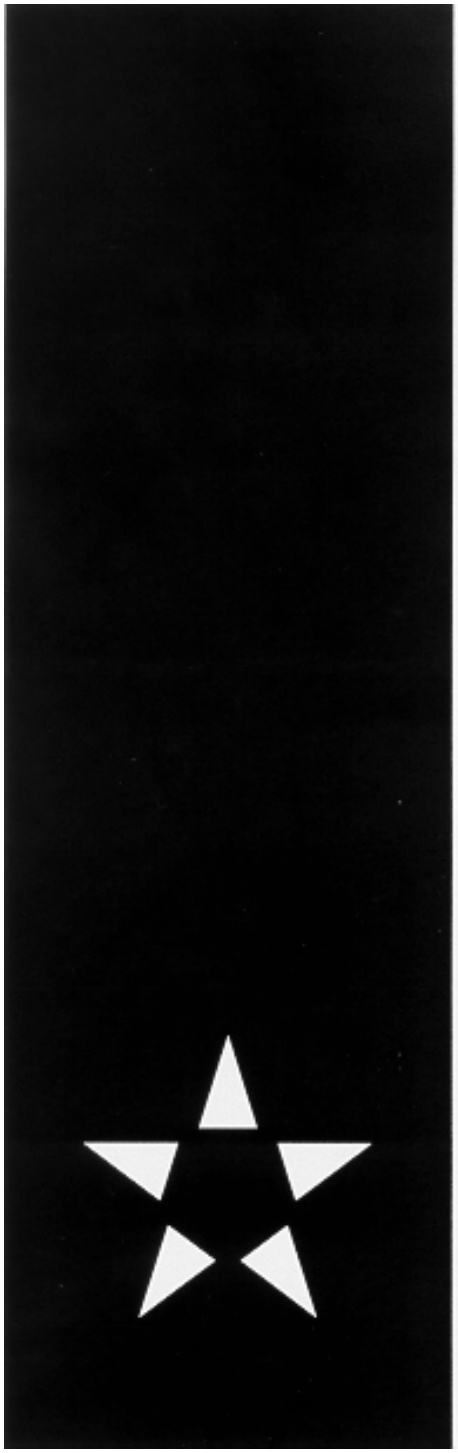

IMN

Internationale
Mathematische
Nachrichten
Nr. 186

Hans Sagan (1928-2000)
Primzahltests
J.-P. Bourguignon im
Interview

Österreichische
Mathematische
Gesellschaft

April 2001

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 Zeitschift 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.mat.univie.ac.at/∼oemg/*

Bezug:

Die IMN erscheinen dreimal jährlich und werden von den Mitgliedern der Österreichischen Mathematischen Gesellschaft bezogen. Jahresbeitrag: 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: Kopitu, Wiedner Hauptstraße 8–10, 1040 Wien.

ISSN 0020-7926.

Internationale Mathematische Nachrichten

International Mathematical News

Nouvelles Mathématiques Internationales

Nr. 186 (55. Jahrgang) **April 2001**

Inhalt

Christa Binder: Hans Sagan(1928–2000) 1

Johann Wiesenbauer: Primzahltests und Faktorisierungsalgorithmen I . . . 9

F. J. Craveiro de Carvalho, Jorge Picado: Interview with Jean Pierre Bourguignon* 25

Buchbesprechungen 35

Internationale Mathematische Nachrichten 74

Nachrichten der Österreichischen Mathematischen Gesellschaft 81

Das Titelblatt zeigt einen fünfeckigen Stern und soll die Zahl 5 und das regelmäßige Fünfeck symbolisieren, die in der Mathematikgeschichte immer wieder eine wichtige Rolle spielten. So erkannten die Griechen anhand des Fünfecks, dass es inkommensurable Strecken — eben die Länge $\sqrt{5}$ — gibt. Es ist auch der goldene Schnitt $\gamma = (1+\sqrt{5})/2$ in dieser Figur *versteckt*. Weiters ist die Zahl $5 = 2^{2^1} + 1$ eine Fermatsche Primzahl, und daher ist — wie Gauß allgemein erkannte — das regelmäßige Fünfeck mit Zirkel und Lineal konstruierbar. Schließlich ist der vollständige Graph C_5 mit 5 Knoten der kleinste nicht-planare Graph.

Internat. Math. Nachrichten
Nr. 186 (2001), 1–7

Hans Sagan (1928–2000)

Christa Binder

Technische Universität Wien

Hans Sagan wurde am 15. Februar 1928 in Wien geboren. Sein Vater war Hans Sagan, seine Mutter Josefa, geborene Seif. Nach Besuch der vierjährigen Pflicht-(Volks-)schule besuchte er mit kurzer kriegsbedingter Unterbrechung die Oberschule und maturierte am 4. Juni 1946 am Bundesgymnasium Wien, Albertgasse, mit Auszeichnung. Anschließend studierte er an der Universität Wien Mathematik mit Nebenfach Physik, verfasste eine Dissertation über ein Thema aus der Variationsrechnung unter der Leitung von Johann Radon und promovierte am 15. Juli 1950 zum Doktor phil. Von der schwedischen Studentenschaft finanziert, konnte er nach der Promotion zwei Monate in Schweden studieren. Danach wurde er

ISSN 0020-7926

Assistent bei Funk an der II. Lehrkanzel für Mathematik an der Technischen Hochschule Wien. Im Mai 1954 trat er von dieser Stelle zurück, um der Fakultät der Montana State University (damals Montana State College) beizutreten. 1957 folgte er einem Ruf als Associate Professor an die University of Idaho, wo er vier Jahre später (1961) zum (full) Professor und Institutsvorstand ernannt wurde. 1963 erhielt er einen Ruf an die North Carolina State University als full Professor, eine Position, die er bis zur Emeritierung 1993 innehielt.

Am 20. März 1954 heiratete er Ingeborg Ulbrich und am 12. Jänner 1956 wurde die Tochter Ingrid geboren.

Im Sommersemester 1964 hielt er eine dreistündige Vorlesung über *Approximationsmethoden vom funktionalanalytischen Standpunkt* als Gastprofessor der Technischen Hochschule München. Im Sommersemester 1972 hielt er eine zweistündige Vorlesung über *Variationsrechnung* als (unbezahlter) Gastprofessor an der Universität Wien. Insgesamt folgte er 51 Einladungen, um an 46 Universitäten und Colleges in 15 Bundesstaaten und 3 kanadischen Provinzen Gastvorträge zu halten. Im Jahre 1969 wurde er secundo loco für den neugeschaffenen Lehrstuhl für Mathematik an der Baufakultät der Universität Innsbruck nominiert (Helmberg nahm die Berufung an) und 1976 wurde er an die Lehrkanzel für technische Mathematik an der Technischen Universität Wien berufen (Nachfolge Bukovics). Diesen Ruf lehnte er nach langen Verhandlungen mit gemischten Gefühlen und einem gewissen Maß an Bedauern ab.

Folgende Ehren und Ehrenämter wurden ihm zuteil: Für die Studienjahre 1959/60 und 1960/61 erhielt er den *Outstanding Faculty Award* von der Studentenschaft der University of Idaho, im Jahre 1960 den *Poteat Award* von der North Carolina Academy of Sciences. Von 1963 bis 1973 war er *Associate Editor* des *Mathematics Magazine* und seit 1963 war er (mit kurzen Unterbrechungen) *Visiting MAA Lecturer*. Von 1965 bis 1974 war er Mitglied und, während der letzten Jahre seiner Amtszeit, Sekretär des Komitees der Mathematical Association of America für den jährlichen Mathematik-Wettbewerb.

1960 erhielt er die US-Staatsbürgerschaft und bald darauf die *Q-clearance*, um Regierungsaufträge durchzuführen. Viele seiner Arbeiten waren *classified*, was die relativ geringe Anzahl an Publikationen in seinen frühen Jahren erklärt. Es kommt selten vor, dass ein Mathematiker mit sechzig Jahren wesentlich mehr veröffentlicht als mit Dreißig. Etliche Jahre lief streng geheim ein Programm mit der *National Testing Station* durch die University of Idaho in Idaho Falls; er musste auch oft persönlich am Testgelände anwesen sein, was wohl nicht ganz ungefährlich war. Auch für die Air Force hat er gearbeitet. Von 1965 bis 1974 hatte er einen Forschungsauftrag der National Aeronautics and Space Administration. Viele dieser Arbeiten hatten mit der Mondlandung zu tun und später auch mit dem *Shuttle*. Auch da war des meiste classified. Drei seiner Doktoranden arbeiteten bei der NASA.

Seine mathematischen Interesssen spiegeln sich in seinen Veröffentlichungen:

Variationsrechnung, optimale Steuerungstheorie, Differentialgeometrie, Wahrscheinlichkeitsrechnung, Operations Research und (in den letzten Jahren) vor allem raumfüllende Kurven.

Nach seiner Emeritierung am 31. Dezember 1993 verbrachte er die Jahre abwechselnd mit Publizieren in geradzahligen Jahren und Vorlesungen in den Jahren dazwischen. 1994 wurde er in den Wissenschaftlichen Beirat der *Monatshefte für Mathematik* aufgenommen. 1995 hielt er als Gastprofessor der Universität Wien eine dreistündige Vorlesung über raumfüllende Kurven und ein zweistündiges Seminar über normale Zahlen und das Gesetz des iterierten Logarithmus. Dieses Seminar wurde auch in den folgenden Jahren fortgeführt, und er besuchte es auch jedes Jahr mindestens einmal.

1977 war er Gastprofessor an der Kansas State University, wo er einen eingeladenen Vortrag und eine Blockvorlesung über raumfüllende Kurven hielt.

Hans Sagan war regelmäßiger Gast in Wien, nicht nur wegen der Mathematik und der Familie. Er und seine Frau nützten die Zeit hier auch ausgiebig für Theater- und Konzertbesuche.

Im Privatissimum von E. Hlawka über *Neuere Arbeiten zur Geschichte der Mathematik* hat er regelmäßig seine neuesten Erkenntnisse zur Entwicklung der raumfüllenden Kurven vorgetragen und er hat auch am *V. Österreichischen Symposion zur Geschichte der Mathematik* im März 1999 in Neuhofen an der Ybbs teilgenommen und vorgetragen. Sein letzter Besuch in Österreich war im September 1999, wo er Hauptvortragender beim Österreichischen Mathematikertreffen in Graz war.

In seinem letzten Lebensjahr beschäftigte er sich mit der 2. Auflage seines Werkes über raumfüllende Kurven und einem Kommentar über Karl Mengers Beziehungen zur Variationsrechnung, der in den Selecta Mathematica von Menger erscheinen wird.

Hans Sagan ist am 4. April 2000 nach kurzer Krankheit, die einer Herzoperation folgte, gestorben.

Mit Hans Sagan haben wir einen österreichischen Mathematiker verloren, dessen Ruf und Werk sicher noch lange bestehen bleibt. Nicht nur seine einführenden und einen ausgezeichneten Überblick bietenden Bücher über Funktionalanalysis sichern ihm einen Platz in der Geschichte. Vor allem aber das Buch über raumfüllende Kurven, ein Gebiet, das ihn in seinem letzten Lebensjahrzehnt beschäftigte, wird sicher ein Klassiker. Er stellt darin nicht nur alle Ergebnisse in einheitlicher, übersichtlicher Weise dar, sondern gibt auch eine ausführliche historische Einleitung. Im Laufe der Studien zu diesem Werk ist es ihm gelungen, eine Reihe von Lücken der Theorie zu füllen und vielfach auch neue einfachere Beweise zu liefern. Seine Vorträge zu diesem Gebiet sind uns allen in unvergesslicher Erinnerung.

Durch den Tod von Hans Sagan hat die mathematische Welt einen originellen und vielseitigen Denker verloren, der die hervorragende Gabe hatte, komplizierte Sachverhalte klar und einleuchtend darzustellen. Eine ganz ungewöhnliche Anerkennung seiner Leistungen auf diesem Gebiet wurde ihm zuteil, als Dover Press in ihrer Reihe “Classics in Mathematics” neben den Werken von Euklid etc. auch zwei seiner Werke aufnahm.

Literatur

Bücher.

1. *Die Laplace-Transformation und ihre Anwendung,* mit Paul Funk und F. Selig, Deuticke, Wien, 1953 (106 S.).

2. *Boundary and Eigenvalue Problems in Mathematical Physics,* Wiley, New York, 1961 (381 S.). Neuauflage Dover, New York, 1989.

3. *Integral and Differential Calculus, An Intuitive Approach,* Wiley, 1962 (329 S.).

4. *Introduction to the Calculus of Variations,* McGraw Hill, New York, 1969. Neuauflage, Dover, 1992.

5. *Advanced Calculus of real-valued functions of a vector variable,* Houghton Mifflin Comp., Boston, 1974 (671 S.).

6. *Ten Easy Pieces,* Hayden, Rochelle Park, N.J., 1979 (gem.m. Carl Meyer). Übersetzung ins Japanische, Orion Press, Tokyo.

7. *Beat the Odds*, Hayden, 1980.

8. *Calculus, accompanied on the Apple*, Reston Publ.Co., Reston, Va. 1984.

9. *Space Filling Curves,* Springer Universitext, New York, 1994 (193 S.) , Übersetzung ins Japanische: Springer-Verlag Tokyo, 1998.

Zeitschriftenartikel.

1. *Some remarks on indirect methods in Laplace-transform,* Proc. of the Montana Acad. of Sciences, Vol 15, 1955.

2. *Über ein einer selbstadjungierten Differentialgleichung zuordenbares dreidimensionales Variationsproblem,* Österr. Ing.-Archiv 10 (1956), 264–267.

3. *Area and Integration, Riemann Integral*, in: Lectures on Calculus, Ed. by Kenneth O. May, Holden-Day, San Francisco, Cambridge, London, Amsterdam, 1967.

4. *Lagrange problems with a variable endpoint as optimal control problems*, North Carolina State University, NASA CR-837, 1967.

5. *Dynamic programming and Pontryagin's maximum principle,* North Carolina State University, NASA CR-838, 1967.

6. *Calculus of variations and optimal control theory,* J. Franklin Inst. 291 (1971), 305–313.

7. *Optimal control problems with a convex and compact control region*, Optim. Control Theor. Appl., Part II, Proc. 14th bienn. Sem. Can. math. Congr., Univ. West Ontario 1973, Lect. Notes Econ. math. Systems 106 (1974), 296–337.

8. *Optimal Control*, in: Handbook of Operations Research, Foundations and Fundamentals, Ed. by Joseph J. Moder and Salah E. Elmaghraby, Van Nostrand Reinhold Company, New York, 1978.

9. *Unscrambling a pseudo random integer sequence,* Zull. Number Theory Relat. Top. 5, Nr. 3 (1980), 1–16.

10. *Markov chains in Monte Carlo,* Math. Mag. 54 (1981), 3–10.

11. *Approximating polygons for Lebesgue's and Schoenberg space filling curves*, Am. Math. Mon. 93 (1986), 361–368.

12. *Kommentar über Radons Zeiträge zur Variationsrechnung,* in: J. Radon, Gesammelte Abhandlungen, Zirkhäuser, Zasel, 1987.

13. *A singular solution to Irrgangs problem,* in: Generalized functions and Convergence, Memorial Volume for Prof. Jan Mikusinski, Ed.: Piotr Antosik and Andrzej Kaminski, Katowice, World Scientific, Singapore, 1988.

14. *On pedestrians, city blocks and traffic lights,* J. Recreational Math. 21 (1989), 116–119.

15. *A singular solution to Irrgangs problem,* in: X. Congresse Zrasileiro de Engenharia Mecanica, Rio de Janeiro, 1989.

16. *On a quasi-regular Lagrange problem,* J. Math. Anal. Appl. 146 (1990), 397–407.

17. *Some reflections on the emergence of space-filling curves: The way it could have happened and should have happened, but did not happen,* J. Franklin Inst. 328 (1991), 419–430.

18. *Optimal allocation of storage space,* Eur. J. Oper. Res. 55 (1991), 82–90 (gem.m.John W. Zishir).

19. *On the geometrization of the Peano curve and the arithmetization of the Hilbert curve,* Int. J. Math. Educ. Sci. Technol. 23 (1992), 403–411.

20. *Approximating polygons for the Sierpinski-Knopp curve,* Zull. Pol. Acad. Sci., Math. 40 (1992), 19–29.

21. *Nowhere differentiability of Sierpinski's space-filling curve,* Zull. Pol. Acad. Sci., Math. 40 (1992), 217–220.

22. *An elementary proof that Schoenberg's space-filling curve is nowhere differentiable,* Math. Mag. 65 (1992), 125–128.

23. *Life on the number line,* Math. Mag. 65 (1992), 264. Autor: Leonard Gamma (as told to Hans Sagan).

24. *The coordinate functions of Sierpinski's space-filling curve are nowhere differentiable,* Zull. Pol. Acad. Sci., Math. 41 (1993), 73–75.

25. *A geometrization of Lebesgue's space-filling curve,* Math. Intell. 15 (1993), 37–43.

26. *A three-dimensional Hilbert curve,* Int. J. Math. Educ. Sci. Technol. 24 (1993), 541–545.

27. *An analytic proof of the nowhere differentiability of Hilbert's space-filling curve,* J. Franklin Inst. 330 (1993), 763–766.

28. *The taming of a monster: A parametrization of the von Koch curve,* Int. J. Math. Educ. Sci. Technol. 25 (1994), 869–877.

29. *Commentary on Hans Hahn's Contributions to the Theory of Curves,* in H. Hahn: Gesammelte Abhandlungen, Springer-Verlag, Wien, 1995.

30. *On the differentiability of the coordinate functions of Polya's space-filling curve,* Monatsh. Math. 121 (1996), 125–138 (gem.m. Karl Prachar).

31. *Nowhere differentiability of the coordinate functions of the von Koch curve,* Int. J. Math. Educ. Sci. Technol. 27 (1996), 146–148.

32. *Skating along the edge of reason,* Math. Japonica, 48 (1998), 311–321.

33. *On the nowhere differentiability of the coordinate functions of the Iseki curve,* Math. Mag. 71 (1998).

34. *Die Peano-Kurven von Schoenberg und Iseki: entdeckt oder erfunden?* in: V. Österreichisches Symposion zur Geschichte der Mathematik: Mathematik – entdeckt oder erfunden?, Hrgb. Ch. Zinder, Neuhofen a.d. Ybbs, 1999, 128–132.

Sonstiges.

35. *Über die wissenschaftliche Arbeit am mathematischen Institut der Universität Wien in den Jahren 1938 bis 1952*, in: Die Wiener Universität - Geschichte, Sendung und Zukunft, Herausgeber: Akademische Arbeitsgemeinschaft, Regina-Verlag, 1952 (gem. m. Karl Prachar).

Fotos aus dem Besitz von Christa Binder.

Internat. Math. Nachrichten
Nr. 186 (2001), 9–23

Primzahltests und Faktorisierungsalgorithmen I

Johann Wiesenbauer

Technische Universität Wien

1 Einleitung

Die im Titel angesprochene Thematik hat in den letzten Jahren durch verschiedene Anwendungen vor allem im Bereich der Kryptographie große Aktualität erlangt und steht heute im Mittelpunkt des Forschungsinteresses, wie die große Zahl an jährlich erscheinenden Publikationen dazu beweist. Gauß hätte jedenfalls daran seine Freude gehabt, schrieb er doch in seinen „Disquisitiones Arithmeticae“ (1801) die folgenden denkwürdigen Worte:

„Daß die Aufgabe, die Primzahlen von den zusammengesetzten zu unterscheiden und letztere in ihre Primfaktoren zu zerlegen, zu den wichtigsten und nützlichsten der gesamten Arithmetik gehört und die Bemühungen und den Scharfsinn sowohl der alten wie auch der neuen Geometer in Anspruch genommen hat, ist so bekannt, daß es überflüssig wäre, hierüber viele Worte zu verlieren. Trotzdem muß man gestehen, daß alle bisher angewendeten Methoden entweder auf spezielle Fälle beschränkt oder so mühsam und weitläufig sind, daß sie auf größere Zahlen meistenteils kaum angewendet werden können. Außerdem aber dürfte es die Würde der Wissenschaft erheischen, alle Hilfsmittel zur Lösung jenes berühmten Problem fleißig zu vervollkommnen.“

Tatsächlich sind die auf diesem Gebiet erzielten Ergebnisse heute auch unter volkswirtschaftlichen Gesichtspunkten von großer Bedeutung, hängt doch die Sicherheit einiger im Nachrichtenaustausch zwischen Banken und im Internet verwendeter Public-Key Kryptosysteme wie z.B. des RSA-Verfahrens (s. [6]) ganz entscheidend davon ab, dass etwa das Faktorisierungsproblem weiter „schwierig“ bleibt, was heute mit Sicherheit niemand garantieren kann (so wurden ja auch schon z.B. für sog. Quantencomputer, von denen man gegenwärtig allerdings noch

ISSN 0020-7926

nicht sagen kann, ob sie je realisierbar sein werden, Algorithmen zur Faktorisierung in Polynomialzeit entworfen, s. [7]).

Dies ist im übrigen auch ein besonders schönes Beispiel für den sog. „Erkenntnisvorlauf“ in der Mathematik. Damit ist der generelle Trend gemeint, dass mathematische Untersuchungen, die ursprünglich um ihrer selbst willen betrieben wurden irgendwann auch einmal für die Anwendungen relevant werden.

