literaturangaben beigefügt. Die Darstellung selbst ist naturgemäß anspruchsvoll, mit vollständigen, klar geführten Beweisen versehen und in sich geschlossen. Das Buch spricht einen Leserkreis an, der sich mit Wahrscheinlichkeitstheorie, deren Anwendungen (auch in der mathematischen Statistik) und auch mit verwandten Gebieten befaßt, und ist als überaus wertvolle Bereicherung des einschlägigen Schrifttums bestens zu empfehlen.

W. Wertz (Wien)

T. Hida, R. L. Karandikar, H. Kunita, B. S. Rajput, S. Watanabe, J. Xong (eds.): Stochastics in Finite and Infinite Dimensions. In Honor of Gopinath Kallianpur. (Trends in Mathematics.) Birkhäuser, Boston, Basel, Berlin, 2001, XXXVI+410 S. ISBN 0-8176-4137-8, 3-7643-4137-8 H/b sfr 198,–.

Es handelt sich um eine Festschrift aus Anlaß des 75. Geburtstages des bedeutenden Stochastikers *Gopinath Kallianpur*, der in Indien und den USA tätig war und ist. Neben einer Beschreibung des Lebens und der Arbeit von G. Kallianpur samt dem beeindruckenden Werkeverzeichnis enthält der Tagungsband die folgenden, auf hohem Niveau verfaßten Forschungsartikel:

– Precise Gaussian lower bounds on heat kernels (*S. Aida*);
– Feynman integrals associated with Albeverio-Høegh-Krohn and Laplace transform potentials (*N. Asai, I. Kubo, H.-H. Kuo*);
– Random iteration of i.i.d. quadratic maps (*K. B. Athreya, R. N. Battacharya*);
– Monte Carlo algorithms and asymptotic problems in nonlinear filtering (*A. Budhiraja, H. J. Kushner*);
– A covariant quantum stochastic dilation theory (*P. S. Chakraborty, D. Goswami, K. B. Sinha*);
– Interacting particle filtering with discrete-time observations: asymptotic behaviour in the Gaussian case (*P. Del Moral, J. Jacod*);
– Hidden Markov chain filtering for generalised Bessel processes (*R. Elliott, E. Platen*);
– On the Zakai equation of filtering with Gaussian noise (*L. Gawarecki, V. Mandrekar*);
– Prediction and translation of fractional Brownian motions (*Y. Hu*);
– Time maps in the study of Feynman's operational calculus via Wiener and Feynman path integrals (*G. W. Johnson, L. Johnson*);

– Two applications of reproducing kernel Hilbert spaces in stochastic analysis (*T. Koski, P. Sundar*);
– Stochastic linear controlled systems with quadratic cost revisited (*N. V. Krylov*);
– Numerical solutions for a class of SPDEs with application to filtering (*T. G. Kurtz, J. Xiong*);
– Nonlinear diffusion approximations of queuing networks (*B. Margolius, W. A. Woyczyński*);
– On equations of stochastic fluid mechanics (*R. Mikulevicius, B. Rozovskii*);
– Infinite level asymptotics of a perturbative Chern-Simons integral (*I. Mitoma*);
– Risk-sensitive dynamic asset management with partial information (*H. Nagai*);
– Existence of a string solution for an integro-differential equation and superposition of diffusion processes (*Y. Ogura, M. Tomisaki, M. Tsuchiya*);
– On the consistency of the maximum likelihood method in testing multiple quantum hypotheses (*K. R. Parthasarathy*);
– Large deviations for double Itô equations (*V. Pérez-Abreu, C. Tudor*);
– The domain of a generator and the intertwining property (*I. Shigekawa*).

W. Woess (Graz)

L. C. G. Rogers, D. Williams: Diffusions, Markov Processes, and Martingales. Volume 1: Foundations. 2nd Edition. (Cambridge Mathematical Library.) Cambridge University Press, 2000, XX+386 S. ISBN 0-521-77594-9 P/b £ 22,95.

L. C. G. Rogers, D. Williams: Diffusions, Markov Processes, and Martingales. Volume 2: Itô Calculus. 2nd Edition. (Cambridge Mathematical Library.) Cambridge University Press, 2000, XIV+480 S. ISBN 0-521-77593-0 P/b £ 24,95.

Die beiden Bände, im Jahre 1979 in der 1. Auflage erschienen, sind bald zu einem Standardwerk über Martingale geworden, sodaß 1994 eine beträchtlich erweiterte und veränderte Neuausgabe erforderlich wurde, deren erster Band jedoch bald vergriffen war. Die vorliegende Neuauflage ist ein broschierter Neudruck der Ausgabe von 1994.

Das Anliegen der beiden Verfasser ist es, eine Einführung in das Gebiet der Martingaltheorie zu geben, die vor allem die heuristisch-begriffliche Seite des Gegenstandes betont. Die Darstellung schließt im wesentlichen an das Buch ‘Probability with Martingales’ von D. Williams an und soll den Leser zu den aktuellen Fragen der Forschung führen und die Brücke zu abstrakten Zugängen errichten. Dementsprechend treten mathematisch-technische Einzelheiten in den Hintergrund, das Werk ist auch nicht streng deduktiv aufgebaut, Beweise sind eher knapp gehalten und betonen die dahinterstehenden Ideen.

Eine Inhaltsübersicht zeigt die breite Anlage der beiden Bände, die aus jeweils 3 Kapiteln bestehen:

Kap. I („Brownsche Bewegung“): grundlegende Eigenschaften der Brownschen Bewegung, Gaußsche und Levysche Prozesse.

Kap. II („Etwas klassische Theorie“) faßt überblicksmäßig den maßtheoretischen Apparat zusammen und entwickelt ihn weiter: Einführung in die Maß- und die Wahrscheinlichkeitstheorie, Martingale mit diskreter Zeit, Supermartingale mit stetigem Zeitparameter, W-Maße auf Lusin-Räumen.