Nachfolgend wird nun versucht, einen kleinen Überblick über die seit Gauß (und z.T. auch schon vorher) erzielten Resultate zu dem angesprochenen Thema zu geben. Bei der Darstellung der Algorithmen werde ich dabei anstelle eines „Pseudo-Pascal“, wie es zu diesem Zweck oft verwendet wird, eine real existierende Programmiersprache, nämlich die des Computeralgebrasystems Derive 5, verwenden.[1]

In der ganzen Arbeit bezeichne N immer eine natürliche Zahl (manchmal mit Zusatzvoraussetzungen, wie z.B. $N > 1$ oder ungerade), die wir un der Regel zunächst einmal darauf testen, ob sie prim ist oder nicht, wobei sich im Falle der Zusammengesetztheit in natürlicher Weise die (i. allg. viel schwierigere Frage) nach einem nichttrivialen Teiler anschließt. Bevor irgendeines der nachfolgend beschriebenen Verfahren zur Anwendung kommt, wird man allerdings stets eine Probedivision durch alle Primteiler $p \leq B$ für eine gewisse Schranke B machen.[2]) Soweit dies notwendig ist, kann man also im folgenden stets voraussetzen, dass N keine „kleinen“ Primteiler mehr hat.

2 Der Fermat-Test

Als Einführung beginnen wir mit einem der wohl einfachsten und wichtigsten Primzahltests überhaupt, dem sog. Fermat-Test, an dessen Beispiel man auch gleich sehr schön einige allgemeine Gesichtspunkte aufzeigen kann. Als Folge des „Kleinen Fermatschen Satzes“ gilt bekanntlich, falls N eine Primzahl ist, für jede ganze Zahl a mit $0 < a < N$

$$a^{N-1} \equiv 1 \bmod N. \tag{1}$$

Beim Fermat-Test zur Basis a wird nun einfach für ein zufällig gewähltes a in obigem Bereich die Bedingung (1) überprüft. Ist sie nicht erfüllt, so ist N sicher

[1] Diese ist nämlich einerseits weitgehend selbsterklärend, da sie sich nur der einfachsten Programmkonstrukte bedient, andererseits gibt es auch die Möglichkeit, im Internet unter der Adresse *www.derive.com* eine sogenannte Demoversion von Derive 5 frei herunterzuladen, welche immerhin für 30 Tage voll lauffähig ist. In dieser Zeit besteht also dann in jedem Falle die Möglichkeit, die vorgestellten Programme selbst auszuprobieren und man kann insbesondere auch eventuell noch benötigte Erklärungen zur Programmsyntax in der Online-Hilfe dort selbst nachlesen.

[2] Für Derive etwa ist diese interne Schranke $B = 1021$.

zusammengesetzt! Leider gilt nicht auch die Umkehrung wie die folgende Rechnung mit Derive für $a = 2$ zeigt:

SELECT(MOD$(2^{n-1}, n) = 1$ AND NOT PRIME?(n), n, 3, 10000, 2)

[341, 561, 645, 1105, 1387, 1729, 1905, 2047, 2465, 2701, 2821,
3277, 4033, 4369, 4371, 4681, 5461, 6601, 7957, 8321, 8481, 8911]

Es gibt somit 22 sogenannte Pseudoprimzahlen zur Basis 2 unterhalb 10000, d.h. zusammengesetzte Zahlen, welche trotzdem den Fermat-Test bestehen. Dem stehen jedoch 9978 Zahlen unter 10000 gegenüber, für die der Fermat-Test das richtige Ergebnis geliefert hat. Die Aussage „N ist prim“ ist somit nach einem bestandenen Fermat-Test mit einer – wenn auch kleinen – Irrtumswahrscheinlichkeit behaftet, während die Aussage „N ist zusammengesetzt“ stets richtig ist. Primzahltests mit dieser Eigenschaft bezeichnet man daher auch oft als „probabilistische Primzahltests“ oder „Zusammengesetztheitstests“. Man könnte jetzt hoffen, obiges Ergebnis durch Wiederholung des Fermat-Tests mit anderen Basen entscheidend zu verbessern, z.B. für $a = 3$:

SELECT(MOD$(2^{n-1}, n) = 1$ AND MOD$(3^{n-1}, n) = 1$
AND NOT PRIME?(n), n, 3, 10000, 2)

[1105, 1729, 2465, 2701, 2821, 6601, 8911]

Dieses doch sehr enttäuschende Ergebnis – fast $1/3$ aller obigen Zahlen werden noch immer nicht als zusammengesetzt erkannt – läßt sich auf das Phänomen zurückführen, dass es zusammengesetzte natürliche Zahlen N gibt (sogar unendlich viele, wie in [1] gezeigt wurde!), welche den Fermat-Test für alle Basen a im Bereich $0 < a < N$ bestehen, die zu N teilerfremd sind! (Die Bedingung der Teilerfremdheit zu N ist dabei klarerweise notwendig, da sie aus (1) folgt.)

Diese Zahlen N, welche nach ihrem Entdecker Carmichael-Zahlen genannt werden, können auch als zusammengesetzte und quadratfreie natürliche Zahlen charakterisiert werden, welche überdies die Bedingung $p - 1 | N - 1$ für jeden Primteiler p von N erfüllen. Sie müssen, wie man daraus leicht folgert, jedenfalls ungerade sein und mindestens 3 Primfaktoren haben (s. [3]). Hier ist eine mit Derive erstellte Liste aller Carmichael-Zahlen bis 100000:

```
Carmichael?(n) :=
    Prog
        If PRIME?(n) AND (n − 1) MOD (n, 2) = 0
            RETURN false
        If SOME(e_ > 1, e_, (FACTORS(n)) COL 2)
            RETURN false
        EVERY(MOD(n − 1, p_ − 1) = 0, p_, (FACTORS(n)) COL 1)
```

SELECT(Carmichael?(n), n, 1, 100000, 2)

[561, 1105, 1729, 2465, 2821, 6601, 8911, 10585, 15841, 29341, 41041, 46657, 52633, 62745, 63973, 75361]

Es stellt sich damit insbesondere heraus, dass nach den zwei Fermat-Tests zu den Basen 2 bzw. 3 von den 7 „durchgerutschten“ Zahlen 6 Carmichaelzahlen waren! Diese werden aber auch bei Wiederholung des Fermat-Tests mit anderen Basen nur in dem (für ein N ohne kleine Primfaktoren sehr unwahrscheinlichen!) Fall ausgeschieden, dass die gewählte Basis zu N nicht teilerfremd ist (wie in unserem Beispiel 561 für $a = 3$).

3 Der Solovay-Strassen-Test

Eine mögliche Verbesserung des Fermat-Tests besteht nun darin, dass man für ein ungerades N und ein ganzes a mit $0 < a < N$ die nachfolgende Bedingung

$$a^{(N-1)/2} \equiv (a/N) \bmod N \tag{2}$$

heranzieht,[3] die jedenfalls nach dem sogenannten Eulerschen Kriterium gelten muss, wenn N prim ist. Da die Gültigkeit von (2) die Gültigkeit von (1) impliziert, ist der daraus resultierende Test, welcher nach seinen Erfindern auch Solovay-Strassen-Test genannt wird, mindestens so stark wie der Fermat-Test. Wie man zeigen kann, ist nun für ein zusammengesetztes N die Anzahl der Basen a mit $0 < a < N$, für welche N den Test besteht, höchstens $\varphi(N)/2$, was jedenfalls eine starke Verbesserung gegenüber dem Fermat-Test darstellt, wo die entsprechende Anzahl für Carmichaelzahlen ja sogar $\varphi(N)$ betrug. Insbesondere hat man damit bei zusammengesetztem N und zufälliger Wahl von a eine mehr als 50% Chance, einen „Zeugen“ für die Zusammengesetztheit von N zu finden. Durch eine k-malige Wiederholung des Solovay-Strassen-Tests ist dann die Irrtumswahrscheinlichkeit für die Aussage „N ist prim“ $< 1/2^k$, also bei genügend großem k, beliebig klein (dies trifft im übrigen in gleicher Weise auch für den Fermat-Test zu, außer eben in dem Fall, dass N eine Carmichaelzahl ist).

Auch die nachfolgende Derive-Demonstration stellt die deutlich höhere Leistungsfähigkeit des Solovay-Strassen-Tests unter Beweis:

SELECT(MOD($2^{n-1}, n$) = JACOBI$(2, n)$ AND
NOT PRIME?(n), n, 1, 10000, 2)

[3] Das Symbol (a/N) bezeichnet dabei das Jacobi-Symbol aus der Theorie der quadratischen Reste.

[561, 1105, 1729, 1905, 2047, 2465, 4033, 4369, 4681, 6601, 8321, 8481, 8911]

SELECT(MOD($3^{n-1}, n$) = JACOBI$(3, n)$, n, [561, 1105, 1729, 1905, 2047, 2465, 4033, 4369, 4681, 6601, 8321, 8481, 8911])

[1105, 1729, 6601]

4 Der Rabin-Miller-Test

Es ist möglich, den Solovay-Strassen-Test noch entscheidend zu verbessern. Man benutzt dazu die einfache Tatsache, dass unter der Voraussetzung der Gültigkeit einer Gleichung

$$a^m \equiv 1 \bmod N \tag{3}$$

für ein gerades $m > 0$, wobei man $m = N - 1$ als ersten Wert für m nehmen kann, jedenfalls $a^{m/2}$ Lösung der Kongruenz

$$x^2 \equiv 1 \bmod N \tag{4}$$

ist. Ist aber N eine Primzahl, so hat (4) nur die Lösungen $\pm 1 \bmod N$, weshalb also

$$a^{m/2} \equiv \pm 1 \bmod N \tag{5}$$

gelten muss. Ist dies nicht erfüllt, so ist daher N sicher zusammengesetzt. Gilt andernfalls in (5) das Vorzeichen + und ist auch noch $m/2$ gerade, so muss in gleicher Weise

$$a^{m/4} \equiv \pm 1 \bmod N \tag{6}$$

gelten usw. Indem man in dieser Weise fortfährt, muss man für ein primes N entweder einmal auf den Wert $-1 \bmod N$ kommen, oder es ist der Wert der a-Potenz zwar $+1 \bmod N$, aber der momentane Exponent ungerade. Trifft beides beim Abbruch des Verfahrens nicht zu, so ist N sicher zusammengesetzt, andernfalls wird es als prim angenommen. Nachfolgend führen wir dieses Verfahren am Beispiel $N = 1729 = 7 \cdot 13 \cdot 19$ für $a = 2$ durch, wobei wegen $N - 1 = 1728 = 2^6 \cdot 27$ maximal 6 Schritte erforderlich sind:

$\text{MODS}(2^{1728/2}, 1729) = 1$
$\text{MODS}(2^{1728/2^2}, 1729) = 1$
$\text{MODS}(2^{1728/2^3}, 1729) = 1$
$\text{MODS}(2^{1728/2^4}, 1729) = 1$
$\text{MODS}(2^{1728/2^5}, 1729) = -664$

Bei der praktischen Durchführung dieses Tests, welcher Rabin-Miller-Test genannt wird, beginnt man allerdings, wenn $N-1$ die Darstellung $N-1=s2^t$ besitzt, mit der Berechnung von $a^s \bmod N$. Ist dieser Wert bereits $\pm 1 \bmod N$, so wurde der Test bestanden, ansonsten muss man durch höchstens $(t-1)$-maliges Quadrieren einmal auf den Wert -1 kommen. In unserem Beispiel sieht der Anfang dieser Sequenz so aus:

$$\text{MODS}(2^{27},1729) = 645$$
$$\text{MODS}(645^2,1729) = -664$$
$$\text{MODS}((-664)^2,1729) = 1$$

wobei wir hier schon sehen, dass der Wert -1 beim weiteren Quadrieren nicht mehr angenommen wird, d.h. 1729 hat den Test wie vorher nicht bestanden.

Nachfolgend ist wieder ein Derive-Programm angegeben, welches die algorithmische Durchführung des Rabin-Miller-Tests für eine ungerade natürliche Zahl $N > 1$ bezüglich einer Basis a mit $0 < a < N$ illustrieren soll.

```
RABIN_MILLER(n,a,s_) :=
    Prog
        s_ := n - 1
        Loop
            s_ : /2
            If ODD?(s_) exit
        a := - ABS(MODS(a^s_,n))
        Loop
            If a = -1 exit
            s_ : *2
            If s_ = n - 1
                RETURN false
            a := MODS(a^2,n)

SELECT(RABIN_MILLER (n,2) AND NOT PRIME?(n), n, 3,
          10000, 2)

[2047, 3277, 4033, 4681, 8321]
```

Aber auch Zahlen mit mehreren hundert Stellen können damit noch schnell und effizient auf Primalität getestet werden. In dem in der Einleitung angesprochenen RSA-Verfahren werden z.B. große Primzahlen benötigt, wobei „groß“ nach heutigen Sicherheitsstandards bedeutet, dass sie in Binärschreibweise mindestens 512 Bits (dezimal sind das etwa 155 Stellen) haben sollen. Die Bereitstellung solcher Primzahlen kann auch mit einem Computeralgebrasystem wie Derive auf einem modernen PC so wie in nachfolgendem Beispiel in typischerweise wenigen Sekunden erfolgen.

(p := NEXT_PRIME(RANDOM(2^{512}))) =
13005885656328892692970275156606507898928566565138194948687197238364294082315116472709795614423527065090746557949297489315097564228414310899308127100680399
(1.25s)

RABIN_MILLER(p, 2) = true (0.02s)[4]

In diesem Zusammenhang stellt sich natürlich auch die Frage nach der Sicherheit von Rabin-Miller-Tests. Es gilt hier nach einem berühmten Satz von Rabin und Monier, dass für ein zusammengesetztes ungerades $N \neq 9$ für höchstens $\varphi(N)/4$ aller Basen a mit $0 < a < N$ der Rabin-Miller-Test erfüllt wird, was gegenüber dem Solovay-Strassen-Test also nochmals eine Halbierung bedeutet. Insbesondere kann durch eine k-fache Wiederholung des Tests mit zufällig gewählten Basen a in dem Bereich $0 < a < N$ die Irrtumswahrscheinlichkeit für die Aussage „N ist prim“ sogar kleiner als $1/4^k$ und damit für genügend großes k wieder beliebig klein gemacht werden.

Rabin-Miller-Tests bilden die Grundlage von Primzahltests in den meisten Computeralgebrasystemen, so auch in Derive. Vor Version 5 von Derive wurden dabei – abgesehen von einer Überprüfung auf kleine Primteiler – nur standardmäßig 6 Rabin-Miller-Tests durchgeführt, was jedoch problematisch ist, da es für jede endliche Menge S von positiven ganzen Zahlen stets unendlich viele zusammengesetzte N gibt, welche den Rabin-Miller-Test für alle Basen a in S passieren. Ist S etwa die Menge aller Primzahlen ≤ 31, so gilt z.B.

N := 1195068768795265792518361315725116351898245581

VECTOR(RABIN_MILLER(N, a), a, [2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31])
[true, true, true, true, true, true, true, true, true, true, true]

RABIN_MILLER(N, 37) = false

Wenn man sich also nur auf Rabin-Miller-Tests für eine gewisse Anzahl von Basen beschränkt, ist es relativ einfach, Zahlen zu konstruieren, welche zusammengesetzt sind, aber den Primalitätstest passieren, wie dies in älteren Versionen von Maple und Derive tatsächlich der Fall war (noch in Derive 4.11 wurde z.B. $N = 22564845703 = 106219 \cdot 212437$ fälschlich für eine Primzahl gehalten).

[4] Die hier und im folgenden angegebenen Rechenzeiten wurden auf einem Pentium 450 MHz PC erzielt.

5 Primzahltests basierend auf Lucas-Folgen

In der Praxis werden daher oft Rabin-Miller-Tests noch mit anderen Primalitätstests kombiniert, wobei sich in diesem Zusammenhang Tests, welche auf gewissen Eigenschaften von sog. Lucas-Folgen beruhen, als besonders wirkungsvoll erwiesen haben. Lucas-Folgen (L_n) sind dabei allgemein definiert durch eine lineare Rekursion 2. Ordnung

$$L_n = PL_{n-1} - QL_{n-2} \tag{7}$$

mit gewissen ganzen Zahlen P und Q, sodass $D = P^2 - 4Q^2 \neq 0$. Außer durch die Wahl von P und Q unterscheiden sie sich noch durch die Wahl der ganzzahligen Startwerte L_0 und L_1. Besonders wichtig sind dabei die Lucasfolgen, welche man für $L_0 = 0, L_1 = 1$ bzw. $L_0 = 2, L_1 = P$, erhält, welche gewöhnlich mit (U_n) bzw. (V_n)) bezeichnet werden. Mit Hilfe der weiteren Rekursionsbeziehungen

$$U_{2n} = U_n V_n, \quad U_{2n+1} = U_{n+1}V_n - Q^n \tag{8}$$

bzw.

$$V_{2n} = V_n^2 - 2Q^n, \quad V_{2n+1} = V_{n+1}V_n - PQ^n \tag{9}$$

ist eine sehr effiziente Berechnung der Folgenglieder auch für große Indices möglich.

Für diese U- bzw. V-Folgen gelten nun eine Fülle an Eigenschaften, welche man für Primalitätstests heranziehen kann. Unter der Voraussetzung, dass N eine ungerade Primzahl mit $(N, QD) = 1$ ist, muss beispielsweise für die U-Folge gelten

$$U_{N-(D/N)} \equiv 0 \bmod N, \tag{10}$$

d.h. $N|U_{N-1}$ für $(D/N) = 1$ und $N|U_{N+1}$ für $(D/N) = -1$. Dies läßt sich unter Ausnutzung von (8) und unter Verwendung einer Darstellung $N = s2^t + (D/N)$ mit ungeradem s auch so ausdrücken, dass wenigstens eine der Zahlen

$$U_s, V_s, V_{2s}, V_{4s}, \ldots, V_{2^{t-1}s} \tag{11}$$

durch N teilbar sein muss. Ferner muss gelten

$$U_N \equiv (D/N) \bmod N, \tag{12}$$

d.h. $N|U_N - 1$ für $(D/N) = 1$ und $N|U_N + 1$ für $(D/N) = -1$.

Noch beliebter als Primzahltests sind Bedingungen für die V-Folge, da sich diese allein unter Verwendung von (9) noch etwas einfacher berechnen läßt. So muss unter denselben Voraussetzungen etwa gelten

$$V_N \equiv P \bmod N, \tag{13}$$

sowie

$$V_{N-(D/N)} \equiv 2Q^{(1-(D/N))/2} \bmod N, \tag{14}$$

d.h. $V_{N-1} \equiv 2 \bmod N$ für $(D/N) = 1$ und $V_{N+1} \equiv 2Q \bmod N$ für $(D/N) = -1$. Ähnlich wie oben für die U-Folge, läßt sich auch (14) noch weiter verschärfen (siehe dazu etwa [5]).

Im Hinblick auf eine Kombination mit Rabin-Miller-Tests ist es dabei günstig, P und Q so zu wählen, dass gilt $(D/N) = -1$. Dazu nimmt man am besten für D die erste Zahl der Folge 5,9,13,17,21, ... mit $(D/N) = -1$ und für P die nächstgrößere ungerade ganze Zahl zu $\sqrt{D}$, womit sich dann Q automatisch zu $(P^2 - D)/4$ ergibt.

Als Beispiel wollen wir die oben betrachtete 155-stellige Zahl p, welche bisher alle Primalitätstests bestanden hat, mit Hilfe der obigen Bedingungen weiter testen. Dazu wählen wir nach dem zuvor Bemerkten $D = 21$, wegen

VECTOR(JACOBI(d, p), d, [5, 9, 13, 17, 21]) = [1, 1, 1, 1, -1],

womit sich $P = 5$ und $Q = 1$ ergibt. Tatsächlich gilt nun unter Verwendung der Funktionen U_MOD(·) und V_MOD(·) aus der Programmbibliothek

U_MOD($p+1, 5, 1, p$) = 0
U_MOD($(p+1)/2^4, 5, 1, p$) = 0
U_MOD($p, 5, 1, p$) - p = -1
V_MOD($p, 5, 1, p$) = 5
V_MOD($p+1, 5, 1, p$) = 2,

womit obiges p auch diese weiteren Tests alle bestanden hat (in insgesamt weniger als 1s auf meinem PC!).

6 Eine „Umkehrung“ des „kleinen Fermatschen Satzes“

Für die im letzten Kapitel vorgestellte Kombination aus Rabin-Miller-Tests und auf Lucasfolgen basierenden Primzahltests, wie sie z.B. in Mathematica und auch Derive verwendet werden, wurden bis heute keine zusammengesetzten Zahlen gefunden, welche sie passieren, obwohl wenig Zweifel daran besteht, dass es sie gibt. Für viele praktische Anwendungen mag daher das Bestehen dieser Tests als „Beweis“ für die Primalität bereits ausreichen, den Ansprüchen der Mathematik genügt das natürlich noch nicht.

Solche streng deterministische Primzahltests gibt es natürlich auch, wenngleich sie für Zahlen vergleichbarer Größe i. allg. bereits deutlich aufwendiger sind.

Wir benötigen dazu Sätze, welche hinreichende Bedingungen für die Primalität von N angeben, die so wie bisher leicht überprüfbar sein sollten. Wie schon im letzten Kapitel ist dabei wieder der „Kleine Fermatsche Satz“ der Ausgangspunkt unserer Überlegungen. Ist nämlich N eine Primzahl, so gilt nicht nur

$$a^{N-1} \equiv 1 \bmod N \tag{15}$$

für alle a mit $0 < a < N$, sondern für spezielle a aus diesem Bereich ist darüberhinaus $k = N-1$ die kleinste positive ganze Zahl mit $a^k \equiv 1 \bmod N$, d.h. für diese a ist $N-1$ ihre Ordnung $\bmod N$, i.Z.

$$\mathrm{ord}_N(a) = N-1. \tag{16}$$

Hat man umgekehrt ein a gefunden, für das (16) gilt, so folgt aus $\mathrm{ord}_N(a) | \varphi(N)$ sofort $\varphi(N) = N-1$, was natürlich nur gelten kann, wenn N prim ist. Für (16) muss aber nun außer (15) auch noch die Gültigkeit von

$$a^{(N-1)/q} \not\equiv 1 \bmod N \tag{17}$$

für jeden Primfaktor q von $N-1$ überprüft werden. Diese in der vorliegenden Form von D.H. Lehmer stammende hinreichende Bedingung für die Primalität konnte später von J.L. Selfridge noch soweit abgeschwächt werden, dass die Zahl a in (15) und (17) nicht für jeden Primfaktor q dieselbe sein muss, sondern von q abhängen darf.

Der Haken an der Sache ist aber, dass man dazu die Primfaktoren von $N-1$ kennen muss, sodass dieser deterministische Primzahltest im allgemeinen nur für relative kleine N in Frage kommt. Eine Ausnahme bilden dabei Zahlen von einer besonderen Form, für die man die Primfaktorzerlegung von $N-1$ von vorherein kennt, etwa wenn N die Gestalt $N = n! + 1$ für eine natürliche Zahl n hat.

Nachfolgend wollen wir z.B. für die 106-stellige Zahl $N = 73! + 1$ einen strengen Primzahltest auf der Grundlage obiger Überlegungen durchführen. Zunächst stellen wir dazu fest, dass N die Bedingung (15), d.h. den Fermat-Test für alle Basen $a = 1, 2, \ldots, 100$ erfüllt, also mit großer Wahrscheinlichkeit eine Primzahl ist.

$N := 73! + 1$
SELECT(MOD(a^{N-1}, N) $\neq 1$, a, 1, 100) = []

Für alle Primfaktoren q von $N-1$, d.h. für alle Primzahlen ≤ 73, versuchen wir dann jeweils ein $a \leq 100$ zu finden, welches die weitere Bedingung (17) erfüllt. Für $q = 2$ sind dabei nur 4 Basen a geeignet, nämlich 79, 83, 89, 97

SELECT(MOD($a^{(N-1)/2}, N$) 1, a, 1, 100) = [79, 83, 89, 97]

Keine dieser 4 Basen deckt auch alle anderen Primfaktoren q von $N-1$ ab, wie die folgende Rechnung zeigt:

S := SELECT(PRIME?(p), p, 1, 73)
[2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73]

SELECT(MOD($79^{(N-1)/q}$,N) = 1, q, S) = [53]
SELECT(MOD($83^{(N-1)/q}$,N) = 1, q, S) = [13, 19]
SELECT(MOD($89^{(N-1)/q}$,N) = 1, q, S) = [3, 7, 37]
SELECT(MOD($97^{(N-1)/q}$,N) = 1, q, S) = [3, 47]

Nach Selfridge ist das aber auch gar nicht notwendig: Wir können z.B. die beiden Basen $a = 79, 83$ gemeinsam nehmen, welche dann zusammen alle Fälle in (17) abdecken und somit einen Beweis für die Primalität von N ergeben.

7 Fermatsche Primzahlen

Einen wichtigen Spezialfall, auf den obiger Primzahltest anwendbar ist, betreffeb die sog. Fermatschen Zahlen $F_n = 2^{2^n} + 1 \ (n \geq 0)$. Nehmen wir zunächst an, F_n ist prim für ein $n \geq 0$. Es muss dann speziell für $a = 3$ den Solovay-Strassen-Test erfüllen, also

$$3^{(F_n-1)/2} \equiv (3/F_n) \bmod F_n. \tag{18}$$

Da aber nun, wie man mit Sätzen aus der Theorie der quadratischen Reste leicht zeigen kann, 3 quadratischer Nichtrest ist für $F_n \ (n \geq 1)$, muss weiter gelten

$$3^{(F_n-1)/2} \equiv -1 \bmod F_n. \tag{19}$$

Dies ist somit eine notwendige Bedingung für die Primalität von F_n für $n \geq 1$. Sie ist aber umgekehrt auch hinreichend, denn $q = 2$ ist ja der einzige Primfaktor von $F_n - 1$ und als Folge von (19) ist dann (15) und (17) mit $a = 3$ erfüllt!

Der Solovay-Strassen-Test (und damit auch der, wie man zeigen kann, stets mindestens gleichstarke Rabin-Miller-Test) für die Basis $a = 3$ ist also für Fermatzahlen F_n mit $n \geq 1$ ein Primzahlkriterium, welches in der Literatur nach seinem Entdecker auch als Satz von Pépin bezeichnet wird.

Obwohl Fermat aufgrund der Tatsache, dass für $n = 0, 1, 2, 3, 4$ prim ist, sich bekanntlich zu dem voreiligen Schluss verleiten ließ, dass dies für alle n so wäre, kennt man bis heute keine weiteren Fermatprimzahlen ($n = 31$ ist übrigens zur Zeit der kleinste Wert, wo es noch unentschieden ist).

Nachfolgend wieder ein kleines Derive-Programm zur Illustration (die tatsächliche Implementierung des Pépin-Tests macht jedoch von der Fast Fourier Transform zur Multiplikation großer Zahlen sowie einer Rückführung der Reduktion $bmodF_n$ auf Schiebeoperationen und Subtraktionen auf Binärebene unter Verwendung von

$$A2^{2^n} + B \equiv A(2^{2^n} + 1) + (B - A) \equiv (B - A) \bmod F_n \tag{20}$$

Gebrauch).

```
PEPIN(n, f_) :=
    Prog
        If n = 0
            RETURN true
        f_ := 2^(2^n) + 1
        SOLVE(MODS(3^((f_-1)/2), f_) = -1)

VECTOR(PEPIN(n), n, 0, 12)
[true, true, true, true, true, false, false, false, false, false, false, false,
false]   (8.29s)
```

8 Mersennesche Primzahlen

In völlig analoger Weise, wie man unter Kenntnis der Primfaktoren von $N-1$ gewissermaßen eine „Umkehrung“ des „Kleinen Fermatschen Satzes“ gewinnen kann, gelingt dies auch, wenn man die Primfaktoren von $N+1$ kennt, für gewisse Sätze über Lucas-Folgen. Wir haben z.B. im 1. Abschnitt u.a. festgestellt, dass für eine ungerade Primzahl N mit $(N,QD)=1$ und $(D/N)=-1$

$$U_{N+1} \equiv 0 \bmod N \tag{21}$$

gelten muss. Kann man nun darüberhinaus die U-Folge (bzw. deren Parameter P und Q) so wählen, dass auch gilt

$$(U_{(N+1)/q}, N) = 1 \tag{22}$$

für alle Primteiler q von $N+1$, so ist N umgekehrt prim.

Speziell für Mersennesche Zahlen $M_p = 2^p - 1$, wo p eine Primzahl ist, läßt sich unter den gleichen Voraussetzungen wie oben daraus die einfachere hinreichende Bedingung

$$V_{2^{p-2}} \equiv 0 \bmod M_p \tag{23}$$

gewinnen (s. [4]). Definiert man nun für $P=4$, $Q=1$ die Folge (s_n) durch

$$s_n = V_{2^{n-1}}, \quad n = 1,2,\ldots, \tag{24}$$

so lässt sich diese Hilfe der ersten Bedingung in (9) auch rekursiv durch

$$s_1 = 4, \quad s_{n+1} = s_n^2 - 2 \tag{25}$$

definieren und (22) wird dann zur einfacheren Bedingung

$$s_{p-1} \equiv 0 \bmod M_p, \tag{26}$$

wobei wir hier $p \neq 2$ voraussetzen müssen, damit $(M_p, QD) = (M_p, 12) = 1$ ist. Umgekehrt kann man zeigen, dass (26) auch notwendig für die Primalität von M_p für $p \neq 2$ ist. Dieses überaus einfache Primzahlkriterium für Mersennesche Zahlen ist in der Literatur auch als Lucas-Lehmer-Test bekannt, da eine Vorversion davon von E. Lucas um 1870 gefunden und dann von D.H. Lehmer um 1930 auf die obige Form gebracht wurde. Mit seiner Hilfe konnten bisher 38 Mersennesche Primzahlen gefunden werden, deren größte zur Zeit

$$M_{6972593} = 2^{6972593} - 1 \tag{27}$$

mit 2098960 Stellen ist (s. *http://www.mersenne.org/prime.htm* bezüglich Einzelheiten der Entdeckung im Rahmen des sogenannten GIMPS-Projekts). Übrigens war der Electronic Frontier Foundation die Entdeckung dieser ersten Primzahl mit mehr als einer Million Stellen 50.000 $ wert und ein Preis von 100.000 $ wurde für die erste Primzahl mit mindestens 10 Millionen Stellen ausgesetzt (s. *http://www.eff.org/*), sodass man mit der Primzahlsuche neuerdings auch viel Geld machen kann.

Mit dem nachfogenden Derive-Programm können demgegenüber aus Zeit- und Speichergründen Mersennesche Zahlen mit höchstens einigen zehntausend Stellen auf Primalität getestet werden, doch für Mersennesche Zahlen mit „nur“ mehreren tausend Stellen noch beeindruckend schnell, wie das angegebene Beispiel zeigt.

```
LUCAS_LEHMER(p, m_) :=
    Prog
        m_ := 2^p − 1
        SOLVE(ITERATE(MOD(s_^2 − 2, m_), s_, 4, p − 2) = 0)

LUCAS_LEHMER(9689) = true  (66.5s)
```

Wiederum ist es so, dass in der Praxis für die Berechnung der Folgenglieder s_n die Fast Fourier Transform verwendet wird, wobei für die laufende Reduktion $\bmod M_p$ wegen

$$A2^p + B \equiv A(2^p - 1) + (B + A) \equiv (B + A) \bmod M_p \tag{28}$$

wieder eine Rückführung auf binäre Schiebeoperationen und Additionen möglich ist. Tatsächlich sind die dazu verwendeten Programme (natürlich auf Maschinensprachebene!) so aufwendig, dass sie sogar dazu verwendet werden, um Pentium-III-Chips vor ihrer Auslieferung nochmals gründlich „durchzuchecken“ (übrigens wurde ja auch der inzwischen schon legendäre „Pentium-Bug“ bei einem Vorgängerchip im Rahmen von ähnlichen Berechnungen im Bereich der Zahlentheorie gefunden!)

9 Deterministische Primzahltests für Zahlen allgemeiner Form

Welche deterministischen Primzahltests gibt es nun für große Zahlen N allgemeiner Form, für welche also die Primfaktoren von $N-1$ bzw. $N+1$ nicht mehr so ohne weiteres angegeben werden können?

Zunächst einmal wäre hier zu erwähnen, dass es unter der Annahme der Richtigkeit der sog. Verallgemeinerten Riemannschen Vermutung für eine zusammengesetzte Zahl N stets eine Basis a mit $0 < a < 2(\log N)^2$ gibt, für die der Rabin-Miller-Test nicht bestanden wird. Da der Rechenaufwand für einen einzelnen Rabin-Miller-Test für N mit $O((\log N)^3)$ veranschlagt werden kann, ergibt sich somit ein Gesamtrechenaufwand bei Überprüfung aller dieser Basen von $O((\log N)^5)$, d.h. es liegt dann ein Polynomialzeitalgorithmus vor. Dieses Resultat, welches sich ohnehin auf eine unbewiesene Vermutung stützt, ist aber nur von allgemeinem Interesse, da man heute viel bessere deterministische Primzahltests kennt.

Ein solcher ist z.B. der sogenannte APRCL-Test (nach L. Adleman und R. Rumely, welche den Test 1980 erfunden, und C. Pomerance, H. Cohen und H.W. Lenstra, die ihn in den Folgejahren entscheidend verbessert haben). Dieser Test hat eine Komplexität von $O((\log N)^{c \log\log\log N})$ für eine reelle Konstante $c > 0$, d.h. es handelt sich dabei, da der iterierte Logarithmus $\log\log\log N$ nur sehr langsam mit N wächst, gewissermaßen „fast“ um einen Polynomialzeitalgorithmus. Da er jedoch verhältnismäßig tiefliegende Resultate aus der algebraischen Zahlentheorie verwendet, verzichte ich hier auf eine ausführliche Darstellung, dies nicht zuletzt auch deshalb, weil er heute weitgehend durch praktikablere Tests ersetzt wurde, welche sich Sätze aus der Theorie der elliptischen Kurven zunutze machen.

Was die Details dieser in der Grundversion auf Goldwasser und Kilian zurückgehenden und später von Atkin umd Morain noch entscheidend verbesserten Tests betrifft, mit dem heute problemlos für Zahlen mit mehreren hundert Stellen[5] streng deterministisch die Primzahleigenschaft nachgewiesen werden kann, so werden diese im 2. Teil dieser Arbeit in einem eigenen Kapitel über elliptischen Kurven nachgetragen. Der Rechenaufwand beträgt dabei in den besten Varianten $O((\log N)^6)$, wobei es sich hier allerdings nur um einen Erwartungswert handelt, der in Einzelfällen überschritten werden kann. Trotzdem darf zumindestens der erste Teil der in der Einleitung von Gauß vorgegebenen Problemstellung als befriedigend gelöst betrachtet werden!

[5] Den Rekord in dieser Hinsicht hält zur Zeit die 3106-stellige Zahl $(348^{1223}-1)/347$, deren Primalität in 50 Tagen Rechenzeit auf einem Pentium 800 PC nachgewiesen wurde (s. *http://www.znz.freesurf.fr/pages/titanixrecord.html*).

Literatur

1. W.R. Alford, A. Granville, C. Pomerance, *There are infinitely many Carmichael Numbers*, Annals of Math. 140 (1994), 703–722.

2. R. Crandall, *Topics in Advanced Scientific Computation, TELOS-Reihe*, Springer, New York, 1996.

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. S. Wagon, *Mathematica in Action*, 2nd ed., TELOS-Reihe, Springer, 1998.

6. J. Wiesenbauer, *Public Key Kryptosysteme in Theorie und Programmierung*, Didaktikhefte der ÖMG, Heft 30 (1999), 144–159.

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

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, welche Primzahltests und Faktorisierungsalgorithmen von ganzen Zahlen betreffen, beteiligt.

Internat. Math. Nachrichten
Nr. 186 (2001), 25–34

Interview with Jean Pierre Bourguignon*

F. J. Craveiro de Carvalho, Jorge Picado

Departamento de Matemática – Universidade de Coimbra, Portugal

Jean-Pierre Bourguignon was a student at *l' Ècole Polytechnique* in Paris. He went on to become *Docteurès Sciences Mathématiques* in 1974 having written a thesis under the supervision of Marcel Berger.

Professor Bourguignon was President of the European Mathematical Society from 1995 to 1998 and since 1994 he is the Director of IHÉS - *Institut des Hautes Études Scientifiques* in Bures-sur-Yvette, near Paris.

*Nachdruck aus: A jar in Tennessee, F. J. Craveiro de Carvalho and Jorge Picado (eds), Departamento de Matemática – Universidade de Coimbra, Portugal, p. 35–49, mit freundlicher Genehmigung von F. J. Craveiro de Carvalho.

ISSN 0020-7926

Professor Bourguignon is also the mathematical author or co-author of the videos *Tambour, que dis-tu?,* which was awarded a prize at the Palaiseau International Science Film Festival in 1987, and *The New Shepherd's Lamp*. That very year he was awarded the *Prix Paul Langevin de l'Académie des Sciences de Paris* and in 1997 he received the *Prix du rayonnement français pour les sciences mathématiques et physiques*.

I am not familiar with the school system in France but from your CV it seems that your first degree was an Engineering one granted by l'École Polytechnique.

Is that so ? What made you change your mind and realize that you wanted to be a mathematician ? An influential teacher ?

The higher education system in France is peculiar. It is split between on the one hand *Grandes Écoles* and the so-called *Classes Préparatoires* leading to them, and Universities on the other hand. Most of the *Grandes Écoles* are engineering schools, with the notable exception of the *Écoles Normales Supérieures*. The *École Polytechnique* was created right after the French Revolution to give engineers some time before studying technical subjects to get a more basic training in fundamental sciences. The school has kept this theoretical bias, and at my time its curriculum offered a substantial exposure to mathematics. Being a student at *l'École Polytechnique* was for me a formidable opportunity to meet some exceptional mathematicians : Gustave Choquet, who was my Analysis teacher there, and Laurent Schwartz, with whom I extensively discussed the curriculum reform.

I date my definite attraction to mathematics from the time I was preparing the baccalauréat. The math teacher I had then suffered a poor reputation from the

point of view of pedagogy but for the first time in my life I was confronted with a real (mathematical) challenge. I should probably say that in my high school years I had the great fortune of having the same (excellent) math teacher for four years out of six. He was very strict and thorough and had the great inspiration of using quicker students to help slower ones. At no moment though, did he trigger in me the desire of becoming a mathematician, or even a scientist. At that time I was much more attracted by humanities, or even foreign languages. From this experience I would be tempted to draw the lesson that it is very important to offer real challenges to young students. A uniform and smooth curriculum is not likely to be what will turn young minds on.

You belong to the Class of 66 at l'École Polytechnique. In the middle of your degree you were caught by the May 68 events. Laurent Schwartz in his „Un mathématicien aux prises avec le siècle" refers to you in a very nice way. Let me quote partially

> *„Deux élèves de la promotion 66, Jean-Pierre Bourguignon et Yves Bamberger, jouèrent, par les initiatives comme par les contacts qu'ils établirent entre enseignants, élèves et direction de l'École, un rôle considérable pendant et après la période de mai 68."*

Would you be willing to share with us some of your recollections of that period ?

This has indeed been a very exciting period, the campus of *l'École Polytechnique* being right in the middle of the *Quartier Latin*, which, in May 1968, became the focus of a lot of attention in France. In fact I think it is worth pointing out that already in 1967 there were signs that the very traditional (and blocked) situation the French society was in had entered a period of major crisis. The *École Polytechnique* itself had reached a stage of deterioration where it was impossible to hide the complete obsolence of its scientific management. Many professors were cut off from recent developments, and offering out of date courses. The Class of 1966 was the first that did not accept this very degraded situation, and asked for a complete revision of the curriculum. Students were fighting at the same time for more freedom in their movements (the military statute of the school forbade students to leave the school during the week for example) and in their choosing topics of study (the curriculum was uniform and quite scholastic). Students had to endure the sharp contrast between the outside image of the school, supposed to train the elite, and the very deteriorated level of the courses offered inside. This was unbearable to a number of them. The strong feeling of living the end of a world was very present before the May 1968 events, and undoubtedly led to them. Afterwards it had to be interpreted as a premonitory sign. In my opinion, this fact is too seldomly acknowledged with the proper emphasis. In the students' governing body, Yves Bamberger and myself (our duo was actually nicknamed *„le*

tandem Bambignon“, as quoted by Laurent Schwartz) shared the responsibility of questions connected with teaching, both from a qualitative and a structural point of view. To set the tone, let me recall an amazing fact : in 1967, our fellow students were ready to give up a weekend of free time to put pressure on the administration to get rid of a poor teacher. Is that not an image which fully contrasts that of May 68 ”baba-cools“ ?

Right in the agitated period, in the military environment of the school, going on strike was quickly identified as a critical step. Thanks to the very intelligent behaviour of the General heading the school, the struggle finally led to a complete restructuration of the courses for the last trimester under the supervision of voluntary professors, such as Louis Leprince-Ringuet and Laurent Schwartz who saw there an opportunity to give a big push to their vigourous claim for reform, and of students who wanted to prove the well-foundedness of their request for a new curriculum. This was of course a time of heated debates, justified fears, and finally important changes in the way some of us chose to conduct the rest of their lives.

For me, the big changes the May 68 riots brought concern the ”way of life“, and the consideration given to various groups of people in the society. I still vividly recall the way Yves Bamberger and myself were greeted by the President of the Board of the school in late June 1968 when, for the first time, representatives of the students chosen by them were allowed to address the Board: *”You must remember that you represent the future only biologically. Decisions will be ours“*. He resigned (or was forced to resign) in July 1968, and the General, who had so skillfully and constructively handled the crisis within the school, was transferred to an unimportant position in Bretagne (in other words sacked !). A *Commission de réforme* worked for the whole summer, and Bambignon was part of it. I must say that, from the point of view of the structure of studies, most of the students' proposals were adopted, and, for the whole academic year 1968-1969, the tandem was associated to their implementation under the supervision of a man with a strong personality, Jean Ferrandon, an engineer who had at the same time built extraordinary dams and harbours and developed a passion for rigorous mathematics. For young students in their early twenties as we were, this was an extraordinary experience, which could in some sense be put in parallel with *l'École de l'an Deux* at the time of the French Revolution. Several of our friends accused us of being recuperated by the system. Although the question is worthy of consideration, we never accepted this view. I really believe that major changes in complex systems can only be achieved under specific circumstances, and then can go quite far without exerting much pressure after they get started, provided the pressure is exerted in the right direction. It is very important not to miss such opportunities, and in such times personal views must become secondary. The May 1968 events made possible a very successful revitalisation of the scientific life at *l'École Polytechnique*, something Louis Leprince-Ringuet and Laurent Schwartz had been fighting for more than ten years without much success.

You became Docteurès Sciences Mathématiques having submitted a thesis with the title „Sur l'espace des structures riemanniennes d'une variété" at Paris VII in 1974. I think Marcel Berger was your thesis advisor. Let us talk about it for a while.

Space in what sense ? Is it possible to give us some idea of the problems you were dealing with ?