Kap. III („Markow-Prozesse“) ist weitgehend von der 1. Ausgabe übernommen: Übergangsfunktionen, Feller-Dynkin-Prozesse, Ray-Prozesse, Martinscher Rand und Anwendungen.

Kap. IV („Einführung in den Itô-Kalkül“): Vorhersehbare Prozesse, Prozesse mit endlicher und integrierbarer Variation, Lokalisierung, L_2-Theorie stochastischer Integrale, stochastische Integrale bezüglich stetigen Semimartingalen, Itô-Formel und deren Anwendung.

Kap. V („Stochastische Differentialgleichungen [SDglen.] und Diffusionen“): Starke und schwache Lösungen von SDglen., Martingalprobleme, Grundlagen der stochastischen Differentialgeometrie, eindimensionale SDglen., eindimensionale Diffusionen.

Kap. VI („Die allgemeine Theorie“): Filter, vorhersehbare Projektionen, Meyerscher Zerlegungssatz, allgemeine stochastische Integrale, Itôsche Theorie der Abweichungen („excursion theory“).

Das vorliegende Werk stellt zweifelsohne ein unentbehrliches Hilfsmittel für Forscher auf dem behandelten Gebiet dar, aber auch für Anwender dieser Theorie in vielen Bereichen, insbesondere in der Finanzmathematik.

W. Wertz (Wien)

H. Sahai, M. I. Ageel: The Analysis of Variance. Fixed, Random and Mixed Models. Birkhäuser, Boston, Basel, Berlin, 2000, XXXV+742 S. ISBN 0-8176-4012-6, 3-7643-4012-6 H/b sFr 128,–.

Die Autoren setzen sich das Ziel, eine Einführung in die Varianzanalyse zu geben, die im Niveau zwischen mathematisch orientierten Darstellungen und Einführungslehrbüchern in die Statistik liegt. Entsprechend dieser Zielsetzung werden die folgenden Modelle der Varianzanalyse systematisch diskutiert: einfache Varianzanalyse, zwei- und mehrfache Varianzanalyse, hierarchische Modelle. Dabei werden sowohl Modelle mit festen Effekten als auch mit Zufallseffekten behandelt.

Die Darstellung aller dieser Modelle ist sehr ausführlich und auf einem mathematisch elementaren Niveau. Für den an der Theorie interessierten Leser werden primär Literaturhinweise geboten. Die Berechnung in den zahlreichen Beispielen wird sowohl explizit als auch mit statistischen Programmsystemen (SPSS, SAS) durchgeführt. Für die manuelle Berechnung werden zahlreiche eher selten zu findende Tabellen für die Verteilungen von Teststatistiken im Anhang angeführt. Ein

gewisser Mangel ist die Tatsache, dass einige heute in den Anwendungen wichtige Bereiche gar nicht oder nur sehr knapp behandelt werden: Lineare Kontraste und verschiedene Parametrisierungen werden nur kurz erwähnt, grafische Darstellungen der Ergebnisse findet man gar nicht.

Zusammenfassend lässt sich feststellen, dass dieses Werk eine eher traditionell orientierte Darstellung der Varianzanalyse für Anwender ist, in der man zwar eine Reihe von selten in Lehrbüchern enthaltenen Details findet, aber für den an statistischer Theorie und Modellierung Interessierten wenig Einblick in die Theorie gibt.

W. Grossmann (Wien)

Einführungen — Introductory — Ouvrages introductoires

T. Andreescu, Zuming Feng (eds.): Mathematical Olympiads 1998–1999. Problems and Solutions From Around the World. The Mathematical Association of America, 2000, XII+290 S. ISBN 0-88385-803-7 £ 19,95.

Die vorliegende Sammlung stellt eine Fortsetzung des Bandes *Mathematical Contests 1997–1998* der Mathematical Association of America dar. Es finden sich Forschungsaufgaben von 25 nationalen und regionalen Mathematischen Olympiaden zu Themenschwerpunkten aus der Algebra, der Geometrie, der Kombinatorik und der Zahlentheorie samt zum Teil mehreren Lösungen oder Lösungsansätzen. Etwa ein Viertel des Textes ist besonders bemerkenswerten Problemen gewidmet, die bei nationalen und regionalen Mathematischen Olympiaden im Jahr 1999 formuliert wurden; dieser Teil ist allerdings ohne Lösungen publiziert. Wieder liegt eine wahre Fundgrube an interessanten Aufgabenstellungen für interessierte Dozenten und Studenten vor!

P. Paukowitsch (Wien)

R. P. Burn: Numbers and Functions. Steps into Analysis. Second Edition. Cambridge University Press, 2000, XXIII+356 S. ISBN 0-521-78836-6 P/b £ 19,95.

Gegenüber der ersten Auflage (besprochen in IMN Nr. 164, Dez. 1993, Seite 50) wurde in der vorliegenden Neuauflage die Behandlung der Peano-Axiome sowie der algebraischen Charakterisierung der reellen Zahlen reduziert. Weitere Änderungen betreffen die Zusammenfassungen, die nun nicht nur am Kapitelende aufscheinen, sondern immer dann, wenn ein wesentlicher Gedanke zu einem Abschluss gebracht wurde. Außerdem wurden Theoreme mit griffigen Namen versehen, um bei späteren Verweisen inhaltliche Assoziationen zu erleichtern. Schließlich wurden noch einige Diagramme sowie historische Bemerkungen und Verweise ergänzt.

M. Kronfellner (Wien)

I. M. Gelfand, M. Saul: Trigonometry. Birkhäuser Verlag, Boston, Basel, Berlin, 2001, X+229 S. ISBN 0-8176-3914-4, 3-7643-3914-4 P/b sFr 38,00.

Dieses Buch behandelt ebene Trigonometrie. Einige interessante Relationen finden sich im Kapitel 7 über "Trigonometric Identities".