Before answering your question per se, I would like to set the stage a little bit. I was very lucky to join the profession at a time where, in France, young researchers were given exceptional opportunities to work. I was hired by the *Centre National de la Recherche Scientifique* at age 21, before I had really done anything substantial. This gave me the possibility of considering in a long term perspective the research work I got engaged in. This contrasts with the great pressure under which young researchers are now forced to work on a short time basis.

From a disciplinary point of view, differential geometry, the domain to which Marcel Berger introduced me during long afternoons of very open and extremely informative discussions, was at that time very poorly considered in France. In fact, if you were not working in algebraic geometry, you were not doing "real" mathematics. It took me a year of stay in the US in 1972-1973 to realize that the direction in which Marcel Berger had led me was of great interest to world famous mathematicians such as Shiing Shen Chern. What was really exciting was to be able to participate in, and modestly contribute to, the emergence of a new field, namely "Global analysis", the blend of analysis and geometry that transformed differential geometry from a specialised, and very computational, subject into a hot and much more center stage topic. Marcel Berger had remarkably foreseen this transformation, and encouraged his geometry students to invest into learning more sophisticated analysis tools, something I had done under the supervision of Gustave Choquet at *l'École Polytechnique*.

A typical question that he liked to consider at this time was to find, on a given manifold, the "best" Riemannian metric. This forces one to consider all Riemannian metrics at once, and to see how one can deform a given metric into more interesting ones. One then has to worry about equivalent metrics, i.e. metrics that are exchanged by the action of a diffeomorphism, in other words by a change of variables. Equivalence classes are called "Riemannian structures", and the purpose of my thesis was to prove the space they form is stratified because of the possible presence of groups of isometries, i.e. the isotropy groups for the action of diffeomorphisms. This space plays an important role in the so-called ADM-presentation of the General Relativity, where solutions of the Einstein equation are sought as paths in the space of Riemannian metrics on a 3-dimensional space-like hypersurface of space-time, for which one has to worry about the action of the group of diffeomorphisms. From that time on I kept interest in questions connected to deformations of metrics and the like.

From that moment on you have had a beautiful professional career. President of the European Mathematical Society from 1995 to 1998, Director of IHÉS since 1994, you probably still have some teaching to do. All these must be very time consuming jobs.

How do you still manage to find some time for mathematical research ?

It is true that in recent years I assumed several responsibilities that have taken time away from my strictly scientific activities. In fact colleagues usually do not realize how time consuming it is to be in charge of an institute like the IHÉS which is a private foundation, i.e. a place where the director must, besides making scientific choices, cope with real managerial and financial problems.

From the scientific point of view, the a priori attractive side of such jobs is that very international research institutes, such as the IHÉS, are extraordinary observatories of the mathematical life, where one can see new tendencies coming up, and also listen to the latest news about challenging problems. Living in such an environment gives fantastic opportunities to meet extraordinary people in the society at large (and not only in the scientific community), and this is a privilege.

Since my job as director of the IHÉS is limited in time (the term is a priori 8 years, but it is now likely that I will stay a bit longer), even before taking the job, I arranged things so that I could spend three half-days a week at *l'École Polytechnique* in a small office in a remote corridor. There, I try and concentrate on my own mathematical agenda. In fact, since for me keeping contacts with students is very important, I am still teaching a course a year, and I am enjoying it very much.

As part of my duties as director, I have to keep alert on new developments, and for that purpose attend a number of conferences each year. This is an exciting part of the job. In my situation, the main difficulty is to find long enough unperturbed periods of concentration on my own research. I must confess that there are definitely moments when I do not achieve it, but I hope to be forgiven for this.

When Professor Friedrich Hirzebruch asked me whether I would be willing to run for president of the European Mathematical Society (EMS) – I was not yet in charge of the IHÉS –, I really hesitated. It was evident to me that Europe is an appropriate level to fight for science, but I still had mixed recollections of the constitutional meeting of the EMS in 1990 in Madralin (Poland), in which I took part as President of the *Société Mathématique de France*. There the attention was focused on legal and political issues, when I am much more interested in developing tools to help European colleagues getting conscious of their interdependence, and learning to work together more closely. I could only convince myself that taking on this challenge could be meaningful after I made sure that our Austrian colleague, Peter Michor, accepted to form a ticket with me and run as EMS secretary. I am proud that through the establishment of the very successful EMS server EMIS (European Mathematical Information Service) Peter was given the

opportunity of putting his passion for electronic tools at work for colleagues, from Europe and elsewhere. Colleagues will judge whether the actions conducted by the EMS are successful, i.e. whether all people engaged in its committees and its actions are doing a good job. For me it was another fantastic experience, during which I was forced to understand and properly acknowledge different approaches, i.e. to face what building Europe is about. If I had one frustration, it came from the extreme slowliness with which the European Commission took up cases made by mathematicians. After some time one really gets impatient. I am very pleased to see that the new EU commissioner for Science, Philippe Busquin, succeeded in getting on its way a much more ambitious agenda, namely the construction of "a European Research Area", a programme which perfectly fits the EMS goals.

You have been making a number of interviews with great mathematicians (Chern, Hirzebruch, Thurston, Atiyah, Jacques-Louis Lions) which were considered to be of sufficient mathematical importance to be reviewed in Zentralblatt Math and Mathematical Reviews for instance.

How and why did you get started ?

Indeed, I devoted time to make a number of interviews of mathematicians. There are some you even did not list, and also some that I could not complete, such as one by Professor Jürgen Moser. I submitted a series of questions to him, and got preliminary answers but his struggle with cancer, which ended his life untimely in December 1999, prevented him from completing them.

Here are my two main motivations: first, I feel that mathematicians do not make enough efforts to collect testimonies of eminent mathematicians; second, the communication in our community has, in my opinion, taken a too formalized form. It now exists mainly through very carefully written articles appearing in refereed journals. Publishing interviews is a way of launching debates in the community on the basis of exchange of opinions. If I fully support the idea that published articles are the final mathematical products, we all know that doing mathematics requires going through many other steps, from identifying a promising area for research to realizing that an attempt to prove a theorem is a failure. If we want that outsiders access to a better understanding of how mathematics functions, we should therefore make also some room for all these steps. To those who fear that such an opening will lower the standards, I would say that this will not be the case if the same strict criteria are applied to this kind of articles.

Having some of these interviews reviewed in the international mathematical databases is not a sure sign of their importance. It nevertheless participates to the movement I was calling for earlier, namely making interviews a natural and significant part of the international mathematical life. You must share this view since you have been even more productive than me on this front.

Shall we talk about your videos ? You are mathematical author or co-author of two videos : „Tambour, que dis-tu ?“ which won a prize at the Palaiseau International Science Film Festival in 1987 and ”The New Shepherd's Lamp“ which you were invited to show now in Coimbra. It seems correct to imply that you attach great importance to the popularisation of Mathematics. . .

To make a transition between your previous question and this one, the interview with Professor Shiing Shen Chern comes from a video, an idea due to an old friend, Professor Anthony Philips.

In fact I participated in two more films but the two you mention are really the ones of which I am the scientific author. Both of them were conceived with a wide public in mind. It is clear to me that mathematicians have not devoted enough attention to the question of how to communicate with the general public on their achievements and the nature of mathematics. Specialists of other disciplines have come up with useful images for all kinds of objects of importance to them. We have to do the same. This will require efforts and a lot of imagination, something that colleagues who have never been in touch with cinema activities often do not correctly appreciate. Producing movies is not only expensive. It is also time consuming !

The making of these two movies has been enlightened by encounters made on these occasions. François Tisseyre and Claire Weingarten, film directors with whom I worked for both, have become friends. What was critical for the success of the entreprise was their thoroughness in filming only a content they felt comfortable with, and this was achieved through lengthy discussions, and back and forth exchanges. As a consequence the production of *The New Shepherd's Lamp* has been a lengthy process during which the initial idea I had was completely transformed into a script based on a much broader historical perspective. This was also an opportunity to see how a professional writer, Romain Weingarten, could turn into a text of literary value the script of the shepherd, the character introduced by the film director structuring the whole movie.

Finding adequate projects where artists and scientists can meet and work together should be a priority in my opinion. In this way mathematicians can get a better acquaintance with the mechanisms through which the media function. Indeed producing videos does not ensure that they will be shown in TV programmes, the only way to gain greater visibility. Some mathematical videos made it, e.g. the video *The Proof* on Fermat's last theorem produced by the BBC which has been shown on the german-french channel ARTE. As far as I am concerned, I have already shown *The New Shepherd's Lamp* about twenty times to extremely different publics. Its length (28 minutes) allows for a short oral presentation and a debate whose content depends very much on the audience. I always find it very challenging and informative.

You were a member of the panel which in 1999 was responsible for the research assessment exercise in Portugal.

I do not want to break any confidentiality which may surround that exercise but could you offer us your overall view of Portuguese mathematics at the end of the century ? You do not have to be particularly kind...

First some general comments. The Portuguese higher education system is expanding rapidly. Worldwide it is now recognized that quality at this level cannot be achieved without active research teams. Therefore it is natural to try and evaluate the research to make sure that university departments are according enough attention to it. The decision to call systematically upon international teams of experts to do this job in Portugal is courageous on the part of your research agency and of your Minister of Science and Technology, but certainly wise in the long run.

The team traveled to several cities in Portugal to visit all research groups in some ten days. It was always well received, and the presentations prepared for it almost always thoroughly informative. The team was confronted with very diverse situations : some labs were already operating at an international level, others just starting to develop significant research activities. In many universities we could witness unreasonable teaching loads that make it almost impossible to pursue actively research at a good level. What makes matter worse in Portugal is the length of the academic year and the time devoted to exams. Too often university professors do not have the free time indispensable to conduct substantial research work. If the government is really serious about developing a full fetched higher education system, it must address this issue which, from what I understand, means establishing stricter rules for students, a move which may be politically difficult. Such rules exist in almost all other countries.

From a more qualitative point of view, Portuguese research teams may not be diversified enough topically. Some important areas are not covered. In some cases, to the contrary some topics are overdevelopped, and such a situation can isolate some groups from what is happening elsewhere in the mathematical community worldwide. Again the antidote is to be open enough, to send advanced students for their PhD training outside as often as possible, and to grant active researchers the possibility of visiting other scientific institutions abroad.

The Portuguese system supports quite generously students while they are preparing their PhDs. In particular it allows them to go abroad by granting them decent support for this purpose. But the acceleration of hirings consecutive to the expansion of universities is likely to come to a hold in a not too distant future when the system will stop expanding. This could mean a major blow to the health of the research system in Portugal since younger people are indispensable for the stimulation of the research. Mechanisms should be designed to ensure that positions will remain available at a steady rate in the years to come. Many countries in

Western Europe have undergone a similar phenomenon in the 70's, and negative effects consecutive to this short-sightedness have been major. If a lesson could be learned from this recent experience, Portugal may be able to achieve a smoother development of its mathematical research.

Fotos aus dem Besitz von F. J. Craveiro de Carvalho.

Buchbesprechungen

Allgemeines, Sammelbände — General, Collections — Généralités, collections

A. K. Dewdney: Reise in das Innere der Mathematik. Aus dem Amerikanischen von M. Zillgitt. Birkhäuser, Basel, Boston, Berlin, 2000, 260 S. ISBN 3-7643-6189-1 P/b sFr 34,–.

Das Buch bietet einen gut lesbaren und vergnüglichen Ausflug ins Reich der Mathematik. In acht Kapiteln wird der Frage nachgegangen, ob Mathematik entdeckt oder erfunden wird. In fiktiven Gesprächen werden der Reihe nach berühmte Resultate mathematischen Forschens vorgestellt: von der griechischen Schule um Pythagoras, den arabischen Mathematikern um Al-Chwarismi über die Beschreibung der Spektralserien durch Balmer bis zur Abstraktion und der Mechanisierung des Denkens durch moderne Computer reicht dabei der Bogen. A. K. Dewdneys Buch ist allen jenen zu empfehlen, die eine angenehm lesbare Einführung in den Umgang mit mathematischen Fragestellungen suchen, die von den historischen Wurzeln bis heute reichen.

O. Röschel (Graz)

H. M. Enzensberger: Zugbrücke außer Betrieb. Die Mathematik im Jenseits der Kultur. Eine Außenansicht. Illustrationen von K. H. Hofmann. (Bilinguale Ausgabe Deutsch/Englisch. Englischer Titel: Drawbridge Up. Mathematics—A Cultural Anathema. Translated by T. Artin.) A. K. Peters, Natick, Massachusetts, 1999, 48 S. ISBN 1-56881-099-7 P/b $ 5,–.

Das Bemerkenswerteste an diesem Buch ist wohl, dass der Autor, Hans Magnus Enzensberger, zu den renommiertesten Schriftstellern der deutschen Literatur seit 1945 zählt. Neben Gedichten und Essays verfasste er 1997 das Buch „Der Zahlenteufel: Ein Kopfkissenbuch für alle, die Angst vor der Mathematik haben“, mit dem er auch in Mathematikerkreisen einen besonderen Bekanntheitsgrad erlangt hat.

Im vorliegenden Buch (die linken Seiten sind in deutscher, die rechten in englischer Sprache) versucht Enzensberger das Phänomen zu erklären, dass selbst gebildete Menschen offen zugeben – nicht selten sogar stolz –, dass sie in der Schule in Mathematik immer schlecht gewesen seien. Sind die Mathematiker

vielleicht selbst schuld, dass sie isoliert auf einer Insel sitzen? Haben sie selbst die Zugbrücke zum Rest der Gesellschaft hochgezogen?

Die extreme Spezialisierung in der Mathematik wie auch ein wechselseitig argwöhnisches Verhältnis zwischen reiner und angewandter Mathematik ist für Enzensberger die Ursache für eine verkümmerte Kommunikation sowohl innerhalb der mathematischen Community als auch zwischen dieser und dem Rest der Gesellschaft. Auch der Schule gelingt es im Fach Mathematik im Gegensatz zu anderen Fächern so gut wie überhaupt nicht, ein bisschen von der Faszination der Mathematik zu vermitteln. Enzensberger hofft auf „semantische Annäherungen“ von Mathematikern in Richtung Laien, d. h. auf das langsam aufkeimende Bewusstsein von Mathematikern, dass sie selbst die Faszination der Mathematik in einer entsprechend vereinfachten Sprache einem größeren Leserkreis zugänglich machen müssen.

M. Kronfellner (Wien)

M. Gazalé: Number. From Ahmes to Cantor. Princeton University Press, Princeton, New Jersey, 2000, XV+297 S. ISBN 0-691-00515-X H/b $ 29,95.

Dieses Buch des Ingenieurs (Telekommunikation, Computerwissenschaft) M. Gazalé wendet sich so wie sein Vorgänger ’Gnomon: From Pharaohs to Fractals’ an interessierte, aber durchaus vorgebildete Laien. Es schildert in breiter Sprache, aber manchmal mit unnötig komplizierter symbolischer Notation historische und mathematische Phänomene um den Zahlbegriff (z.B. Zahldarstellungen für natürliche, rationale und reelle Zahlen und ihre Eigenschaften; elementare Sätze der Zahlentheorie, Kettenbrüche). Dabei wechseln Standardthemen mit sehr speziellen eigenständigen Beiträgen des Autors und einigen eher isolierten Fragestellungen (z.B. Stern-Brocot-Bäume für Brüche). Sehr ausführlich werden ’cleavages’ behandelt, eine zweidimensionale Veranschaulichung Dedekindscher Schnitte mit dem Ziel ’[to] shed light on the mysterious nature of irrational numbers . . . ’. Immer wieder werden allerdings Resultate en passant ohne Beweis verwendet, ohne Literaturhinweise zu geben. Eine weitere Kritik betrifft die Verwendung von Begriffen (wie z.B. Konvergenz von Folgen oder Reihen), ohne diese zu erläutern oder anzumerken, in welchem Sinne sie verwendet werden. Die manchmal belächelte Genauigkeit und Stringenz in der Mathematik ist eben doch für ein tiefergehendes Verständnis unerläßlich. Und so manches, was hier als ’Paradoxie’ bezeichnet wird (z.B. bedingte Konvergenz von Reihen), klärt sich bei exakter Behandlung einfach auf. Bei der Lektüre spürt man die persönliche Faszination des Autors, würde sich aber gerade in einem solchen Buch Hinweise wünschen darauf, warum und in welchen Zusammenhängen die Begriffe und Methoden entwickelt wurden. Sonst bekommt manches Thema zu leicht den Anstrich des Mystischen oder der Beliebigkeit. Mathematik ist aber kein Mysterium, sondern durch und durch verstehbares Ergebnis menschlicher Kreativität!

W. Dörfler (Klagenfurt)

R. Laubenbacher, D. Pengelley: Mathematical Expeditions. Chronicles by the Explorers. With 94 Illustrations. (Undergraduate Texts in Mathematics, Readings in Mathematics.) Springer, New York u.a., 1999, X+275 S., ISBN 0-387-98433-X P/b DM 69,–, ISBN 0-387-98434-8 H/b.

Die beiden Autoren haben fünf mathematische Bereiche ausgewählt, an deren jahrhundertelanger Erforschung sehr viele Mathematiker mehr oder weniger erfolgreich, jedenfalls aber mit intensivstem Forschergeist gearbeitet haben, für die weiters die ‘uralten‘ Ausgangsfragen jetzt im großen und ganzen als zufriedenstellend gelöst angesehen werden, wobei aber schließlich die Fragestellungen auch heute noch sehr großes und allgemeines Forschungsinteresse erwecken und immer weitere aktuelle Themenkreise erzeugen. Das Buch führt auf folgende mathematische Reisen: 1. Geometry: The Parallel Postulate, 2. Set Theory: Taming the Infinite, 3. Analysis: Calculating Areas and Volumes, 4. Number Theory: Fermat's Last Theorem, 5. Algebra: The Search for an Elusive Formula. Den Beginn eines jeden Kapitels macht jeweils ein einleitender Abschnitt, in welchem in der Sprache der modernen Mathematik einerseits die Problemstellungen und andererseits die Ideen und Lösungskonzepte jener in all den Jahren daran tätigen Mathematiker vorgestellt werden, welche substantielle ‘Meilensteine‘ zur Lösung beigetragen haben. Anschließend folgen — natürlich in der zum Teil notwendigen sprachlichen und begrifflichen Anpassung an den heutigen Leser — möglichst originale Ausführungen der Wege und Irrwege dieser Mathematiker.

Eine — zweifellos nur bruchstückhafte — Beschreibung der fünf Abschnitte soll durch die Aufzählung der von den beiden Autoren als jeweils wichtigste Wegbereiter herangezogenen und daher im Inhaltsverzeichnis explizit angeführten Mathematiker versucht werden: *ad 1:* Von Euklid über Legendre und Lobachevsky zu Poincaré; *ad 2:* Von Bolzano über Cantor zu Zermelo; *ad 3:* Von Archimedes über Cavalieri, Leibniz und Cauchy zu Robinson; *ad 4:* Von Euklid über Euler, Germain und Kummer zu Wiles; *ad 5:* Von Euklid über Cardano und Lagrange zu Galois.

Wenn auch das eine oder andere historisch bedeutsame Ereignis erzählt wird, so liegt absolut kein historisches, sondern ein mathematisches Buch vor; es geht vor allem um das Kennenlernen der Entwicklung der zentralen mathematischen Ideen von frühen Zeiten bis hin zum aktuellen Forschungsstand.

P. Paukowitsch (Wien)

E. Neuwirth: Musikalische Stimmungen. Mit CD-ROM. Springer, Wien, New York, 1997, VII+73 S. ISBN 3-211-83000-6 P/b öS 550,–.

Das Buch ist die Papiervariante einer beigefügten CD-ROM, die nicht nur den gesamten Text, sondern vor allem auch instruktive akustische Beispiele (Tonfolgen und Akkorde) enthält, die die mathematisch beschriebenen Unterschiede auf geschickte Weise hörbar machen (besonders instruktiv ist dabei das gleichzeitige

Hören verschiedener Stimmungen!). Ausführlich werden vier Stimmungen dargestellt, die reine Stimmung, die pythagoreische Stimmung, die mitteltönige und die gleichschwebende Stimmung (die wohl bekannteste der temperierten Stimmungen). Schade, dass sich keine Hinweise finden, wie stark man in der Aufführungspraxis von den vorgestellten idealen Stimmungen abweicht.

F. Schweiger (Salzburg)

Geschichte, Biographie — History, Biography — Histoire, biographies

J. Albree, D. C. Arney, V. F Rickey: A Station Favorable to the Pursuits of Science. Primary Materials in the History of Mathematics at the United States Military Academy. (History of Mathematics, Vol. 18.) American Mathematical Society, Providence, Rhode Island — London Mathematical Society, 2000, XII+272 S. ISBN 0-8218-2059-1 H/b $ 59,–.

Der überwiegende Teil des Buches (S. 41 234) gibt einen Überblick über die reiche Sammlung mathematischer Werke an der U.S. Military Academy in West Point. Auf den Seiten davor wird die Entwicklung der USMA dargestellt, wobei insbesondere auf den Unterricht in Mathematik und Mechanik eingegangen wird. Vier Anhänge beschließen das Werk („Catalog of 1803“, „Photographs“, „Portraits in the Collection“, „Frontispieces in the Collection“).

M. Kronfellner (Wien)

A. Stubhaug: Niels Henrik Abel and his Times. Called Too Soon by Flames Afar. Translated from the Norwegian by R. H. Daly. With 51 Figures, 13 in Colour. Springer, Berlin u.a., 2000, X+580 S. ISBN 3-540-66834-9 H/b DM 79,–.