J. Hertling (Wien)

P. Meunier: Cours de mathématiques. Grandes écoles scientifiques. MP-MP*-PSI-PSI*. (Mathématiques.) Presses Universitaires de France, Paris, 1999, 277 S. ISBN 2-13-050436-1 P/b FF 248,–.

P. Meunier: Problèmes de mathématiques spéciales. Agrégation interne. Classes spéciales MP-MP*. Grandes écoles scientifiques. MP-MP*-PSI-PSI*. (Mathématiques.) Presses Universitaires de France, Paris, 1999, 281 S. ISBN 2-13-050435-3 P/b FF 288,–.

Die vorliegenden zwei Bücher behandeln — auf hohem Niveau — den standardisierten Lehrstoff für Prüfungen an den "grandes écoles scientifiques". Nach Kapiteln geordnet: 1. Folgen und Reihen, summierbare Familien (Summierung durch Cesàromittel, Cauchymultiplikation von Reihen als Faltung), 2. Lineare Algebra: Endomorphismenreduktion = Spektraltheorie, 3. Bilineare und hermitesche Algebra, 4. Topologie (im wesentlichen mengentheoretisch für Analysis), 5. Folgen und Reihen von Funktionen, Potenzreihen, Fourierreihen, 6. Differentialrechnung in endlich-dimensionalen Räumen, 7. Gewöhnliche Differentialgleichungen. Die letzten 50 Seiten präsentieren 15 Probleme, von denen jedes eine Subtheorie darstellt, die den vorangehenden Stoff vertieft. Gelöst werden die 15 Probleme im Band "Problèmes".

Eine größere Zahl von Tippfehlern tut der gebotenen mathematischen Qualiltät keinen Abbruch. Auch wenn eine Einleitung, eine Bibliographie und ein Stichwörterverzeichnis fehlen, ist die Präsentation übersichtlich und didaktisch einprägsam.

An mathematischen Ungenauigkeiten konnte ich nur feststellen, daß gewisse Begriffe verwendet werden, die erst später erklärt werden (z.B. „stückweise stetig") oder, daß auf p. 154 $\pi/2$ als kleinste positive Nullstelle von cos definiert wird, ein entsprechender Satz aber erst auf p. 169 bewiesen wird. Um einen exemplarischen Eindruck von der Qualität der Bücher zu geben, zitiere ich Problem 15 im Wortlaut (in deutscher Übersetzung):

• *Frage 1: Untersuchung der Differentialgleichung von Riccati*: $y' = x^2 + y^2$:

Wir betrachten die Differentialgleichung (E_1) $y' = x^2 + y^2$, in der y eine unbekannte reelle Funktion der reellen Variablen x ist.

— 1. Sei φ eine maximale Lösung von (E_1) und I ihr offenes Definitionsintervall. (a) Zu zeigen: φ ist strikt monoton wachsend. (b) Unter der Annahme, es existiere $x_0 \in I$ mit $\varphi(x_0) > 0$, ist zu beweisen, daß $\varphi'(x)/\varphi(x)^2 \geq 1$ für $x \geq x_0$, $x \in I$ gilt. Leiten

Sie daraus her, daß I nach oben beschränkt ist. (c) Was kann über I ausgesagt werden, wenn es $x_1 \in I$ mit $\varphi(x_1) < 0$ gibt? (d) Zu zeigen: I ist beschränkt. (e) Bestimmen Sie das Bild von I unter φ. (f) Wieviele ungerade maximale Lösungen gibt es?

— 2. Wir wählen ein festes $\alpha \in \mathbb{R}$; für jedes $\beta \in \mathbb{R}$ bezeichnen wir mit $I(\beta)$ das Definitionsintervall der maximalen Lösung, die $\varphi(\alpha) = \beta$ erfüllt. Vergleichen Sie die Grenzen der Intervalle $I(\beta_1)$ und $I(\beta_2)$ für $\beta_1 \leq \beta_2$.

— 3. Sei H die Menge der Punkte $(u,v) \in \mathbb{R}^2$, für die eine Lösung φ von (E_1) mit $\varphi(u) = v$ und $\varphi''(u) = 0$ existiert. Skizzieren Sie H, indem Sie die Asymptote angeben und ebenso die Punkte, in denen die Tangente parallel zu einer der Koordinatenachsen ist.

— 4. Fixieren wir eine reelle Zahl t und bezeichnen mit φ_t jene maximale Lösung, die in t verschwindet. Zu berechnen: die Krümmung und den Krümmungsmittelpunkt von φ_t im Punkt $(t,0)$.

• *Frage 2: Untersuchung der Differentialgleichung: $y'' + x^2 y = 0$*

Wir bezeichnen mit $\mathcal{S}$ den Vektorraum der auf $\mathbb{R}$ definierten, reellen Funktionen $f \in C^2$, die der Differentialgleichung (E_2) $y'' + x^2 y = 0$ genügen.

— 1. Geben Sie die Dimension von $\mathcal{S}$ an.

— 2. (a) Bestimmen Sie Lösungen von (E_2) als Potenzreihen und berechnen Sie ihren Konvergenzradius. (b) Stellen Sie damit Funktionen $f_1, f_2 \in \mathcal{S}$ mit $f_1(0) = 1,\ f_1'(0) = 0,\ f_2(0) = 0,\ f_2'(0) = 1$ als Potenzreihen dar. (c) Sei f eine Funktion aus $\mathcal{S}$. Drücken Sie f durch f_1, f_2 und die Zahlen $a = f(0),\ b = f'(0)$ aus. Untersuchen Sie die Position des Graphen von f bezüglich seiner Tangente im Punkt $(0,a)$, wenn sich a und b ändern.

— 3. Zeigen Sie, daß f_1 strikt positiv auf dem Intervall $[-2,2]$ ist. [Untersuchen Sie die ersten 4 Terme der Reihe.]