Das vorliegende Buch ist eine neue Biographie von Niels Henrik Abel. Der Autor hat sich der Aufgabe unterzogen, das Leben des norwegischen Genies bis ins letzte Detail nachzuvollziehen (wer wußte z.B., daß Abel auf seiner Reise durch Europa für ein paar Tage in Graz Station gemacht hat?). Es erstaunt den Leser, daß sich nach 180 Jahren noch so viele Detailinformationen auffinden lassen. Neben den biographischen Informationen wird auch das historische Umfeld genauestes beleuchtet, sodaß man einen umfänglichen Überblick bekommt.

Die Biographie beginnt beim Großvater (!) Abels, setzt sich dann über den Vater und dessen glückloses politisches Intermezzo im norwegischen Reichstag fort und kommt dann endlich (auf Seite 150!) zum eigentlichen Protagonisten des Buches. Einerseits ist der Detailreichtum und die Genauigkeit, mit der der Autor das Leben Abels rekonstruiert hat, verblüffend, andererseits ergeht er sich streckenweise in

zu kleinen (und manchmal auch spekulativen) Details, die dann einfach zu weit führen. Manchmal würde man sich als Mathematiker vielleicht auch eine Formel zur Erläuterung wünschen; solches wird aber konsequent vermieden.

Insgesamt ein empfehlenswertes Buch, das auch einiges über die Wissenschaftswelt der damaligen Zeit vermittelt.

P. Grabner (Graz)

Logik und Grundlagen — Logic, Foundations — Logique et fondements

T. Tymoczko, J. Henle: Sweet Reason. A Field Guide to Modern Logic. Springer, New York u.a., 2000, XXII+644 S. ISBN 0-387-98930-7 P/b DM 79,–.

Diese bereits 1995 bei Freeman erschienene Einführung in die Logik in ihrer vollen Breite (das Vorwort weist auf ihre grundlegende Stellung für Philosophie, Mathematik, Informatik, Linguistik und Kognitionswissenschaften hin) besticht durch ihren Aufbau: Jedes der neun Kapitel gliedert sich in vier Unterabschnitte mit immer den gleichen Titeln: “formal logic”, “with & about logic” (Abstecher zu verwandten Gebieten mit Hintergrundwissen), “informal logic” (Logik im Alltag, Argumentation, ...), “curiosities & puzzles” (enthält Übungen; ausgewählte Lösungen im Anhang), die sich durch Markierungen am Buchrand leicht auffinden lassen. Das erlaubt bequemes selektives Lesen und das Extrahieren verschiedenster Logikkurse mit unterschiedlicher Ausrichtung. Durchgehend wird darauf geachtet, die Nützlichkeit der symbolischen Logik in den unterschiedlichsten Situationen zu untermauern. Die Beispiele aus dem Alltag vermögen für europäische Leser nicht immer das gleiche Interesse zu wecken wie für Amerikaner, aber wo es zum Beispiel um Paradoxien geht, die einen besonderen Stellenwert im Buch einnehmen, ist sicher jeder gebildete Laie angesprochen. Die Abschnitte über formale Logik sind ordentlich, verlassen aber niemals elementares Niveau. Aber für Studenten der formalen und mathematischen Logik gibt es ja genügend Alternativen am Markt.

P. Teleč (Wien)

Kombinatorik und Graphentheorie — Combinatorics and Graph Theory — Combinatoire, théorie des graphes

J. M. Aldous, R. J. Wilson: Graphs and Applications. An Introductory Approach. With 644 illustrations by S. Best. Mit CD-ROM. Springer u.a., 2000, XI+444 S. ISBN 1-85233-259-X P/b DM 89,–.

Diese elementare und detailliert geschriebene Einführung in die grundlegenden Teile der Theorie ungerichteter und gerichteter Graphen weist einige Besonderheiten auf, die sie sehr empfehlenswert für Anfänger und Anwender machen. Das Buch entstand aus einem langjährig erprobten Kurs an der British Open University und ist durch seine didaktische Aufbereitung auch zum Selbststudium geeignet. Es gibt zahlreiche Diagramme (mehr als 600), Beispiele, Übungsaufgaben (mit Lösungen), Anwendungen mit methodischen Hinweisen sowie eine CD-ROM (Windows). Letztere enthält eine Datenbank mit Graphen sowie Software zur Konstruktion und Manipulation von Graphen. Im Anhang gibt es Anregungen zur Verwendung der Software. Das gesamte Layout macht den Text angenehm lesbar und wirkt motivierend auf den Leser. Bei Verwendung in Vorlesungen für Mathematiker müßte allerdings eine Reihe von Beweisen ergänzt werden.

W. Dörfler (Klagenfurt)

R. Diestel: Graph Theory. Second Edition. With 122 Illustrations. (Graduate Texts in Mathematics 173.) Springer, New York u.a., 2000, XIV+312 S. ISBN 0-387-95014-1 H/b, ISBN 0-387-98976-5 P/b DM 69,–.

Im Band 174 (1997) der IMN wurde die deutsche Fassung des vorliegenden Werkes bereits besprochen. Die Aufnahme in die Serie “Graduate Texts in Mathematics” des Springer-Verlages ist begrüßenswert und entspricht durchaus dem Charakter des Werkes.

Obwohl die Erstausgabe erst 1996 erschien, kann das Buch bereits jetzt als Standardwerk eines modernen Zugangs zur Graphentheorie gewertet werden. Hervorzuheben sind vom Inhalt her eine ausführliche Behandlung planarer Graphen, neuere Resultate über Listenfärbung von Graphen, Ramsey-Theorie auf Graphen, Zufallsgraphen und Graph-Minoren.

Der Autor gibt bei etlichen Resultaten mehrere Beweise an und bietet damit tiefere Einsicht in die Materie. Eine Fülle von Übungsaufgaben sehr unterschiedlichen Schwierigkeitsgrades bietet den Studierenden ausreichend Gelegenheit, auch selbst Hand anzulegen. Bibliographische Notizen am Ende eines jeden Kapitels geben interessante Hintergrundinformation.

Insgesamt hat das Buch die besten Voraussetzungen, sich als Standardwerk der Graphentheorie zu etablieren.

F. Rendl (Klagenfurt)

J. M. Harris, J. L. Hirst, M. J. Mossinghoff: Combinatorics and Graph Theory. With 124 Illustrations. (Undergraduate Texts in Mathematics.) Springer, New York u.a., 2000, XIII+225 S. ISBN 0-387-98736-3 H/b DM 69,–.

Ist man an Graphentheorie und Kombinatorik als anspruchsvollen, tiefgehenden und faszinierenden mathematischen Gebieten interessiert, so bietet sich dieses Buch zur Lektüre oder als Grundlage für Vorlesungen bestens an. Die Stoffauswahl in den drei Kapiteln orientiert sich deutlich an der mathematischen Ergiebigkeit, jedoch kaum an Anwendungen, und bringt teilweise sonst weniger behandelte Themen. Allerdings liegt dadurch das Niveau trotz eines sehr gut lesbaren Schreibstils stellenweise eindeutig über 'undergraduate'. Aus dem Inhalt seien nur (neben den Standardthemen) erwähnt: im 1. Kapitel (Graphen) Ramsey-Theorie und im 2. Kapitel (Kombinatorik) Polya'sche Abzähltheorie, Stirling-, Bell- und Euler-Zahlen. Das 3. Kapitel behandelt Variationen des Schubfachprinzips und der Ramsey-Sätze für unendliche Mengen. Das erfordert eine knappe Einführung in ZFC einschließlich Ordinal- und Kardinalzahlen und führt in sehr gedrängter Form zu regulären, unerreichbaren und schwach kompakten Kardinalzahlen. Zu jedem Abschnitt gibt es zahlreiche und auch anspruchsvolle Aufgaben (ohne Lösungen) und Hinweise für weiteres Studium.

W. Dörfler (Klagenfurt)

K. H. Rosen, J. G. Michaels, J. L. Gross, J. W. Grossman, D. R. Shier (Eds.): Handbook of Discrete and Combinatorial Mathematics. CRC Press, Boca Raton, London, New York, Washington, D. C., 2000, 1232 S. ISBN 0-8493-0149-1 H/b DM 156,–.

Die Diskrete Mathematik ist eine der am schnellsten wachsenden Disziplinen der zeitgenössischen Mathematik. Dieses exzellente Handbuch versucht auf über 1200 Seiten einen Überblick über die komplexe Materie zu geben. Behandelt werden Grundlagen (Logik, Axiomatik,. . .), Zählmethoden, rekursive Folgen, die Grundlagen der Zahlentheorie, der Algebra und der diskreten Wahrscheinlichkeitstheorie, sowie Graphentheorie, Designs, endliche Geometrien, Codierungstheorie, Kryptologie, diskrete Optimierung und schließlich Themen aus der theoretischen Informatik (Grammatiken, Komplexität, Datentypen und -strukturen, dynamische Algorithmen). Jeder Abschnitt enthält die wichtigsten Definitionen, Sätze und Beispiele, Informationen über offene Probleme, wichtige Algorithmen und interessante Anwendungen nach dem Schema "Definitions – Facts – Examples". Querverweise vernetzen den gesamten Text zu einem Ganzen. Der weitaus größte Teil der 76 beteiligten Autoren kommt interessanterweise aus den USA. Sehr gut ausgewählte Literaturzitate, Tabellen und historische Kommentare runden den Text hervorragend ab. Dieses Handbuch ist nicht hoch genug einzuschätzen; es gehört auf den Schreibtisch einer/eines jeden, die/der mit Diskreter Mathematik zu tun hat.

G. Pilz (Linz)

M. Atkinson, N. Gilbert, J. Howie, St. Linton, E. Robertson: Computational and Geometric Aspects of Modern Algebra. (London Mathematical Society Lecture Note Series 275.) Cambridge University Press, 2000, XVIII+279 S. ISBN 0-521-78889-7 P/b £ 27,95.

Im Juli 1998 fand an der Heriot-Watt University (Edinburgh, UK) ein Workshop über die im Titel des Buches genannten Themen statt. Unter den über 100 Teilnehmern befand sich ein Großteil der führenden Forscher auf diesen Gebieten. Dieser Sammelband der Tagung enthält daher einen repräsentativen Querschnitt des heutigen Wissens zu dieser Themen. Stellvertretend für die 18 Artikel seien genannt: ”Constructing hyperbolic manifolds” (Epstein-Holt), ”Some applications of prefix-rewriting in monoids, groups, and rings” (Madlener-Otto) und ”Cancellation diagrams with non-positive curvature” (Huck-Rosebrock).

G. Pilz (Linz)

J. A. Beachy: Introductory Lectures on Rings and Modules. (London Mathematical Society Student Texts 47.) Cambridge University Press, 1999, VIII+238 S. ISBN 0-521-64340-6 H/b £ 42,50, ISBN 0-521-64407-0 P/b £ 15,95.

The title of the book might be slightly misleading, since it is its declared goal to focus on the noncommutative aspects of rings and modules, hence complementing the book “Steps in Commutative Algebra” by R. Y. Sharp.

The first two chapters present the basic definitions of Rings and Modules, while the third presents an analysis of certain aspects of noncommutative rings, mainly the Jacobson radical and semisimple artinian rings.

The fourth chapter introduces representations of finite groups and focuses on character theory. The author wants to illustrate a successful application of (noncommutative) ring theory, and although the choice is contestable in a book which claims to be introductory, the chapter is short and actually readable, hence presenting a rather interesting addition.

The book is complemented with an Appendix reviewing a variety of basic materials, e.g. vector spaces and Zorn’s Lemma.

C. Alos-Ferrer (Wien)

W. Bruns, J. Herzog : Cohen-Macaulay Rings. Revised edition. (Cambridge studies in advanced mathematics 39.) Cambridge University Press, 1998, XIV+ 453 S. ISBN 0-521-56674-6 P/b £ 24,95, ISBN 0-521-41068-1 H/b £ 55,–.

The sequence $X_1, X_2, \ldots, X_n$ of the indeterminates in the polynomial ring $S[X_1, \ldots, X_n]$ gives rise to the more general concept of an "M-sequence", and this in turn leads to Cohen-Macaulay rings which generalize rings of polynomials or formal power series. Like these, Cohen-Macaulay rings play an essential part in modern commutative algebra and in the connections to geometry and algebraic combinatorics attached to it. Homological methods are ubiquitous. Despite the non-trivial nature of the subject, the presentation is kept as elementary as possible, many connections to other theories are opened up, applications are treated, and many exercises (with hints to their solutions) are presented.

G. Pilz (Linz)

P. M. Cohn: Introduction to Ring Theory. (Springer Undergraduate Mathematics Series.) Springer, London u.a., 2000, X+229 S. ISBN 1-85233-206-9 P/b DM 49,–.

Ring theory has become a vast area of algebra. A guided tour through the most important topics is a difficult task. The author - one of the masters of this theory - has come up with a beautiful work which leads the reader along easy pathways to the highlights of ring theory. Difficulties in the theory are addressed (and hence tamed) and not hidden in abstract and short arguments. After an introduction to the basic concepts (including categories), the author treats rings and algebras with chain condition, PIDs, ring constructions (with tensor products), projective and injective modules, rings of fractions, skew polynomial rings, and free ideal rings. Many exercises (with solution outlines) and carefully chosen examples will help the reader to easily digest the material. If only there were more books of this kind!

G. Pilz (Linz)

M. Hazewinkel (Ed.): Handbook of Algebra, Volume 2. North Holland — Elsevier, Amsterdam, Lausanne, New York, Oxford, Shannon, Singapore, Tokyo, 2000, XIX+878 S. ISBN 0-444-50396-X H/b $ 177,50.

Seit mehreren Jahren verfolgt Michiel Hazewinkel ein anspruchsvolles (und anstrengendes) Programm: den wichtigsten Inhalt der modernen Algebra in etwa 10 (dicke) Bände zu kondensieren. Der 1. Band erschien 1995; Band 3 ist für 2001 geplant. Die einzelnen Artikel werden von führenden Forschern auf den jeweiligen Gebieten geschrieben und haben üblicherweise eine Länge zwischen 25 und 50 Seiten. Dieser Band enthält folgende Beiträge: "Some aspects of categories in computer science" (P.J. Scott), "Algebra, categories and databases" (B. Plotkin), "Homology for the algebras of analysis" (A.Ya. Helemskii), "Stable groups" (F. Wagner), "Artin approximation" (D. Popescu), "Fixed rings and

noncommutative invariant theory" (V.K. Kharchenko), "Modules with distributive submodule lattice" (A.A. Tuganbaev), "Serial and semidistributive modules and rings" (A.A. Tuganbaev), "Modules with the exchange property and exchange rings" (A.A. Tuganbaev), "Separable algebras" (F. Van Oystaeyen), "Varieties of Lie algebra laws" (Yu. Khakimdjanov), "Varieties of algebras" (V.A. Artamonov), "Infinite-dimensional Lie superalgebras" (Yu. Bahturin, A.A. Mikhalev and M. Zaicev), "Nilpotent and solvable Lie algebras" (M. Goze and Yu. Khakimdjanov), "Infinite Abelian groups: Methods and results" (A.V. Mikhalev and A.P. Mishina), "Infinite-dimensional representations of quantum algebras" (A.U. Klimyk), "Burnside rings" (S. Bouc), "A guide to Mackey functors" (P. Webb). Ich wünsche dem Herausgeber weiterhin alles Gute für sein Mammutprojekt zum Wohl der Algebra!

G. Pilz (Linz)

A. A. Ivanov: Geometry of Sporadic Groups I. Petersen and tilde geometries. (Encyclopedia of Mathematics and Its Applications 76.) Cambridge University Press, 1999, XIII+408 S. ISBN 0-521-41362-1 H/b £ 45,–.

Einige der sporadischen Exemplare unter den endlichen einfachen Gruppen wurden als Automorphismengruppen geometrisch-kombinatorischer Strukturen entdeckt. In einer Reihe von bahnbrechenden Arbeiten entwickelte vor allem Jacques Tits daraus die sogenannten „Diagramm-Geometrien". Hierher gehören auch die zwei im Buchtitel genannten Klassen von Geometrien, die mit dem Petersen-Graph beziehungsweise dem verallgemeinerten Viereck der Ordnung $(2,2)$ in engem Zusammenhang stehen.

Eines der Hauptziele des vorliegenden Buches und des daran anschließenden zweiten Bandes ist eine vollständige Klassifikation der Petersen- und Tilde-Geometrien mit flaggentransitiver Automorphismengruppe. Aus Platzgründen können wir auf den äußerst reichen Inhalt des ersten Bandes nur in Ansätzen eingehen: So bringt etwa das 2. Kapitel die Existenz und Eindeutigkeit des binären Golay-Codes, die Existenz und Eindeutigkeit des „großen Witt-Blockplans", also des Steiner-Systems $S(5,8,24)$, den Zusammenhang mit der projektiven Ebene der Ordnung 4 und ferner die „großen" und die „kleinen" Mathieugruppen. Es folgt ein Kapitel über das Leech-Gitter und die Geometrien zu gewissen Untergruppen von Conway-Gruppen. Ferner werden etwa das „Monster", die zugehörigen Tilde-Geometrien und vieles andere mehr diskutiert.

H. Havlicek (Wien)

A. Schinzel: Polynomials with Special Regard to Reducibility. (Encyclopedia of Mathematics and Its Applications 77.) Cambridge University Press, 2000, X+558 S. ISBN 0-521-66225-7 H/b £ 60,–.

Das vorliegende Werk gibt einen äußerst aktuellen Überblick über Polynomalgebra mit Schwerpunkt Reduzibilität über allgemeinen Körpern. Spezielle Resultate, die nur über endlichen Körpern, über lokalen Körpern oder über $\mathbb{Q}$ gelten, wurden nicht berücksichtigt. Kapitel 1 beginnt mit dem Satz von Lüroth und bringt einen konstruktiven Beweis. Danach findet man eine Darstellung der Ritt'schen Theorie über die Komposition von Polynomen. Ferner wird in diesem Kapitel die Reduzibilität von Polynomen der Form $(f(x)-g(y))/(x-y)$ behandelt. Es wird der neue von G. Turnwald angegebene Beweis des Satzes von M. Fried wiedergegeben. Im zweiten Kapitel werden die Sätze von Capelli und M. Kneser behandelt. Dieses Kapitel beschäftigt sich ferner mit einer Verallgemeinerung eines Satzes von Gouvin und mit der Reduzibilität von Trinomen über rationalen Funktionenkörpern $k(y)$. Gerade zur Entwicklung dieser Theorie hat der Autor selbst grundlegende Beiträge geleistet und der Referent erinnert sich mit Vergnügen an eine Vortragsreihe, die A. Schinzel über Reduzibilität von Trinomen anläßlich einer Zahlentheorie-Tagung in Graz hielt. Kapitel 3 behandelt Polynome über algebraisch abgeschlossenen Körpern und beginnt mit einem Satz von E. Noether, wonach eine Form vom Grad d in n Variablen über einem algebraisch abgeschlossenen Körper genau dann reduzibel ist, wenn die Koeffizienten ein gewisses System von algebraischen Gleichungen (nur abhängig von d und n) erfüllen. Ebenfalls behandelt wird hier der Satz von Ruppert, der für $n = 3$ und Charakteristik 0 eine explizite Konstruktion des genannten Gleichungssystems angibt. Schließlich enthält dieses Kapitel noch den Satz von Bertini und mehrere bemerkenswerte und aktuelle Resultate über das Mahler-Maß von Polynomen über $\mathbb{C}$. Kapitel 4 ist Polynomen über endlich erzeugten Körpern gewidmet. Hier findet sich auch eine gründliche Diskussion des Hilbertschen Irreduzibilitätssatzes. Dieser Satz steht in enger Beziehung zu diophantischen Gleichungen: Falls eine algebraische Gleichung $F(x,t) = 0$ in ganzen Zahlen x für hinreichend viele t lösbar ist, dann ist die Gleichung lösbar für x in $\mathbb{Q}[t]$. Das fünfte Kapitel beschäftigt sich nun mit Verallgemeinerungen dieses Sachverhalts auf Gleichungen in mehreren Unbekannten und auf algebraische Zahlkörer (anstelle von $\mathbb{Q}$). Das letzte Kapitel behandelt Polynome über Kroneckerschen Körpern, das sind entweder total reelle Zahlkörer oder komplexe quadratische Erweiterungen solcher Körper. Hier findet sich insbesondere eine Darstellung der Arbeiten von Győry über Reduzibilität von zusammengesetzten Polynomen $F(G(x))$ über Kroneckerschen Körpern. Am Ende des Buches finden sich mehrere Anhänge über verschiedene Hilfsmittel, die vom Autor benutzt werden. Insbesondere ist ein Anhang zu erwähnen, der von U. Zannier verfaßt wurde und ein Problem löst, das in der ersten Fassung von Kapitel 4 noch als Vermutung formuliert wurde.

Mit dem vorliegenden Werk liegt eine gediegene Monographie über Polynom-

algebra vor, die in keiner mathematischen Bibliothek fehlen sollte. Sie wird allen Algebraikern und Zahlentheoretikern zur Lektüre wärmstens empfohlen.

R. Tichy (Graz)

Zahlentheorie — Number Theory — Théorie des nombres

R. A. Mollin: Algebraic Number Theory. (The CRC Press Series on Discrete Mathematics and Its Applications.) Chapman & Hall/CRC, Boca Raton, London, New York, Washington, D. C., 1999, XIV+483 S. ISBN 0-8493-3989-8 H/b £ 55,50.

Das vorliegende Lehrbuch geleitet den Leser durch die Anfänge der algebraischen Zahlentheorie, wobei er durch viele Zahlenbeispiele und Rechnungen motiviert werden soll und ihm immer wieder versichert wird, daß er keine großartigen Voraussetzungen (etwa abstrakte Algebra) zur Lektüre benötigt.[1]

Der Stoff wird ohne strengen logischen Aufbau angeboten: Begriffe werden vor ihrer Definition verwendet und Beweisteile - manchmal gerade die interessantesten - werden als nachfolgende Übungsaufgabe gestellt. Der redundante Sprachstil behindert manchmal ein verständnisvolles Lesen, und die mathematischen Grundgedanken bleiben öfter verborgen. Die Formulierungen sind oft ungenau (Exercise 1.55 ist für transzendentes α falsch, in Theorem 1.63 und Corollary 1.68 muß es $q_{i,k} \in \mathbb{Q}$ heißen, in der Erklärung von „kompakt“ in Fußnote 2.18 sollten die Mengen offen sein) und einige Beweise falsch: der Beweis von Theorem 2.26 läßt jedem Algebraiker die Haare zu Berge stehen, der Beweis der letzten Aussage von Theorem 2.39 ist ebenso falsch wie der erste Teil des Beweises von Theorem 2.45. Im Beweis von Proposition 5.3 werden viele einfache Details erklärt, nicht jedoch erwähnt, wieso die Norm jedes zu 3 primen Primelements von $\mathbb{Q}(\zeta_3)$ kongruent zu 1 modulo 3 ist. Aus der Formulierung von Proposition 5.80 geht nicht hervor, daß die Norm jedes zu n primen Primideals von $\mathbb{Q}(\zeta_n)$ kongruent zu 1 modulo n ist.

Obwohl sich viele biographische, nicht nur deren mathematisches Leben betreffende Details über Mathematiker in Fußnoten finden, wird Theorem 2.54 nicht als Dirichletscher Approximationssatz bezeichnet. Diesen mit Hilfe des Minkowskischen Linearformensatzes zu beweisen, erscheint dem Rezensenten wie ein Kanonenschuß auf Spatzen! Endgültiges Ärgernis bereitet der Anhang über abstrakte Algebra: Bilden alle Elemente eines Körpers wirklich eine multiplikative Gruppe (sie erfüllen A.2, A.8, A.9 und A.12)? Was ist „das“ erzeugende Element einer

[1] Als gutes Beispiel, wie man einen Leser mit wenigen mathematischen Vorkenntnissen durch ausgewählte Zahlenbeispiele motiviert und über die Grundlagen der Algebra zur algebraische Zahlentheorie hinführt, möchte ich etwa A. Leutbechers Buch „Zahlentheorie – Eine Einführung in die Algebra“ (1996; vgl. Buchbesprechung in IMN 176, S. 15f.) erwähnen.

zyklischen Gruppe (A.15)? Braucht ein Schiefkörper bzw. Ring nur *ein* Distributivgesetz zu erfüllen (A.22)? Ist die multiplikative Gruppe jedes Körpers zyklisch (A.26)? Theorem A.16 ist eine Meisterleistung falscher Formulierung!

Bei der Lektüre dieses Buches mußte der Rezensent an ein modernes Zeitgeistmagazin denken: solide Information wird nur häppchenweise und ohne Strukturierung geboten, aktuelle Mode-Themen werden angerissen (A.Wiles und der große Fermat, Kryptographie, Zahlkörpersieb, Faktorisierungsmethoden mit elliptischen Kurven), ohne in die Tiefe gehen zu können, dafür wird das Buch mit Inhalten belastet, die mit algebraischer Zahlentheorie wenig bis gar nichts zu tun haben: Einzelheiten aus der elementaren Zahlentheorie, ein Kapitel über elliptische Kurven, ein Anhang über Folgen und Reihen reeller Zahlen sowie eine Tabelle mit lateinischen Redewendungen (die im Text nicht verwendet werden). Im Sinne der heute üblichen "corporate identity" wird auch laufend auf die anderen Bücher des Autors verwiesen.

Jedem, der algebraische Zahlentheorie lernen möchte, kann der Rezensent nur empfehlen, eines der vielen guten Lehrbücher zu wählen, nicht jedoch dieses.

G. Lettl (Graz)

A. Reznikov, N. Schappacher (eds.): Regulators in Analysis, Geometry and Number Theory. (Progress in Mathematics, Vol. 171.) Birkhäuser Verlag, Boston, Basel, Berlin, 2000, XV+324 S. ISBN 0-8176-4115-7, 3-7643-4115-7 H/b sfr 128,–.

Das vorliegende Buch ist das Resultat eines Workshops desselben Titels, der 1996 an der Hebrew University in Jerusalem abgehalten wurde. In 11 Einzelbeiträgen wird ein Überblick über den Stand des Wissens in der Theorie der Regulatoren gegeben. Ausgehend von der analytischen Klassenzahlformel, durch die ein Zusammenhang zwischen dem Wert der ζ-Funktion eines Zahlkörpers an der Stelle 0 und dem Regulator des Zahlkörpers hergestellt wird, kam die natürliche Frage auf, ob man die Werte von arithmetisch oder geometrisch definierten L-Reihen an ganzzahligen Stellen durch arithmetisch oder geometrisch definierte Größen beschreiben kann. In diesem Zusammenhang sind etwa die Beilinsonschen Vermutungen oder auch die Vermutung von Birch und Swinnerton-Dyer zu nennen.

Zum Inhalt:

D. Blasius and J. Rogawski: Cohomology of Congruence Subgroups of $SU(2,1)^p$ and Hodge Cycles on Some Special Complex Hyperbolic Surfaces

S. Bloch: Remarks on Elliptic Motives

C. Deninger: On Dynamical Systems and Their Possible Significance for Arithmetic Geometry

H. Esnault: Algebraic Differential Characters

H. Gangl: Some Computations in Weight 4 Motivic Complexes

A. B. Goncharov: Geometry of the Trilogarithm and the Motivic Lie Algebra of a Field

K. Köhler: Complex Analytic Torsion Forms for Torus Fibrations and Moduli Spaces

K. Künnemann and V. Maillot: Théorèmes de Lefschetz et de Hodge arithmétiques pour les variétés admettant une décomposition cellulaire

A. Levin: Polylogarithmic Currents on Abelian Varieties

J. Lott: Secondary Analytic Indices

J. Wildeshaus: Variations of Hodge-de Rham Structure and Elliptic Modular Units.

P. Grabner (Graz)

P. Ribenboim: Fermat's Last Theorem for Amateurs. Springer, New York u.a., 1999, XIII+407 S., ISBN 0-387-98508-5 H/b DM 79,–.

Der Verfasser hat 1979 das Buch '13 Lectures on Fermat's Last Theorem' veröffentlicht, das eine sehr gute Darstellung des berühmten Fermatschen Problems (des „großen Fermat") gibt und großen Anklang gefunden hat. Damals war jenes Problem noch nicht gelöst, das erfolgte erst durch A. Wiles. Diese Tatsache wurde dann auch von der Boulevardpresse groß herausgebracht.

Was will man mehr? Was ist der Unterschied gegenüber den '13 Lectures' ? Zunächst einmal hat das erste Buch in fast prophetischer Weise auf den Zusammenhang des Fermatschen Problems mit den elliptischen Kurven aufmerksam gemacht, indem der Autor auf die Arbeit von Y. Hellegouarch von 1972 hingewiesen und die Arbeit von G. Frey zitiert hat. Es gibt bisher keine durchsichtige Darstellung des Beweises von A. Wiles. Selbst ein Berufsmathematiker, wenn er nicht ein Spezialist in der Zahlentheorie und in der Theorie der Modulfunktionen ist und die zugehörige Literatur genau studiert hat, wird sich schwer tun. Hier will nun der Verfasser eine Brücke schlagen. Das vorliegende Buch gibt uns die Grundlagen, die für das Verständnis des Beweises notwendig sind.

Das Buch gliedert sich in elf Kapitel und zwei Anhänge. Die Kapitel werden noch durch sogenannte „Zwischenspiele" ergänzt. Die Darstellung ist meisterhaft, gut verständlich und bringt viel gut brauchbare Mathematik auf bequeme Weise global und lokal auch für jene, die sich für das Fermatsche Problem als zu speziell nicht interessieren. Auf die Arbeiten von G. Frey, K.A. Ribet und A. Wiles, den Lösern des Fermatproblems, wird nicht vergessen. Die Lektüre dieses Buches kann nur empfohlen werden. Die Ausstattung des Buches mit einem Bild von Fermat und dem des Verfassers ist nobel. Die Literatur ist ausführlich angegeben.

E. Hlawka (Wien)

P. Ribenboim: My Numbers, My Friends. Popular Lectures on Number Theory. Springer, New York u.a., 2000, XI+375 S. ISBN 0-387-98911-0 P/b DM 79,–.

Ein hübsches Buch über sehr subjektiv ausgewählte Gebiete der Zahlentheorie mit einem völlig irreführenden Untertitel. Behandelt werden rekurrente Folgen, binäre quadratische Formen, Primzahlformeln, Potenzen, irrationale und transzendente Zahlen, oft nur durch Auflisten von Ergebnissen; soweit aber Herleitungen gegeben werden, erfordern sie umfangreiches zahlentheoretisches Grundwissen, angefangen vom Quadratischen Reziprozitätsgesetz bis zur Riemannschen ζ-Funktion. Wenn auf der hinteren Umschlagklappe von "einfacher Sprache, zugänglich für jeden mathematisch Interessierten" steht, so gleicht dies der Behauptung, dass die Klaviersonaten von Beethoven einfach und zugänglich für jeden musisch Interessierten sind.

Die meisten Kapitel stellen unveränderte oder nur leicht veränderte Fassungen von alten Vorträgen dar. Das verursacht manchmal Wiederholungen, manchmal großzügiges Übergehen von neuen Ergebnissen. So werden z.B. Unterfälle des Großen Fermat behandelt, ohne auch nur in einer Fußnote zu sagen, dass der Satz bewiesen ist.

Auf die Beispiele wurde beim Korrekturlesen nicht viel Sorgfalt verwendet. So muss es auf Seite 3 heissen 0,1,1,2, ... anstelle von 0,1,2, ... und auf Seite 176 sollte 4,8,9, ... anstelle von 4,5,9, ... stehen.
Empfehlen würde ich das Buch niemandem, der zu seinem Vergnügen etwas über Zahlen erfahren möchte, wohl aber Fachleuten, die sich mit den genannten Gebieten näher beschäftigen und die dann auch mit den Literaturangeben gut bedient sind.

W. Knödel (Stuttgart)

P. Ribenboim: The Theory of Classical Valuations. (Springer Monographs in Mathematics.) Springer u.a., 1999, XI+403 S. ISBN 0-387-98525-5 H/b DM 129,–.

This is a self-contained exposition of the theory of valuations of fields which starts with the valuations of the field of rational numbers and moves up all the way to Krull valuations. In between, there are gems that are hard to find elsewhere, such as the treatment of algebraic extensions of infinite degree over the rationals and their valuations. The specialist will also derive pleasure from the excellent exposition of the theory of decomposition, inertia, and ramification. For the novice, the author offers a well-paced introduction to valuation theory. Armed with this material, the reader will be well prepared for further studies, for instance in the theory of algebraic number fields and function fields. The book is written in the careful and lively style for which the author is known.

H. Niederreiter (Wien)

M. Waldschmidt: Diophantine Approximation on Linear Algebraic Groups. Transcendence Properties of the Exponential Function in Several Variables. (Grundlehren der mathematischen Wissenschaften 326.) Springer, Berlin u.a., 2000, XXIII+633 S. ISBN 3-540-66785-7 H/b DM 169,–.

Bei der vorliegenden Monographie handelt es sich um eine gediegene Darstellung der neuesten Entwicklungen auf dem Gebiet der diophantischen Approximation. Da die diophantische Approximation gegenwärtig ein äußerst rasch wachsendes und umfangreiches Gebiet darstellt, beschränkt sich der Autor auf die Transzendenztheorie mit dem Schwerpunkt: kommutative lineare Gruppen. Ein zentrales Resultat dieses Buches ist der Lineare Untergruppensatz, der in einer qualitativen und in einer quantitativen Form gezeigt wird. Die qualitative Version gibt eine untere Schranke für die Dimension eines Teilraumes von $\mathbb{C}^d$, der von Punkten aufgespannt wird, deren Koordinaten entweder algebraische Zahlen oder Logarithmen von algebraischen Zahlen sind. Die quantitative Fassung beschäftigt sich mit simultaner Approximation solcher Punkte. Obwohl das Buch keine Abelschen Varietäten oder nicht-lineare algebraische Gruppen behandelt, werden immer wieder Ausblicke dorthin gegeben. Zentrales technisches Hilfsmittel in der vorliegenden Monographie ist M. Laurents Methode der Interpolationsdeterminanten.

Nach einer historischen Einführung werden die klassischen Transzendenzsätze von Gelfond-Schneider und Hermite-Lindemann gegeben. Danach kommen Sätze über Höhen algebraischer Zahlen und das Kriterium von Schneider-Lang. Der zweite Hauptteil des Buches ist den Nullstellenabschätzungen von D. Roy und Maßen für lineare Unabhängigkeit gewidmet. Der dritte Hauptteil ist mehrdimensionalen Problemen gewidmet, insbesondere einer entsprechenden Darstellung der Bakerschen Theorie der Linearformen von Logarithmen algebraischer Zahlen. Teil 4 behandelt den linearen Untergruppensatz und Teil 5 die simultane Approximation von Werten der Exponentialfunktion in mehreren Variablen.

Jeder Abschnitt enthält Übungsaufgaben mit Hinweisen und viele historische Kommentare. Die Entstehungsgeschichte des Buches geht über zehn Jahre zurück und viele Abschnitte basieren auf Vorlesungen und Vortragsreihen des Autors. Das Buch ist äußerst liebevoll geschrieben und sollte in keiner mathematischen Bibliothek fehlen. Es kann auch als Grundlage für Seminare und Spezialvorlesungen empfohlen werden.

R. Tichy (Graz)

Geometrie, Topologie — Geometry, Topology — Géométrie, topologie

E. Casas-Alvero: Singularities of Plane Curves. (London Mathematical Society Lecture Note Series 276.) Cambridge University Press, 2000, XV+345 S. ISBN 0-521-78959-1 P/b £ 29,95.

Eine häufige Antwort auf eine beliebige mathematische Frage über Kurven, gestellt an einen spanischen algebraischen Geometer, lautet: Fragen Sie doch Eduardo Casas. Nun legt Casas (s)ein Buch über ebene algebraische Kurven vor und belegt damit, dass er zu Recht als Experte auf diesem Gebiet gilt.

Knapp 15 Jahre nach Brieskorn-Knörrers Klassiker „Ebene algebraische Kurven“ ein Buch, das als gute Ergänzung und Fortsetzung dient und eher dem Weierstrassschen Blickpunkt folgt, geprägt von formalen oder konvergenten Potenzreihen, die das Studium der lokalen Geometrie durchdringen.

So werden en detail die Newton-Puiseux-Entwicklung samt Konstruktionsverfahren, die analytischen Zweige einer Kurve und ihre Parametrisierung, die Aufblasung und die Auflösung von ebenen Kurven besprochen. Wie überhaupt das Buch um die unendlich benachbarten Punkte eines singulären Punktes einer Kurve kreist, sozusagen als Ausgangs- und Endpunkt vieler Betrachtungen.

In diesem Zusammenhang beschreibt Casas ausführlich die charakteristischen Exponenten, die zugehörige Kettenbruchentwicklung, angenäherte Wurzeln, Polarkurven und Äquisingularität. Im letzten Abschnitt wird die Bewertungstheorie am Beispiel der ebenen Kurven exemplarisch und mit Klassifikation vorgeführt. Im Anhang zeigt Casas, wie die lokalen Techniken zu globalen Ergebnissen führen, dies im Zusammenhang mit der Jacobi-Vermutung in Dimension zwei, dem Satz von Jung und van der Kulk und den Resultaten von Abhyankar und Moh.

Abgerundet wird dieses empfehlenswerte Buch durch eine Reihe von Übungsaufgaben und einer an die hundert Zitate umfassenden Literaturliste.

H. Hauser (Innsbruck)

J. H. Conway, N. J. A; Sloane: Sphere Packings, Lattices and Groups. Third Edition. With Additional Contributions by E. Bannai, R. E. Borcherds, J. Leech, S. P. Norton, A. M. Odlyzko, R. A. Parker, L. Queen and B. B. Venkov. With 112 Illustrations. (Grundlehren der mathematischen Wissenschaften 290.) Springer, New York u.a., 1999, LXXIV+703 S., ISBN 0-387-98585-9 H/b DM 139,–.

Es liegt die dritte Auflage eines Klassikers vor. Wie die Autoren im Vorwort höchst richtig erwähnen, wendet sich das Buch an alle, welche an endlichen Gruppen oder quadratischen Formen oder Geometrie der Zahlen oder Kombinatorik interessiert sind.

Ich rücke zwei Kommentare zur ersten Auflage ein:

> *Gian-Carlo Rota:* "This is the best survey of the best work in one of the best fields of combinatorics, written by the best people. It will make the best reading by the best students interested in the best mathematics that is now going on."
>
> *G. David Forney:* "What is so often said in book reviews happens to be precisely true here: this book will be an essential reference for anyone whose work involves lattices for the foreseeable future. There is nothing else like it, and as an intellectual accomplishment it is breathtaking."

Typische Themen sind: Kugelpackungen, Überdeckungsprobleme, das kissing number problem und das quantizing problem, welches mit „kleinen" Voronoi-Diagrammen zu tun hat.

Diese Auflage enthält nun mehr als 800 Literaturzitate und einen Bericht von 60 Seiten, welcher Neuerungen beschreibt, die seit den früheren Auflagen erzielt worden sind.

Der folgende Kommentar von *N. Sloane* ist allerdings zu berücksichtigen:

> "A page was omitted. Unfortunately the publisher omitted a crucial page from the Preface to the Third Edition. The following material should be inserted between pages xx and xxi. (...)"

Diesen Kommentar findet man auf: *http://www. research. att. com/∼njas/doc/splag.html*

Es ist auch interessant, darauf hinzuweisen, daß wohl Conway und Sloane die hauptsächlichen Autoren sind, aber in kleineren Kapiteln auch andere Autoren zu Wort kommen, etwa Andrew Odlyzko, der ja vor kurzem in einem Interview von M. Drmota ausführlich in den IMN gewürdigt worden ist.

Ich erspare mir ein abschließendes Lob; das hieße Eulen nach Athen tragen.

H. Prodinger (Johannesburg)

A. F. Costa, B. Gómez: Arabesques and Geometry. (Springer ViedoMATH.) Springer, Berlin, Heidelberg 1999. ISBN 3-540-92640-2 VHS/PAL DM 58,–.

The authors use details of the buildings of the Alhambra in Grenada as motivation for studies of ornaments in plane Euclidean geometry. It is a good idea to connect the outstanding masterpiece of Islamic architecture with geometric considerations. The video tape (20 minutes) explains the different types of plane displacements. Later on it shows the structure of the 17 ornament groups of the Euclidean plane using motives from the Alhambra. The tape is amazing and serves well as an

introduction into the field of displacements in the Euclidean plane. A leaflet helps to follow the presented topics and gives hints for further literature in this field. The only shortcoming of the video: it mentions that there are 17 different ornament groups, but not all of them are actually displayed as motives from the Alhambra.

O. Röschel (Graz)

Goldman W. M: Complex Hyperbolic Geometry. (Oxford Mathematical Monographs.) Clarendon Press, Oxford, 1999, XX+316 S., ISBN 0-19-853793-X H/b £ 65,–.

The book offers a comprehensive treatment of the geometry of the complex hyperbolic space and its boundary. Its subject is closely connected with a number of branches of mathematics, such as Riemannian geometry, complex analysis, harmonic analysis. The goal of the work is — according to the author — to be a "user's guide" to complex hyperbolic geometry and to stimulate research in this field. The book consists of nine chapters which will shortly be described.

Ch. I reviews complex one-dimensional geometry.

Ch. II contains the algebraic and geometric background needed to understand the following.

Ch. III develops the geometry of the unit ball in $\mathbb{C}^n$, its projective model and the trigonometry of complex hyperbolic space.

Ch. IV introduces the second projective model of H^n_C, the so called Siegel domain; also the elements of Heisenberg geometry are presented.

Ch. V develops the theory of bisectors and spinal spheres.

Ch. VI pursues the automorphisms of H^n_C.

Ch. VII treats three important numerical invariants, Cartan's angular invariant, the complex cross-ratio and one concerning real geodesics and complex hyperplanes.

Ch. VIII discusses the general theory of extors in P^n_C which generalize metric bisectors in complex hyperbolic and elliptic geometry.

Ch. IX finally treats the theory of intersections of bisectors in H^n_C.

This book will be of good use for everybody who intends to penetrate into complex hyperbolic geometry and who also plans to work in this area.

F. J. Schnitzer (Leoben)

G. Kalai, G. M. Ziegler (Eds.): Polytopes — Combinatorics and Computation. (DMV Seminar, Band 29.) Birkhäuser, Basel, Boston, Berlin, 2000, VI+225 S. ISBN 3-7643-6351-7 P/b sFr 48,–.

Der vorliegende Band enthält die Vorträge des DMV-Seminars "Polytopes and Optimization" in Oberwolfach im November 1997, sowie weitere Arbeiten. In den einzelnen Artikeln werden zahlreiche Beziehungen der Polytoptheorie zur Algorithmentheorie, zur Linearen und Kombinatorischen Optimierung, zur Computational Geometry, zum Wissenschaftlichen Rechnen und zur Diskreten Geometrie dargestellt. Solche Beziehungen stellen einen Motor für die moderne Polytoptheorie dar, zeigen aber auch die Kraft, mit der die Konvexgeometrie in andere Gebiete hinein wirkt. Das Buch ist daher sowohl Konvexgeometern als auch Mathematikern, die zu den anderen genannten Gebieten arbeiten, sehr zu empfehlen.