• *Frage 3: Vergleich der Lösungen von (E_1) und von (E_2).*

Wir bezeichnen mit φ eine C^1-Funktion, definiert auf einem Intervall I, mit Φ eine Stammfunktion von φ. Wir setzen: $f(x) = e^{-\Phi(x)}$ für $x \in I$.

— 1. Welcher notwendigen und hinreichenden Bedingung muß φ genügen, damit f Lösung von (E_2) ist?

— 2. Sei φ eine maximale Lösung von (E_1) und I ihr offenes Definitionsintervall. (a) Bestimmen Sie den Grenzwert von $f(x)$, wenn x gegen die Grenzen von I geht. (b) Wir setzen φ ungerade voraus. Was folgt daraus für I? Berechnen Sie die Ableitung $\varphi^{(n)}(0)$, wenn n nicht die Form $4k+3$ hat.

— 3. Sei $f \in \mathcal{S}$, f nicht identisch 0. (a) Sei x_0 eine Nullstelle von f. Zu zeigen: es gibt eine Umgebung von x_0, auf welcher $f \neq 0$ ist außer in x_0. (b) Zeigen Sie, daß die Menge $f^{-1}(\{0\})$ der Nullstellen von f weder nach oben noch nach unten beschränkt ist. (c) Wie verändert sich f zwischen 2 aufeinanderfolgenden Nullstellen? (d) Ermitteln Sie eine Reihenentwicklung im Ursprung bis zur 7. Potenz der ungeraden Lösung der Differentialgleichung (E_1).

(Anmerkung: Die Lösungen können durch Besselfunktionen ausgedrückt werden. Vgl. E. Kamke: Differentialgleichungen, Teubner, Stuttgart, 1977, 9. Aufl., p. 21, 4.8.; p. 295, 1.14; p. 401, 2.13; p. 440, 2.162, (10), (11))

Beide Bücher können zum „Durcharbeiten“ bestens empfohlen werden.

N. Ortner (Innsbruck)

Internationale Mathematische Nachrichten

Symposium on Logic, Mathematics, and Computer Science: Interactions

We would like to invite you to the *Symposium on Logic, Mathematics, and Computer Science: Interactions* in honor of Bruno Buchberger's 60th birthday. The colloquium will be held from October 22 to October 24, 2002 in Hagenberg, Austria.

Henk Barendregt (University of Nijmegen, Netherlands), *Manfred Broy* (TU München, Germany), *Dana Scott* (Carnegie Mellon University, Pittsburgh), *Doron Zeilberger* (Rutgers Mathematics Department, New Brunswick) and also *Bruno Buchberger* (RISC, Universit"at Linz) will present their views on the interaction of logic, mathematics, and computer science.

Tuesday, October 22 (Bruno's actual birthday!) will be devoted to the invited lectures, Wednesday and Thursday will feature contributed talks. The Call for Papers and some submission guidelines can be found on the web page (see the address below).

If you are interested in attending the symposium, visit the symposium's web-page under *http://www.risc.uni-linz.ac.at/conferences/LMCS2002/* or send an email to *Betina.Curtis@risc.uni-linz.ac.at*.

(The faculty of RISC-Linz)

Gottfried Wilhelm Leibniz-Ausstellung

Vom 19. Juli bis 4. Oktober 2002 findet in der Aula des Hauptgebäudes der Österreichischen Akademie der Wissenschaften (Dr. Ignaz Seipel-Platz 2, 1010 Wien) eine Ausstellung über Gottfried Wilhelm Leibniz statt.

(ÖAW)

Wittgenstein- und START-Preise

Der Wittgenstein-Preis 2002 wurde dem Physiker *Ferenc Krausz* (TU Wien) für seine Arbeiten auf dem Gebiet der Ultrakurzpuls-Lasertechnik verliehen.

Die START-Preise gingen an den Physiker *Wolfgang Heiß* (Univ. Linz), den Altorientalisten *Michael Jursa* (Univ. Wien), den Mediziner *Georg Schett* (Univ. Wien), den Informatiker *Dieter Schmalstieg* (TU Wien) und an den Mathematiker *Joachim Schöberl* (Univ. Linz).

(FWF)

Sunyer i Balaguer-Preis

Alexander Lubotzky (Hebrew University of Jerusalem) und *Dan Segal* (Oxford University) erhielten den Sunyer i Balaguer-Preis 2002 für ihre Monographie "Subgroup Growth" und *André Unterberger* (University of Reims) für seine Monographie "Automorphic Pseudodifferential Analysis and Higher-Level Weyl Calculi".

(Notices AMS)

Rollo Davidson-Preis

Der Rollo Davidson-Preis 2002 wurde *Stanislav Smirnov* (Royal Institute of Technology, Stockholm) und *Balaji Prabhakar* (Stanford University) verliehen.

(Notices AMS)

O.Univ.Prof. Mag.rer nat. Dr.phil habil. Hans Sachs: 60 Jahre

Am 15. 1. 2002 wurde im Rahmen einer internationalen Tagung über „Algebra, Analysis und Geometrie" im Tagungshotel Lipa in Szentgotthárd (Ungarn) der 60. Geburtstag von Univ.-Prof. Dr. *Hans Sachs* (Montanuniversität Leoben) gefeiert. In einem ausgezeichnet organisierten Festkolloquium wurden die folgenden Vorträge zu Ehren des Jubilars gehalten:

Univ.-Doz. Dr. F. Mészáros (Leoben): Laudatio I.

o.Univ.Prof. Dr. Gy. Maurer (Budapest): Laudatio II.

o.Univ.Prof. Dr. A. Schmid-Kirsch (Hannover): Bewegung in der Geometrieausbildung.

o.Univ.Prof. Dr. F. Schipp (Budapest): Fast Fourier Transform for Rational Systems.

o Univ.Prof. Dr. G. Tironi (Trieste): Compattificazioni e misure a valori zero-uno.

Prof. Dr. L. Kászonyi (Szombathely): Über einige Anwendungen von DLI-Sprachen.

o Univ.Prof. Dr. B. Wegner (Berlin): Ein Konvexifizierungsproblem von Erdős – Seine Geschichte und neuere Entwicklung dazu.

Die niveauvollen Vorträge zeigten nicht nur die neueren Entwicklungen auf diesen verschiedenen mathematischen Teilgebieten auf, sondern dokumentierten wieder einmal, wie sehr unterschiedliche Fachdisziplinen miteinander verknüpft sein können. Der festliche Rahmen wurde durch ein Streichquartett, eine ungarische Volkstanzgruppe und eine Zigeunerkapelle abgerundet. Abschließend bedankte sich der Jubilar mit einem von ihm verfassten elegischen Distichon, das von Dr. M. Fink in einfühlsamer Weise ins Ungarische übersetzt wurde. Auf Grund der großen Nachfrage nach diesem Gedicht, erlaube ich mir, es nachstehend mit Genehmigung des Verfassers abzudrucken:

DANKSAGUNG

Sechzig Jahre vergehen im Fluge, was bleibt noch vom Leben?
Sehnsucht nach glücklicher Zeit, kurz wie ein flüchtiger Tag.
Wahrlich man fragt sich gedankenversunken mit Schwermut im Herzen
Gibt es ein wirkliches Jetzt? Gibt es ein wirkliches Hier?

Noch aber leuchtet mir strahlend die Sonne, es blüht die Akazie,
Und längs der Mauer dahin, duftet der gelbe Jasmin.
Wenn ich im Grase oft träumend verweile, die Wolken betrachtend,
Dann denk ich oft so bei mir, Zeit warum bleibst du nicht steh'n?
Oder wenn nicht, so schenk mir noch einmal, drum bitt ich dich sehnlichst
Nur einen Tag jener Zeit, die mir die glücklichste war.
Aber du schweigst mir, erhabener Kosmos, du lässt mich alleine,
Gleich einem einsamen Tor, der auf der Suche stets ist.

Doch die Erkenntnis, sie liegt oft so nahe, man muss sie nur sehen.
Freundschaft, Liebe und Dank – ihr seid das einzige Gut,
Das uns're ängstlichen Seelen beflügelt in Freude und Kummer,
Ihr seid ein himmlischer Tau – ferne der spießigen Welt.
Und so dank' ich euch allen, euch lieben und ehrlichen Freunden,
Bleibt auch in Zukunft mir hold – bis uns einst scheidet der Tod.

HÁLÁS KÖSZÖNET

60 év elröppen, akár egy másodperc, és mi marad belled élet?
A vágy a boldog idk után, mely rövid mint a tiszavirág léte.
Az ember töprengve és mélabs szívvel kérdi:
Igazi valóság a „most"? Igazi valóság az „itt"?

Ma még ragyogón süt a nap, az akác virágzik,
A fal mentén bódítón illatoz a sárga jázmin.
A pázsiton álmodva, a felhkön merengve,
Gyakori az óhaj: Id állj meg most, azonnal!
De ha ezt nem tennéd meg, akkor sóvárogva kérlek:
letem legboldogabb napját hozd vissza még egyszer.
De te hallgatsz, fenséges kozmosz, szóra sem méltatod,
Magányos lelkem, és én megszállottan a megoldást keresem.

Holott a felelet gyakran oly közeli, csak fel kell ismerni:
Barátság, szeretet, köszönet – ti vagytok az egyedüli kincs.
Háborgó lelkünknek, mely öröm és bánat között csapong,
Ti adtok mennyei malasztot, távol a világ durvaságaitól.
gy mondok köszönetet szeretett, igaz barátaimnak,
Legyetek hozzám kegyesek, holtomiglan, holtodiglan.

Fordította: Dr. M. Fink

(F. Mészáros, Leoben)

Nachrichten der Österreichischen Mathematischen Gesellschaft

Brief des Vorsitzenden

Ich möchte Sie darüber informieren, was seit dem Erscheinen des letzten Heftes der IMN im Rahmen der ÖMG geschehen ist und Sie insbesondere über in meinem letzten Brief beschriebene Aktivitäten auf dem Laufenden halten:

Die Frage einer gesamtösterreichischen Evaluierung der Mathematik hat die Diskussion der vergangenen Monate in der ÖMG beherrscht. Dieser und schon der vorige Vorstand der ÖMG sind sehr vorsichtig an dieses Projekt herangegangen, wir haben uns für eine Beteiligung an dieser Evaluierung nur unter den beiden Voraussetzungen ausgesprochen, dass die Betroffenen diese in ihrer überwiegenden Mehrheit für gut halten und dass aus einer solchen Evaluierung (positive) Konsequenzen für die österreichische Mathematik und die einzelnen Standorte zu erwarten sind. Um dies sicherzustellen, wurde einerseits eine Meinungsbildung in den Landessektionen eingeleitet und andererseits das Ministerium ersucht, die Rektoren aller betroffenen Universitäten um ihre Stellungnahme zu diesem Vorhaben zu bitten.

Die interne Meinungsbildung hat zu einem überwiegend positiven Ergebnis geführt, wenn auch nicht ausschließlich: Skepsis bis Ablehnung kam insbesondere aus Klagenfurt, Leoben und Salzburg, vom Mathematischen Institut der Universität Wien war über die Landessektion Wien keine Stellungnahme zu erhalten. Eine Weiterführung der Diskussion ist aber angesichts der negativen Stellungnahmen von vier Rektoren, insbesondere der Rektoren der Universitäten Wien und Graz, ohnehin sinnlos. Ob es nun zu einer gesamtösterreichischen Evaluierung der Mathematik kommen wird oder nicht, ist unklar, jedenfalls wird sich aber die ÖMG daran nicht beteiligen; und angesichts der erwähnten Stellungnahmen der Rektoren halte ich eine solche Evaluierung für nicht sinnvoll, da eine Umsetzung von Ergebnissen in keiner Weise gewährleistet ist. Wenn auch der ÖMG-Vorstand erklärt hat, einer Evaluierung weiterhin offen gegenüberzustehen, falls sich in näherer Zukunft die Voraussetzungen ändern sollten, so meine ich, dass der gegenwärtige Zeitpunkt (gerade noch rechtzeitig vor dem Übergang ins neue Universitätsgesetz) der einzige sinnvolle in der näheren Zukunft für ein solches Unternehmen gewesen wäre.