P. Gruber (Wien)

N. Steenrod: The Topology of Fibre Bundles. (Princeton Landmarks in Mathematics.) Princeton University Press, Princeton, New Jersey, 1999, VIII+229 S., ISBN 0-691-00548-6 P/b $ 19,95.

This reedition of Steenrod's seminal work on Fibre Bundles (originally published in 1950) is a must in any mathematician's library. Although admittedly the discipline has evolved since 1950, Steenrod's book is still a good introduction to the subject. Frequent comments and explanations of the underlying motivations allow the reader to get a valuable overall feeling for the theory.

When the book was written, the author found no extensive treatments of homotopy groups or cohomology theory in book form. Hence, the author felt the need to include surveys of both matters. In retrospective, this gives the book the added value of being (reasonably) self-contained.

The book is structured in three parts. The first presents the general theory, while the second and third focus on homotopy and cohomology respectively. The first part is of special historical value, since it contains Steenrod's intuitions about the very concept of fibre bundle.

C. Alos-Ferrer (Wien)

Chuanming Zong: Sphere Packings. Edited by J. Talbot. With 32 Illustrations. (Undergraduate Texts in Mathematics.) Springer, New York u.a., 1999, XIII+241 S. ISBN 0-387-98794-0 H/b DM 79,–.

Zweifellos gehören Fragestellungen über Packungen und Überdeckungen, insbesondere aus Kugeln aufgebauten, zu den interessantesten, aber auch schwierigsten mathematischen Problemen. Zumeist relativ einfach formulierbar, aber dann oft jahrhundertelang als ungelöstes Problem weitergegeben. Die typischen Beweismethoden zeigen Querverbindungen zu nahezu allen mathematischen Disziplinen — aber gerade die typischen Methoden versagen oft im Einzelfall, und nur

unübliche und unerwartete Gedankensprünge führen zum Ziel, wie alle jene schon erfahren haben, die sich mit unterschiedlichen Packungs- und Überdeckungsproblemen auseinandergesetzt haben.

Das vorliegende Lehrbuch versucht, die gesamte einschlägige Literatur, beginnend mit der Gregory-Newton-Fragestellung bis hin zum letzten Forschungsstand, nicht nur anzuführen, sondern zu vernetzen und die optimalen Beweisideen anzugeben. Dieses hochgesteckte Ziel kann wirklich als erreicht angesehen werden. Der Text ist wegen des außerordentlich großen Umfanges der behandelten Fragestellungen zwar sehr knapp, aber trotzdem sehr verständlich gehalten.

Wegen der Komplexität und extremen Vielfalt der behandelten Probleme können hier nur die Kapitelüberschriften angeführt werden: 1. The Gregory-Newton Problem and Kepler's Conjecture, 2. Positive Definite Quadratic Forms and Lattice Sphere Packings, 3. Lower Bounds for the Packing Densities of Spheres, 4. Lower Bounds for the Blocking Numbers and the Kissing Numbers of Spheres, 5. Sphere Packings Constructed from Codes, 6. Upper Bounds for the Packing Densities and the Kissing Numbers of Spheres I, 7. Upper Bounds for the Packing Densities and the Kissing Numbers of Spheres II, 8. Upper Bounds for the Packing Densities and the Kissing Numbers of Spheres III, 9. The Kissing Numbers of Spheres in Eigth and Twenty-Four Dimensions, 10. Multiple Sphere Packings, 11. Holes in Sphere Packings, 12. Problems of Blocking Light Rays, 13. Finite Sphere Packings. Den Abschluß bildet eine wirklich umfaßende Bibliographie. Insgesamt liegt meines Erachtens *das* aktuelle einschlägige Standardwerk vor.

P. Paukowitsch (Wien)

Funktionalanalysis — Functional Analysis — Analyse fonctionnelle

B. Bollobás: Linear Analysis. An introductory course. Second edition. (Cambridge Mathematical Textbooks.) Cambridge University Press, 1999, XI+240 S., ISBN 0-521-65577-3 P/b £ 16,95.

Das 15. Kapitel (Fixpunktsätze) wird eingeleitet: "*In Chapter 7 we proved the doyen of fixed-point theorems, the contraction-mapping theorem. In this chapter we shall prove some considerably more complicated results: Brouwer's fixed-point theorem and some of its consequences. It is customary to deduce Brouwer's theorem from some standard results in algebraic topology, but we shall present a self-contained combinatorial proof.*" Dieses Zitat zeigt die Originalität dieses Werkes über „Funktionalanalysis im engeren Sinn", deren "*core the study of normed spaces together with linear functionals and operators on them*" ist. Da der Autor tieferliegende Anwendungen aus der Theorie der partiellen Differentialgleichungen oder der nichtkommutativen, harmonischen Analysis zur „Funktionalanalysis im weiteren Sinn" rechnet, fehlen solche in vorliegender Darstellung.

Die Originalität zeigt sich auch an vielen anderen Details: Das Buch beginnt mit einem Kapitel "basic inequalities" - dem Kern der funktionalanalytischen Stetigkeitsaussagen. In Kapitel 3 wird die Fortsetzbarkeit linearer Funktionale bewiesen, die nach oben durch konvexe und nach unten durch konkave Funktionale beschränkt sind (Theorem 11, p. 53). Ein letztes Beispiel: "*Let us return to the opening statement of this chapter: the isomorphic classification of finite-dimensional normed spaces is trivial, with two spaces being isomorphic if and only if they have the same dimension. Based on this, one could come to the hasty verdict that there is nothing to finite-dimensional normed spaces: they are not worth studying. As it happens, this would not only be a hasty verdict but it would also be utterly incorrect. There are a great many important and interesting questions, only the isomorphic classification is not one of them. All these questions, many of which are still open, concern the metric properties of the finite-dimensional normed spaces.*" Neben der Stoffauswahl ist auch die Darstellung bestechend und führt zu Ergebnissen bis 1997. Zum Vorteil des Lesers schreckt der Autor nicht vor Wiederholungen zurück: "*Most of these facts have already been proved, but for the sake of convenience we prove them again.*"

Eine glänzende Darstellung der elementaren Funktionalanalysis, die ich uneingeschränkt empfehle.

N. Ortner (Innsbruck)

S. Helgason: The Radon Transform. Second Edition. (Progress in Mathematics, Vol 5.) Birkhäuser, Boston, Basel, Berlin, 1999, XII+188 S. ISBN 0-8176-4109-2, 3-7643-4109-2 H/b öS 643,–.

Die 2. Auflage dieses Standardwerks über die Radontransformation zeichnet sich nicht nur durch verbesserte Ausstattung (typographisch, Figuren) oder Beseitigung kleinerer Fehler aus, sondern auch durch eine inhaltliche Weiterentwicklung: der frühere Appendix „Distributionen und Riesz-Potentiale" wurde zu einem eigenen Kapitel V am Ende des Buches ausgebaut. Neu und klarer (als in der 1. Auflage) sind beispielsweise: die Behandlung der Wellengleichung, die Funktransformierte, die Darstellung des Poissonintegrals als Radontransformierte oder der Abschnitt: „Maximal Tori and Minimal Spheres in Compact Symmetric Spaces" in Chapter III: The Radon Transform on Two-Point Homogeneous Spaces. Daß auch die interessanten bibliographischen Notizen an jedem Kapitelende bis 1998 aktualisiert wurden, sei am Rande bemerkt. Auch wenn fraglich ist, ob ich zu diesem Urteil berechtigt bin: Helgasons Buch ist ein Meisterwerk über die Radontransformation.

N. Ortner (Innsbruck)

H. Radjavi, P. Rosenthal: Simultaneous Triangularization. (Universitext.) Springer, New York u.a., 2000, XII+318 S. ISBN 0-387-98467-4 H/b, ISBN 0-387-98466-6 P/b DM 69,–.

A collection of linear transformations is called simultaneously triangularizable if there is a basis for the vector space such that all transformations in the collection have upper triangular matrix representations with respect to that basis. Starting from that definition, the book gives an overview of the classical results and most recent developments of triangularizabilty in both the finite and infinite dimensional case. The first five chapters are devoted to the finite dimensional results, starting from the very basics; only some prerequisites on linear algebra and functional analysis are necessary. Chapter six contains basic material for the infinite dimensional case. In the following chapters, algebras and semigroups of compact operators are investigated for triangularizability. The last chapter is on bounded operators. Each chapter ends with a short section commenting original research results and suggestions for further reading. The book contains interesting material for a graduate course on matrices.

M. Husty (Innsbruck)

Dynamische Systeme —Dynamical Systems — Systèmes dynamiques

F. Blanchard, A. Maass, A. Nogueira (Eds.): Topics in Symbolic Dynamics and Applications. (London Mathematical Society Lecture Note Series 279.) Cambridge University Press, 2000, XVI+245 S. ISBN 0-521-79660-1 P/b £ 24,95.

Der Band aus der Lecture Notes-Serie der LMS enthält acht Artikel von jeweils rund 30 Seiten. Diese Artikel fassen in teilweise überblicksartiger Form Kurse zusammen, welche im Rahmen einer Sommerschule im Jänner 1997 in Temuco (Chile) von verschiedenen Autoren gegeben wurden. Insgesamt entsteht dadurch ein sehr schöner Einblick in das Gebiet, der zwar keine Monographie ersetzen möchte, der aber einen Einstieg geben kann, dem mancher Leser gegenüber einem umfassenden Lehrbuch vielleicht den Vorzug geben mag.

Es kommen verschiedene Aspekte zur Sprache, welche die Verbindungen zu anderen Gebieten aufzeigen wie z.B. Automatentheorie, Zahlentheorie, Ergodentheorie, Graphentheorie, Algebra, Stochastische Prozesse und Ramsey-Theorie.

Es fehlt der Platz, um mit mehr als einer Aufzählung der einzelnen Artikel zu schließen: *Sequences of Low Complexity: Automatic and Sturmian Sequences* von V. Berthé, *Substitution Subshifts and Bratteli Diagrams* von B. Host, *Algebraic Aspects of Symbolic Dynamics* von M. Boyle, *Dynamics of $\mathbb{Z}^d$-actions on Markov subgroups* von B. Kitchens, *Asymptotic Laws for Symbolic Dynamical*

Systems von Z. Coelho, *Ergodic Theory and Diophantine Problems* von V. Bergelson, *Number Representation and Finite Automata* von Ch. Frougny und *A Note on the Topological Classification of Lorenz Maps on the Interval* von R. Labarca.

R. Winkler (Wien)

R. Feres: Dynamical Systems and Semisimple Groups: An Introduction. (Cambridge tracts in mathematics 126.) Cambridge University Press, 1998, XVI+ 245 S. ISBN 0-521-59162-7 H/b £ 35,–.

Dynamical systems are generated by a group G (often $\mathbb{R}$ on $\mathbb{Z}$) representing the time parameter. The action of G on the states describes the evolution of the system. The global properties and invariants of this group are basic items of systems theory. In this context, G is often a semisimple Lie group (or a discrete subgroup thereof). Therefore, the author first develops the theory of semisimple Lie group in an (essentially) self-contained form, including the Cartan and Iwasawa decompositions. Differential geometry is a ubiquitous tool. The main developments in this theory are due to Margulis and Zimmer, and they are presented as well. Also, topological prerequisites and ergodic theory are treated as far as they are needed for the context. Most of these results are interpreted in the context of dynamical systems. Many exercises are given; they play an essential part in this book. This text might well become a standard one for the interplay between Lie theory and dynamical systems.

G. Pilz (Linz)

M. Foreman, A. S. Kechris, A. Louveau, B. Weiss: Descriptive Set Theory and Dynamical Systems. (London Mathematical Society Lecture Note Series 277.) Cambridge University Press, 2000, 291 S. ISBN 0-521-78644-4 P/b £ 27,95.

Der Band aus der Lecture Notes-Serie der LMS geht auf ein internationales Workshop am CIRM in Marseille/Luminy im Juli 1996 zurück, welches den tiefgreifenden Beziehungen zwischen Dynamischen Systemen und Deskriptiver Mengenlehre gewidmet war. Der Band (insgesamt knapp 300 Seiten) enthält neun Übersichtsartikel von jeweils meist ca. 20-40 Seiten Länge und von verschiedenen Autoren. Der besondere Reiz der Artikel besteht unter anderem darin, dass der Leser einen angemessenen Zugang zu wichtigen aktuellen Forschungsströmungen bekommt, ohne sich durch zu Spezielles (wie oft in Originalarbeiten) oder zu Ausführliches (wie oft in Monographien) durchackern zu müssen.

Besonders hervorzuheben ist der Artikel *A Descriptive View of Ergodic Theory* von M. Foreman. Nicht nur wegen seiner überdurchschnittlichen Länge von über 80 Seiten stellt er ein Kernstück des Bandes dar. Er macht es sich auch zur Aufgabe, sowohl Dynamiker als auch Mengentheoretiker in das jeweils andere Gebiet einzuführen und die Relevanz der Gebiete füreinander zu verdeutlichen.

Was die anderen, durchwegs deutlich kürzeren Artikel betrifft, müssen wir uns mit einer Aufzählung begnügen: *An Overview of Infinite Ergodic Theory* von J. Aaronson; *The Multifarious Poincaré Recurrence Theorem* von V. Bergelson; *Groups of Automorphisms of a Measure Space and Weak Equivalence of Cocycles* von S. Bezuglyi; *Structure Theory as a Tool in Topological Dynamics* von E. Glasner; *Orbit Properties of Pseudo-homeomorphism Groups of a Perfect Polish Space and their Cocycles* von V. Ya. Golodets, V. M. Kulagin und S. D. Sinel'shchikov; *Descriptive Dynamics* von A. S. Kechris; *Polish Groupoids* von A. B. Ramsay und *A Survey of Generic Dynamics* von B. Weiss.

R. Winkler (Wien)

P. Le Calvez: Dynamical Properties of Diffeomorphisms of the Annulus and of the Torus. Translated by Ph. Mazaud. (SMF/AMS Texts and Monographs, Vol. 4 — Astérisque, Numéro 204, 1991.) American Mathematical Society, Providence, Rhode Island — Société Mathématique de France, 2000, IX+105 S. ISBN 0-8218-1943-7 P/b $ 21,–.

Das etwa 100 Seiten umfassende Büchlein wurde erstmals 1991 in französischer Sprache veröffentlicht. Bei der neuen Ausgabe handelt es sich um eine Übersetzung.

Zunächst stehen die sogenannten twist-Abbildungen f auf zweidimensionalen Mannigfaltigkeiten im Zentrum des Interesses. Sie sind dadurch gekennzeichnet, dass bei festgehaltener ersten Komponente x für $f(x,y) = (x',y')$ die Zuordnung $y \mapsto x'$ einen Diffeomorphismus liefert und ebenso für f^{-1}. Nach der Präsentation einführender Beispiele und grundlegender Begriffe (Rotationszahl) werden die Theorien von Aubry-Mather und von Birkhoff für den flächenerhaltenden Fall dargestellt. Die erste arbeitet mit Methoden der Variationsrechnung, die zweite hat topologischen Charakter.

Schließlich werden allgemeinere Situationen behandelt, indem teils auf die Voraussetzung der Flächenerhaltung, teils (im zweiten Teil) auf die „twist"-Eigenschaft verzichtet wird.

Ein relativ spezielles Thema wird auf überschaubarem Raum auf sehr ansprechende Weise dargestellt und kann deshalb dennoch als sehr geeignete Einführung nicht nur in die behandelten Themen, sondern in wesentliche Teile der Theorie Dynamischer Systeme angesehen werden.

R. Winkler (Wien)

S. Morosawa, Y. Nishimura, M. Taniguchi, T. Ueda: Holomorphic Dynamics. (Cambridge Studies in Advanced Mathematics 66.) Cambridge University Press, Cambridge, 2000, XI+338 S. ISBN 0-521-66258-3 H/b £ 45,–.

Das Buch gibt eine Einführung in die Dynamik holomorpher Funktionen. Gerade durch die Vergabe des Fields-Preises an *C. McMullen* hat dieses Gebiet wieder neue Aufmerksamkeit auf sich gezogen. Nach einer ausführlichen Behandlung der klassischen Theorie der Iteration von Polynomfunktionen, ganzer Funktionen und rationaler Funktionen wird die Analogie zwischen gewissen Aspekten der holomorphen Dynamik und Resultaten aus der Theorie der Kleinschen Gruppen dargestellt. Danach werden in mehreren Kapiteln die dynamischen Eigenschaften multivariater holomorpher Funktionen diskutiert.

Insgesamt handelt es sich bei dem Buch um eine sehr ausführliche und umfängliche Einführung in das aktuelle Forschungsgebiet der holomorphen Dynamik, die bis zu neuesten Resultaten vordringt.

P. Grabner (Graz)

M. Zinsmeister: Thermodynamic Formalism and Holomorphic Dynamical Systems. Translated by C. G. Anderson. (SMF/AMS Texts and Monographs, Vol. 2 — Panoramas et Synthèses, Numéro 4, 1996.) American Mathematical Society, Providence, Rhode Island — Société Mathématique de France, 2000, IX+82 S. ISBN 0-8218-1948-8 P/b $ 19,–.

Das vorliegende Buch ist eine Übersetzung des französischen Originals ins Englische durch die American Mathematical Society. Nach Angabe des Autors war es seine Intention, den Themodynamischen Formalismus und seine Anwendungen besonders in der holomorphen Dynamik darzustellen. In der Einleitung werden acht (!) Bücher erwähnt, die dieser Darstellung zugrunde liegen. Daraus ist schon ersichtlich, daß es sich bei diesem 82-seitigen Buch um eine sehr komprimierte Darstellung des Themenkreises handeln muß. Tatsächlich verlangt es einige Vorkenntnisse aus der Ergodentheorie und der holomorphen Dynamik und ist daher nur zur weiterführenden Lektüre und besonders als „Appetitanreger“ geeignet.

P. Grabner (Graz)

Differentialgleichungen — Differential Equations — Équations différentielles

P. Knabner, L. Angermann: Numerik partieller Differentialgleichungen. Eine anwendungsorientierte Einführung. Springer, Berlin u.a., 2000, XI+365 S. ISBN 3-540-66231-6 P/b DM 59,90.

Die inhaltlichen Schwerpunkte dieses Lehrbuches sind wie folgt zu charakterisieren:

- Eine ausführliche und mathematisch sauber begründete Darstellung der Methode der Finiten Elemente (für stationäre und zeitabhängige Probleme);
- Iterationsverfahren für große lineare und nichtlineare Gleichungssysteme (dies umfaßt auch eine Darstellung von Multilevel-Verfahren im FE-Kontext);
- Diskretisierungsverfahren für konvektionsdominierte Probleme.

Natürlich wird auch Basiswissen über Finite-Differenzen-Verfahren vermittelt.

Darüber hinaus wird in einem einleitenden Kapitel beispielhaft der Modellierungsprozess (besser: eine Hierarchie von Modellen) aus einem bestimmten Anwendungsgebiet detailgetreu beschrieben (nämlich zu Transport- und Reaktionsprozessen in porösen Medien). Der nicht einschlägig vorgebildete Leser ist hier sehr gefordert – aber vielleicht war das so beabsichtigt.

Die Darstellung ist recht ausführlich geraten; insgesamt findet der Vortragende Materialien für eine bis zu 2×3-stündige Vorlesung. Es werden auch Themen behandelt, die ansonsten in Lehrbüchern kaum zu finden sind, etwa a-posteriori Fehlerabschätzungen und ihre Bedeutung für die adaptive Gittergenerierung bei FE-Verfahren, oder Finite-Volumen-Verfahren.

Viele der behandelten Themen (etwa optimale Fehlerabschätzungen beim FE-Verfahren oder die Konstruktion von a-posteriori-Fehlerschätzern) stellen hohe didaktische Anforderungen, wenn man nicht nur die reinen Formalismen, sondern auch ein tatsächliches Verständnis vermitteln will. Diesem Anspruch wird das Buch (wie viele andere) – bei allen sonstigen Qualitäten – nicht hundertprozentig gerecht.

Gesamtbeurteilung: Bei der Vorbereitung einer einschlägigen Lehrveranstaltung sollte das Buch seinen festen Platz auf dem Schreibtisch haben.

W. Auzinger (Wien)

V. V. Mityushev, S. V. Rogosin: Constructive Methods for Linear and Nonlinear Boundary Value Problems for Analytic Functions. Theory and Applications. (Chapman & Hall/CRC Monographs and Surveys in Pure and Applied Mathematics 108.) Chapman & Hall/CRC, Boca Raton, London, New York, Washington, D. C., 2000, XI+283 S. ISBN 1-584-88057-0 H/b £ 49,–.

In Standardvorlesungen über partielle Differentialgleichungen werden als Prototypen elliptischer Randwertprobleme im allgemeinen Dirichlet- und Neumannproblem für Operatoren 2. Ordnung behandelt. Es wäre ein Irrtum zu glauben, damit seien die wichtigsten Randwertprobleme gelöst: mechanische Probleme mit Einschlüssen oder Rissen, Probleme in geschichteten Medien ("composite media", Transmission, Beugung) führen - bereits in 2 Raumdimensionen - zu „gemischten" Randwertproblemen, die mit singulären Integralgleichungen vom „Cauchy-Hauptwerttyp" oder mit der Wiener-Hopf-Methode gelöst werden können. Diese können ihrerseits als Spezialfälle des Hilbertschen und des Riemannschen Randwertproblems betrachtet werden. Ein lesenswerter Überblick ist zu finden in: E. Meister: Das Riemannsche Randwertproblem. In: Überblicke Mathematik VI, hrsg. von D. Laugwitz, p. 113-178, 1973. Ausführlicher ist das Lehrbuch: Randwertaufgaben der Funktionentheorie (Teubner, 1983 - Besprechung in IMN Nr. 139/140, 1985, p. 85) von E. Meister.