Ob das geschilderte Ergebnis der aufwendigen Evaluierungsdiskussion ein gutes Ergebnis ist, werden wir wohl nie erfahren. Wir alle sparen uns viel Arbeit, allerdings werden künftige Entscheidungsträger eben ihre Entscheidungen ohne die objektiven Grundlagen, die eine Evaluierung durch internationale Gutachter hätte bringen können, treffen müssen (oder können). Ob man das als gut oder schlecht ansieht, hängt von der subjektiven Sichtweise ab.

Jedenfalls: dass die österreichische Mathematik international gut dasteht, können wir auch auf andere Weise darstellen, etwa durch die große Zahl von mathematisch orientierten Spezialforschungsbereichen, Forschungsschwerpunkten, Wissenschaftskollegs und Kompetenzzentren sowie die überdurchschnittliche Häufung von Start- und Wittgenstein-Preisen im Bereich der Mathematik. Auch die Österreichische Akademie der Wissenschaften überlegt eine wesentliche Verstärkung ihrer mathematischen Aktivitäten durch die Gründung eines großen Instituts auf dem Gebiet der Angewandten Mathematik. Und schließlich ist auch noch zu erwähnen, dass auf dem nur alle vier Jahre stattfindenden Weltkongreß der Angewandten Mathematik, dem International Congress for Industrial and Applied Mathematics (ICIAM, Sydney, 7. bis 11. Juli 2003) gleich zwei österreichische Mathematiker Hauptvorträge halten werden, nämlich Peter Markowich (Universität Wien) und Harald Niederreiter (derzeit Singapur). Als Mitglied des Programmkomitees von ICIAM möchte ich auch über diese Hauptvorträge hinaus eine starke österreichische Beteiligung anregen, etwa durch die Organisation von Minisymposia; Informationen über deren Einreichung finden Sie unter *http://www.iciam.org*.

Die Diskussion mit der DMV und der AMS über die 2005 stattfindenden Kongresse ist inzwischen abgeschlossen. Wir werden im September 2005 wie üblich den „großen“ ÖMG-Kongreß gemeinsam mit der DMV veranstalten, und zwar in Klagenfurt; ein besonderer Schwerpunkt, den die ÖMG und die DMV dabei gemeinsam verfolgen wollen, wird dabei der Kontakt zu Mathematikern in Südosteuropa sein. Im Frühjahr 2005 wird eine kleinere Tagung in Mainz veranstaltet werden, und zwar von DMV, EMS und ÖMG gemeinsam. Die Vorbereitungen für die Nachbarschaftstagung in Bozen (22. bis 26. September 2003) laufen unter der Leitung von Herrn Oberguggenberger planmäßig.

Eine erste Aktivität im Bereich der Öffentlichkeitsarbeit stellt eine Veranstaltung in Graz am 4. 10. 2002 mit dem Titel „Faszination Mathematik“ dar, die sich hauptsächlich an Lehrer und Schüler höherer Klassen richtet. Das Programm finden Sie an anderer Stelle in diesem Heft. Diese Veranstaltung soll auch die Gründungsveranstaltung einer Lehrersektion der ÖMG sein. Der plötzliche Tod von Hans-Christian Reichel hat uns nicht nur den Vorsitzenden der Didaktikkommission genommen, der diese Kommission sehr engagiert geleitet hat, sondern auch einen wissenschaftlich sehr angesehen Kollegen, der sich für die Anliegen der österreichischen Mathematik insbesondere im Zusammenhang mit dem Schulunterricht und auch für die ÖMG sehr engagiert hat. Die Lücke, die er hinterlas-

sen hat, wird schwer zu schließen sein. Im Herbst werden der Vorstand und der Beirat der ÖMG diskutieren, wie man die schulbzogenen Aktivitäten der ÖMG (auch unter Berücksichtigung der in Gründung befindlichen Lehrersektion) optimal strukturieren kann. Ich bitte um Anregungen dazu.

In der Generalversammlung am 9. Dezember 2002, zu der Sie die Einladung an anderer Stelle in diesem Heft finden, werden wieder der Förderungspreis und die Studienpreise der ÖMG vergeben. Die Schülerpreise wurden für dieses Jahr ausgesetzt, weil der Vorstand der Meinung war, dass die bisherige Einschränkung auf mathematische Fachbereichsarbeiten zu eng war, wie auch die Anzahl der Einreichungen gezeigt hat. Wir überlegen eine Ausweitung der Ausschreibung etwa auf Gruppenarbeiten zu mathematischen Themen oder zur Anwendung mathematischer Methoden, möglicherweise auch für die Unterstufe. Auch dazu wären Anregungen höchst willkommen.

o.Univ.-Prof. Dipl.-Ing. Dr. Heinz W. Engl
Institut für Industriemathematik
Johannes Kepler Universität Linz
Altenbergerstraße 69
4040 Linz
e-mail *engl@indmath.uni-linz.ac.at*

Hans-Christian Reichel: 16. 5. 1945 – 28. 6. 2002

Am 28. 6. 2002 verstarb der Wiener Mathematiker und Vorsitzende der Didaktikkommission der ÖMG, Univ. Prof. Dr. *Hans-Christian Reichel*. Zwei seiner ehemaligen Kollegen am Institut für Mathematik der Universität Wien, Harald Rindler und Stefan Götz, haben einen kurzen Nachruf verfasst.

Die Nachricht vom Hinscheiden von Kollegen Reichel hat große Betroffenheit ausgelöst. Ich habe aus ganz Österreich, aber auch aus dem Ausland schon viele bestürzte Rückmeldungen erhalten, nicht nur von Mathematikern, Didaktikern, maßgeblichen Persönlichkeiten aus dem Schulbereich sowie Wissenschaftstheoretikern, sondern auch von anderen Geisteswissenschaftern, Theologen und aus vielen anderen Bereichen, zu denen Hans-Christian Reichel auch in enger Verbindung stand.

Auch international gesehen gibt es nur wenige Mathematikdidaktiker von Rang, die derart viel für die Ausbildung in der Lehre an Hoch- und Mittelschulen getan

und gleichzeitig auch wesentliche wissenschaftliche Beiträge zur Mathematik geleistet haben wie Kollege Reichel zur Topologie, seinem Habilitationsgebiet, wo er ebenso internationale Anerkennung gefunden hat, (belegt durch Gastprofessuren in Deutschland oder längere Auslandsaufenthalte, etwa in Oxford). Seine großartigen Leistungen waren nur aufgrund seiner vielfältigen Begabungen und seiner großen Allgemeinbildung möglich und wegen seines unerhörten aufopfernden Arbeitseinsatzes bis zu letzt, trotz seiner schweren Erkrankung.

Viele von uns verlieren in ihm auch einen lieben treuen Freund, wie er heutzutage kaum mehr zu finden ist. Wesentliches, was wir nunmehr verloren haben, wird uns erst jetzt so richtig bewusst.

Unser Institut verdankt ihm außerordentlich viel; in seinen Werken wird er weiterleben.

Harald Rindler

Ich habe Herrn Professor Reichel in den späten 80-er Jahren in einer seiner Vorlesungen kennengelernt. Neben den modernen Inhalten (damals hat gerade die Stochastik Eingang in den österreichischen Mathematikunterricht gefunden), die er präsentierte, war es vor allem seine Begeisterung für die Mathematik an sich, die mich und so viele andere faszinierte, und die ihren Niederschlag in einem mitreißenden Vortrag fand. Seine Art zu lehren ist vielen von ihm ausgebildeten Lehrerinnen und Lehrern zum Vorbild geworden.

Stets war er auch bemüht, in seinen Lehrveranstaltungen Querverbindungen innerhalb der Mathematik aufzuzeigen sowie Anwendungen derselben. Seine Studentinnen und Studenten sollten ein adäquates Bild der modernen Mathematik erhalten, das sie dann selbst als Lehrerin bzw. Lehrer weitergeben konnten. Das Schulfach „Mathematik“ hat er auf diese Weise als einen sich immer weiter entwickelnden Beitrag zur (Allgemein-)Bildung verstanden. Dies ist in seiner Lehre und Haltung eindrucksvoll zum Ausdruck gekommen.

Überhaupt war ihm diese mathematische Haltung sehr wichtig, die sich während des Studiums in jeder/jedem Studierenden entwickeln sollte. Sie sollte den Schülerinnen und Schülern ein Beispiel geben, wie die Beschreibung von Sachverhalten, Problemen, Situationen – der Welt an sich bzw. Teilaspekten davon – gelingen kann. Dies macht eigentlich die Stellung der Mathematik innerhalb des schulischen Fächerkanons aus.

Sein Einsatz hat sich in mannigfachen Funktionen manifestiert. Er war u.a. Vorsitzender der ÖMG-Didaktikkommission, Studiendekan, Mitherausgeber der „Mathematischen Semesterberichte“, Mitglied des wissenschaftlichen Beratungskomitees des „Journals für Didaktik der Mathematik“, Lehrbuchautor etc. Seine Vielfalt, seine wissenschaftliche Breite war eine seiner herausragenden Stärken.

Mich persönlich hat Christian Reichel in das wissenschaftliche und universitäre Leben sehr behutsam eingeführt. Von der Betreuung meiner Diplomarbeit über

die Dissertation bis zur Habilitation hat er mich in fürsorglicher Art und Weise begleitet. Seine Ratschläge haben mir immer neue Sichtweisen eröffnet und seine schon angesprochene Begeisterung und Fähigkeit, auch andere zu begeistern, waren für mich immer Ansporn zu jener Weiterentwicklung, die für die Wissenschaft essentiell ist. Das Erbe, welches er hinterlässt, ist gewaltig, und die Herausforderungen, die auf uns zukommen, sind es auch wie sehr hätten wir daher seinen Rat auch weiterhin gebraucht!

Aus unserer wissenschaftlichen Zusammenarbeit ist auch eine persönliche Freundschaft entstanden. Er wird mir sehr fehlen.

Stefan Götz

Persönliches

Prof. *Peter Gruber* erhielt im Oktober 2001 das Österreichische Ehrenkreuz für Wissenschaft und Kunst, 1. Klasse. Weiters wurde er im Februar 2002 als korrespondierendes Mitglied in die Bayrische Akademie der Wissenschaften gewählt.

Neue Mitglieder

Stefan Haller, Dr. — Institut für Mathematik, Universität Wien, Strudlhofg. 4, A 1090 Wien, Österreich. geb. 1971. 1990–1999 Studium der Mathematik Universität Wien (1995 Mag.rer.nat., 1999 Dr.rer.nat.) 2000/01 Forschungsstipendium Ohio State University, seit 2001 FWF-Forschungsassistent und seit Mai 2002 halbbeschäftigter Assistent am Institut für Mathematik der Universität Wien. e-mail *stefan@mat.univie.ac.at*.

Gert Kadunz, Dr. — Abteilung für Didaktik der Mathematik, Institut für Mathematik, Universität Klagenfurt, Universitätsstr. 65, A 9020 Klagenfurt. geb. 1958. Lehramtsstudium Mathematik, Philosophie, Psychologie und Pädagogik, 1984–1991 Unterrichtstätigkeit BRG Klagenfurt-Viktring, 1991 Vertragsassistent, und seit 1992 Universitätsassistent Institut für Mathematik, Universität Klagenfurt (Didaktik der Mathematik, Visualisierung, Entwicklung und Bewertung von Geometriesoftware) e-mail *gert.kadunz@uni-kln.ac.at*.

Walther Neuper, Dr. techn. — Getreideg. 33, A 5020 Salzburg. geb. 1949. AHS-Lehrer, Consultant für UNESCO, UNO-Institut, Projektleiter Softwareentwicklung, HTL-Lehrer. e-mail *neuper@ist.tugraz.at*.

Faszination Mathematik

4. 10. 2002
TU Graz

Vorläufiges Programm

9:30– 9:45: Begrüßung.

9:45–10:15: *Prof. Heinz Engl* (Univ. Linz): Mathematik in der Industrie.

10:15–10:45: *Dr. Jürgen Krasser* (AVL List GesmbH, Graz): Der Einsatz mathematischer Methoden in der AVL.

10:45–11:15: *Prof. Robert Tichy* (TU Graz): Faszination der reinen Mathematik.

11:30–12:00: *Dr. Marion Schulz-Reese* (Univ. Kaiserslautern): Mathematische Modellierungswettbewerbe für Schüler.

12:00–12:30: *Prof. Franz Kappel* (Univ. Graz): Mathematik in den Biowissenschaften.

12:30–15:00: *Forschungspräsentationen*: Dr. Steve Keeling (Univ. Graz, Koordination), Doz. Grabner (TU Graz), Prof. Otmar Scherzer (Universität Innsbruck) Inst. für Geometrie (TU Wien), Inst. für Geometrie (TU Graz), Dr. Michael Hintermüller (Univ. Graz), Dr. Jerry Batzel (Univ. Graz), Doz. Gunther Peichl (Univ. Graz), Doz. Wolfgang Ring (Univ. Graz), Doz. Bernd Thaller (Univ. Graz).

Buffet.

15:00–16:00: *Podiumsdiskussion*: Mathematik in der neuen Oberstufe: Was sollte kommen, was wird kommen?

Konzept und Ziel

Diese von der ÖMG organisierte Veranstaltung hat zum Ziel, eine möglichst breite Öffentlichkeit über mathematische Forschung zu informieren, und zwar mit besonderem Hauptaugenmerk auf die derzeit an österreichischen mathematischen Instituten stattfindende Forschung. Besondere Schwerpunkte sollen im Bereich der technisch anwendbaren Mathematik, wie sie speziell für Graz eine große Bedeutung hat, gesetzt werden. Gleichzeitig sollen auch die Motivationen der Forschenden zur Auseinandersetzung mit diesen Bereichen an interessierte Schüler und Lehrer weitervermittelt werden.

Die ÖMG möchte als Veranstalter ein Zeichen dafür setzen, dass der Schnittstelle Schule – Universität in Zukunft noch viel mehr Beachtung als bisher geschenkt werden soll. So ist diese Veranstaltung auch als “Kick-off” für die im Entstehen begriffene Lehrersektion gedacht, und es soll im Rahmen der Veranstaltung dafür geworben werden, dass sich möglichst viele Lehrer zu einer Mitgliedschaft und vor allem Mitarbeit bei der ÖMG entschließen. Für die Vortragenden bzw. für die Betreuer der Forschungspräsentationen ist diese Veranstaltung eine Möglichkeit, künftigen Studenten und Mitarbeitern die aktuellen Forschungsbereiche vorzuführen. Es besteht die Hoffnung, dass es möglich sein sollte, mehr Maturanten für diese Studien- und Forschungsbereiche zu begeistern, vor allem unter dem Gesichtspunkt, dass ein großer Bedarf an Absolventen in diesen Bereichen herrscht. Schülern (und manchen ihrer Lehrer) ist die Vielfalt der mathematischen Forschung möglicherweise nicht hinreichend bekannt, und dem soll hier abgeholfen werden. Für Schüler und Lehrer ist dies eine Informationsveranstaltung, die über Studien- und Forschungsmöglichkeiten, aber auch über Berufsmöglichkeiten, Auskunft geben soll.

Schließlich soll diese Veranstaltung auch in der Öffentlichkeit Beachtung finden. Besonders durch die Podiumsdiskussion (und die geplante Teilnahme von Journalisten und öffentlichen Meinungsträgern) sollen mediengerecht die Anliegen der ÖMG und der mathematischen Forschung in die Öffentlichkeit transportiert werden.

Organisation: Dr. Robert Geretschläger *robert.geretschlaeger@brgkepler.at*

Forschungspräsentationen: Dr. Stephen Keeling *keeling@uni-graz.at*

Lokale Organisation am Institut für Mathematik
der TU Graz: Univ.Prof. Robert Tichy *tichy@tugraz.at*

Gesamtleitung: Univ Prof. Heinz Engl *engl@indmath.uni-linz.ac.at*

Einladung zur Generalversammlung der ÖMG

Montag, 9.12.2002, 16 Uhr c.t.

Nöbauer-Hörsaal, TU Wien

Tagesordnung:

1. Feststellung der Beschlussfähigkeit
2. Berichte des Vorsitzenden und weiterer Vorstandsmitglieder, insbesondere des Kassiers
3. Berichte aus den Landessektionen
4. Bericht der Rechnungsprüfer und gegebenenfalls Entlastung des Vorstands
5. Neuwahl der Landesvorsitzenden und des Beirats
6. Neuwahl der Rechnungsprüfer
7. Verleihung des Förderungspreises und der Studienpreise
8. Organisation der schul- und fachhochschulbezogenen Aktivitäten der ÖMG: Kommissionen, Lehrersektion
9. Allfälliges.

Im Anschluss: Vorführung des Videointerviews mit Harald Niederreiter.