Im vorliegenden Buch wird unter dem (linearen) Riemannschen Problem verstanden: Gesucht ist eine im Inneren (oder Äußeren) einer Jordankurve C holomorphe Funktion F, so daß für gegebene, komplexwertige Funktionen f und g auf C gilt: $\Re(fF) = g$. Das Buch untersucht systematisch die Art der Gebiete sowie Bedingungen an f und g, so daß Lösungen existieren, weiters explizite Lösungsverfahren sowie Verallgemeinerungen, insbesondere nichtlineare, um damit Anwendungen auf elastisch-plastische Probleme zu ermöglichen. Die Darstellung ist umfassend (die Bibliographie umfaßt 295 Titel) und bezieht insbesondere Forschungsergebnisse der letzten 20 Jahre ein. Der einzige Nachteil ist das katastrophale Englisch.

N. Ortner (Innsbruck)

B. Scarpellini: Stability, instability, and direct integrals. (Chapman & Hall/CRC Research Notes in Mathematics Series 402.) Chapman & Hall/CRC, Boca Raton, London, New York, Washington, D. C., 1999, XII+346 S., ISBN 0-8493-0685-X P/b $ 74,95.

In this book, stability of periodic equilibria of partial differential equations in two-dimensional unbounded (plate-like) domains is investigated. Three types of systems are considered, described by reaction diffusion equations, Navier Stokes equations and Boussinesq equations.

The main focus is not to prove stability but to prove the principle of linearized instability, that is to show that the physical (or observed) instability of a periodic

equilibrium coincides with the instability under a certain perturbation in a proper function space. Of course, such a result is strongly influenced by the choice of the underlying function space, a fact which is carefully discussed. As a consequence also proper spectral formulas are supplied.

In order to prove the principle of linearized instability, the concept of direct integrals of Hilbert spaces is used which was first introduced by von Neumann. By the way, these direct integrals have also been used with great success in the treatment of the Schrödinger equation with periodic potential. Formulas found there are extended to the non-selfadjoint case treated in this book.

A careful exposition is given which, however, is restricted to the abstract functional analytic treatment since no applications are considered.

H. Troger (Wien)

Wirtschaftsmathematik — Mathematics of Economy — Économétrie

W. Eichholz, E. Vilkner: Taschenbuch der Wirtschaftsmathematik. 2., neubearbeitete und erweiterte Auflage. Mit 55 Abbildungen, 208 Beispielen und zahlreichen Tabellen. Fachbuchverlag Leipzig im Carl Hanser Verlag, 2000, 284 S. ISBN 3-446-21469-0 P/b DM 29,80.

Das Buch sieht sich als Brücke zwischen den mathematischen Verfahren und ihren Anwendungen zur Lösung von Problemen aus dem Wirtschaftsleben. Die in der vorliegenden zweiten Auflage behandelten Themen sind die Lineare Algebra und Optimierung (Kap. 2), Funktionen, Folgen, Reihen (Kap. 3), Grundzüge der Finanzmathematik (Kap. 4), Funktionen einer und mehrerer Veränderlicher (Kap. 5, 6), Numerische Verfahren (Kap. 7), Statistik (Kap. 8) und Ausgewählte Probleme des OR (Kap. 9). Das Buch unterscheidet sich von einer reinen Formelsammlung durch viele Beispiele, die die Anwendung der behandelten mathematischen Verfahren illustrieren. Auffallend ist auch, daß manche Kapitel nur sehr skizzenhaft ausgeführt sind, während andere Abschnitte einen hohen Detaillierungsgrad aufweisen. Besonderes Gewicht haben die lineare Algebra und die Statistik. Erweiterungen gegenüber der ersten Auflage betreffen u.a. Eigenwerte, Interpolationsverfahren und Lagerhaltungsprobleme. Vor allem Studierenden der Wirtschaftswissenschaften kann das Taschenbuch als nützlicher Begleiter empfohlen werden.

P. Hackl (Wien)

H. Milbrodt, M. Helbig: Mathematische Methoden der Personenversicherung. Walter de Gruyter, Berlin, New York, 1999, XI+654 S. ISBN 3-11-014226-0 H/b DM 134,–.

Das Buch bietet (dem stochastisch vorgebildetem Mathematiker) eine weitreichende Einfhrung in das Gebiet der Personenversicherung und beleuchtet in eindrucksvoller Weise, welch schöne und anspruchsvolle Mathematik in diesem Bereich zur Anwendung kommen kann.

Insbesodere wird deutlich gemacht, daß die „abstrakte“ Theorie der stochastischen (Sprung-) Prozesse in natürlicher Weise ihre Entsprechungen beispielsweise in der Modellierung der kumulativen Versicherungsleistungen eines Unternehmens findet. Die benötigten mathematischen Hilfsmittel (abzüglich Wahrscheinlichkeitstheorie) werden im Text entwickelt, es gibt weiters einen Anhang für einige in Standardvorlesungen über Wahrscheinlichkeitstheorie selten behandelte Themen.

Das Buch wird mit Sicherheit alle, die bis heute die Versicherungsmathematik für die Metaphysik der geometrischen Reihe gehalten haben, überraschen, und diejenigen, die schon lange ein anspruchsvolles Einführungsbuch in diese Thematik in deutscher Sprache gesucht haben, außerordentlich erfreuen.

G. Leobacher (Linz)

R. Seydel: Einführung in die numerische Berechnung von Finanz-Derivaten. Computational Finance. Mit 34 Abbildungen, 4 Tabellen und 36 Übungsaufgaben. Springer, Berlin u.a., 2000, XII+154 S. ISBN 3-540-66889-6 P/b DM 49,90.

Das vorliegende Buch ist für Leser mit Vorkenntnissen aus der Finanzmathematik, speziell mit Vorkenntnissen aus dem Bereich der Optionsbewertung eine sehr gut lesbare, elementare Einführung in den Einsatz numerischer Methoden auf diesem Gebiet. Das Buch dient sicher nicht als Einführung in die Finanzmathematik und in die Theorie der Optionsbewertung als solcher. Zwar sind die grundlegenden Prinzipien angeführt, sie werden aber nur sporadisch und nicht im Detail erläutert. Ansonsten werden kaum weitere Vorkenntnisse beim Leser vorausgesetzt. So wird etwa die Bedeutung und die Anwendung stochastischer Integrale und stochastischer Differentialgleichungen unter Vermeidung sämtlicher technischer Details soweit erklärt, als es zur numerischen Behandlung in diskreter Form notwendig ist. Es werden weiters in kurzer, bündiger und sehr gut verständlicher Form alle benötigten numerischen Hilfsmittel zur Verfügung gestellt. Natürlich wird auch bei den numerischen Methoden nicht auf tiefere Behandlung, etwa auf gute Fehlerabschätzungen Wert gelegt, sondern das Buch gibt auch hier lediglich eine Einführung in die grundlegendsten numerischen Methoden.

Das Buch wird somit für einen Leser, der sich bereits mit numerischen Anwendungen in der Finanzmathematik beschäftigt hat, sicher zuwenig an neuer Information erhalten. Es ist aber ohne Zweifel empfehlenswert als begleitendes Buch

zu einer Vorlesung oder zu einem Seminar über numerische Methoden in der Finanzmathematik, oder aber für Anwender und Entwickler finanzmathematischer Software mit Kenntnissen aus der Theorie der Optionsbewertung.

Zum Inhalt: Nach einem ersten Kapitel, in dem in kurzen Paragraphen die nötigsten Informationen über Optionen, partielle Differentialgleichungen, stochastische Prozesse, stochastische Differentialgleichungen und den Ito-Calculus gegeben werden, folgt ein Kapitel über die numerische Berechnung von Zahlen nach vorgegebenen Verteilungen. Dieses Kapitel enthält auch Methoden zur effizienten Erzeugung von Pseudo-Zufallszahlen und zur Erzeugung von niedrig-diskrepanten Punktmengen für den Einsatz in diversen Monte Carlo-Methoden. Im folgenden Kapitel werden Methoden (stochastische Taylorentwicklungen, Monte Carlo-Simulation) zur numerischen Lösung stochastischer Differentialgleichungen angegeben. In Kapitel 4 werden Finite-Differenzen-Methoden auf die Bewertung europäischer und auch amerikanischer Optionen angewendet. Im letzten Kapitel werden schließlich Finite-Element-Methoden eingeführt und zur Optionsbewertung verwendet.

G. Larcher (Linz)

Mathematische Physik — Mathematical Physics — Physique mathématique

J. J. Callahan: The Geometry of Spacetime. An Introduction to Special and General Relativity. With 218 Illustrations. (Undergraduate Texts in Mathematics.) Springer, New York, Berlin, Heidelberg, Barcelona, Hong Kong, London, Milan, Paris, Singapore, Tokyo, 2000, XVI+451 S. ISBN 0-387-98641-3 H/b DM 98,–.

Mit diesem Buch liegt eine physikalisch und geometrisch gut motivierende und argumentierende, aber selbst unter Berücksichtigung des Reihentitels mathematisch ziemlich elementare Einführung in die beiden Relativitätstheorien vor. (So werden z.B. in Abschnitt 2.2 Hyperbelfunktionen erklärt.) Der Zugang zu den allgemein-relativistischen Gleichungen des Schwerefeldes über Gezeiteneffekte ist einleuchtend und ansprechend, und alle geometrischen Überlegungen werden durch zahlreiche Skizzen erläutert. Es fehlt allerdings fast jeder Versuch, dem Leser Wege zu einer differentialgeometrisch anspruchsvolleren Sicht zu weisen, und sei es nur durch entsprechende Bemerkungen mit passenden Schrifttumshinweisen in einem Anhang. So ist dieses Buch vor allem für Leser empfehlenswert, deren Erwartungen durch den ersten Satz dieser Besprechung umrissen sind.

W. Bulla (Graz)

J. Dittrich, P. Exner, M. Tater (eds.): Mathematical Results in Quantum Mechanics. QMath7 Conference, Prague, June 22–26, 1998. (Operator Theory, Advances and Applications, Vol. 108.) Birkhäuser, Basel, Boston, Berlin, 1999, X+393 S., ISBN 3-7643-6097-6, 0-8176-6097-6 H/b öS 1373,–.

Dieser Konferenzbericht enthält Beiträge, die sich grob in zwei Gruppen aufteilen lassen: einerseits solche, die sich mit Themen aus der Theorie meist selbstadjungierter Operatoren in Hilberträumen befassen, die durch Fragestellungen aus der Quantenmechanik motiviert sind, unter ihnen etliche mit Spektraltheorie. Die andere Gruppe enthält Beiträge zu konkreten mathematischen Einzelproblemen der Quantenmechanik, wobei fast nur Schrödingeroperatoren betrachtet werden. Der Tagungsband bietet einen notwendigerweise selektiven, aber insgesamt dennoch guten Überblick über Ergebnisse und offene Fragen auf dem erwähnten Gebiet.

W. Bulla (Graz)

R. A. Minlos: Introduction to Mathematical Statistical Physics. (University Lecture Series, Vol. 19.) American Mathematical Society, Providence, Rhode Island, 2000, VII+103 S. ISBN 0-8218-1337-4 P/b $ 24,–.

Das Werk mit dem Titel von weitgespannter Bedeutung ist einem bestimmten Zugang zum Problem des thermodynamischen Limes gewidmet, also dem Übergang zu räumlich immer ausgedehnteren Systemen bei festgehaltenen intensiven Größen. Und zwar werden Bedingungen dafür angegeben, unter denen dieser Übergang nicht mit den wahrscheinlichkeitstheoretischen Mittelwerten von Messgrößen, sondern mit den Wahrscheinlichkeitsmaßen selbst ausgeführt werden kann, die die Zustände in der statistischen Mechanik (SM) beschreiben; dabei wird im Rahmen der sogenannten Pirogov-Sinai-Theorie auch ein Zugang zur Beschreibung von Phasenübergängen erläutert. Die Behandlung beschränkt sich auf die klassische SM, im Hauptteil des Buches außerdem auf Gittermodelle. Das konkrete Auftreten mehrerer Phasen wird nur im Zweidimensionalen untersucht. Das vorliegende Werk, das von Literatur- und Sachverzeichnis abgeschlossen wird, kann als überschaubarer Einstieg in diesen bekanntermaßen schwierigen Problemkreis empfohlen werden.

W. Bulla (Graz)

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

M. Bramson, R. Durrett (Eds.): Perplexing Problems in Probability. Festschrift in Honor of Harry Kesten. (Progress in Probability, Vol 44.) Birkhäuser, Boston, Basel, Berlin, 1999, X+398 S. ISBN 0-8176-4093-2, 3-7643-4093-2 H/b öS 1154,–.

Dies ist eine Festschrift, die Harry *Kesten* gewidmet ist, um 40 Jahre beeindruckender Forschungstätigkeit in der Wahrscheinlichkeitstheorie zu ehren. In der Tat hat Kesten zu vielen Gebieten der Wahrscheinlichkeitstheorie wichtige Beiträge geliefert. Mit seiner Dissertation hat er die Theorie der Irrfahrten auf diskreten Gruppen begründet. In jungen Jahren hat er sich übrigens auch mit Kettenbrüchen und Gleichverteilung modulo 1 befasst. Mit Furstenberg hat Kesten das Studium von Produkten von Zufallsmatrizen initiiert. Besonderen Ruhm erntete Kesten auf dem Gebiet der Perkolation, wo er bewies, dass der kritische Koeffizient im zweidimensionalen Gitter $p_c = 1/2$ ist. Diese und viele weitere Höhepunkte der Forschung von Harry Kesten werden im ersten Artikel des Buches ("Harry Kesten's Publications - A Personal Perspective" von Rick Durrett) beleuchtet. Die weiteren 20 Artikel, alle von höchster Qualität, stammen von den bedeutendsten Forschern in diversen Gebieten der Wahrscheinlichkeitstheorie, zu denen auch Kesten selbst wichtige Inspiration gegeben hat. Hier die vollständige Liste:

"Lattice Trees, Percolation and Super-Brownian Motion" (G. Slade); "Percolation in $\infty + 1$ Dimensions at the Uniqueness Threshold" (R. H. Schonmann); "Inequalities and Entanglements for Percolation and Random-Cluster Models" (G. R. Grimmett); "From Greedy Lattice Animals to Euclidean First-Passage Percolation" (C. D. Howard and Ch. M. Newman); "Reverse Shapes in First-Passage Percolation and Related Growth Models" (J. Gravner and D. Griffeath); "Double Behaviour of Critical First-Passage Percolation" (Y. Zhang); "The van den Berg-Kesten-Reimer Inequality: A Review" (C. Borgs, J. T. Chayes, and T. Randall); "Large Scale Degrees and the Number of Spanning Clusters for the Uniform Spanning Tree" (I. Benjamini); "On the Absence of Phase Transition in the Monomer-Dimer Model" (J. van den Berg); "Loop-erased Random Walk" (G. Lawler); "Dominance of the Sum over the Maximum and Some New Classes of Stochastic Compactness" (P. S. Griffin and R. A. Maller); "Stability and Heavy Traffic Limits for Queueing Networks" (M. Bramson); "Rescaled Particle Systems Converging to Super-Brownian Motion" (T. Cox, R. Durrett, and E. A. Perkins); "The Hausdorff Measure of the Range of Super-Brownian Motion" (J-F. Le Gall); "Branching Random Walks on Finite Trees" (T. M. Liggett); "Toom's Stability Theorem in Continuous Time" (L. F. Gray); "The Role of Explicit Space in Plant Competition Models" (C. Neuhauser); "Large Deviations for Interacting

Particle Systems" (S. R. S. Varadhan); "The Gibbs Conditioning Principle for Markov Chains" (A. Meda and P. Ney).

W. Woess (Graz)

Jie Chen, A. K. Gupta: Parametric Statistical Change Point Analysis. Birkhäuser, Boston, Basel, Berlin, 2000, VIII+184 S. ISBN 0-8176-4169-6, 3-7643-4169-6 H/b sFr 108,–.

Das Buch behandelt nicht, wie man aus dem Titel schließen würde, statistische Aspekte der Strukturbruch-Analyse, sondern (asymptotiche) Eigenschaften von Teststatistiken, die in der Strukturbruch-Analyse Anwendung finden. Der Großteil des Buches geht von Folgen von normalverteilten uni- (Kap. 2) und multivariaten (Kap. 3) Zufallsvariablen aus und diskutiert asymptotische Eigenschaften von Teststatistiken für das Testen von Änderungen im Erwartungswert oder in der Varianz und von simultanen Änderungen dieser Parameter. Die Teststatistiken basieren jeweils auf dem Likelihood-Quotienten und auf Informationskriterien. Ein recht kurz gehaltenes Kapitel befaßt sich mit Strukturbrüchen bei Regressionsmodellen. Schließlich werden Verfahren für Folgen von gamma-, exponentialverteilten sowie von diskreten Zufallsvariablen behandelt.

Das weitgehend im Satz/Beweis-Stil vefaßte, von den Autoren als "research monograph" bezeichnete Buch zeichnet sich durch über viele Seiten gehende, detaillierte Beweise aus. Aspekte des Statistikers oder des Anwenders spielen kaum eine Rolle, obwohl die Autoren im Vorwort auf die praktische Relevanz der Strukturbruch-Analyse in verschiedenen Disziplinen extra hinweisen. Weitere Kritikpunkte: Die umfangreiche Literatur (im CIS werden zum Stichwort "change point" 35 Arbeiten aus dem Jahr 1998, 49 aus 1997, 46 aus 1996 angeführt) ist nur in sehr knapper Auswahl zitiert, von der neueren nur Arbeiten der Autoren. Im Vorwort wird eine "annotated bibliography" versprochen (im Umschlagtext sogar eine "comprehensive bibliography"); tatsächlich findet man keinerlei Kommentierung. Im Text werden Arbeiten zitiert, die in der Bibliographie nicht vorkommen und umgekehrt.

Das Buch verlangt ein fortgeschrittenes Niveau an mathematischer Vorbildung. Wegen der sonst kaum zugänglichen, detaillierten Darstellung der behandelten Teststatistiken und der entsprechenden Ableitungen kann das Buch zur Vervollständigung für Literaturbestände zur Strukturbruch-Analyse empfohlen werden.

P. Hackl (Wien)

M. E. Tarter: Statistical Curves and Parameters: Choosing an Appropriate Approach. A. K. Peters, Natick, Massachusetts, 2000, XIII+386 S. ISBN 1-56881-105-5 H/b $ 56,–.

Dieses Buch ist anders als übliche Bücher zur Statistik. Es kann nicht als eine Einführung empfohlen werden, obwohl es teilweise grundlegende Probleme der Statistik sehr breit behandelt. Der Autor schreibt im Vorwort, dass es als ,,graduate text and reference guide for researchers and students" gedacht ist. Er beschreibt Probleme der stochastischen Modelle für reale Phänomene, die auch für Leser mit statistischer Vorbildung interessant sind. Auch historische Bemerkungen bilden gelegentlich eine willkommene Abwechslung. Wie der Titel des Werkes angibt, spielen Dichte- und Verteilungsfunktionen die dominierende Rolle, wobei aber viele der wichtigsten Dichten als bekannt vorausgesetzt werden. Man kann das Buch als kritischen Ergänzungstext zur Statistik betrachten. Das Literaturverzeichnis ist interessant. Ein guter Index sowie ein ausführliches Symbolverzeichnis und die gute Druck- und Bindequalität, der die Qualität der Abbildungen leider nachhinkt, machen den Band zu einem außergewöhnlichen Statistikbuch.

R. Viertl (Wien)

Einführungen, Elementar- und Schulmathematik — Introductory, Elmentary and School Mathematics — Ouvrages introductoires, mathématiques élémentaires, enseignement

E. B. Burger, M. Starbird: The Heart of Mathematics. An invitation to effective thinking. Key College Puglishing, Emeryville, in cooperation with Springer, New York, 2000, XXV+646 S. ISBN 1-55953-407-9 H/b DM 130,–.

If people don't come up to mathematics, mathematics has to come up to them. This motto paraphrases the authors' intention, who not only undertake to make the stringent mathematical thinking accessible to the man in the street, but even try to train him and make him enthusiastic about it. The topics chosen to do this job may be found also in other books of this kind, perhaps not in this abundance: the fascination of numbers, the handling of the infinite, gems from geometry and topology, chaos and fractals etc. What makes the difference is the trendy fashioning and presentation: short units, a bunch of figures, illustrations and 3D-pictures, stories and jokes spread over the text, so called mindscapes which include exercises for solidifying ideas, problems for creating new ideas, links for working in groups and further challenges. A book which surely will appeal to a broad readership.

G. Kowol (Wien)

R. Hartshorne: Geometry: Euclid and Beyond. With 550 Illustrations. (Undergraduate Texts in Mathematics.) Springer, New York u.a., 2000, XI+526 S. ISBN 0-387-98650-2 H/b DM 98,–.

The present book is a beautiful introduction to geometry intended for undergraduate students by one of the leading experts in algebraic geometry. Usually geometry is one of the first courses a student entering university has to take. Hence it is particularly important to motivate and, at the same time, lead the student towards a modern formulation of the theory. Here the author has chosen to use Euclid's "Elements" as a touchstone provoking questions and further investigations. This is then used to rediscover modern geometry step by step. Topics include the theory of area (Hilbert's third problem), field extensions, non-Euclidean geometries, and the regular and semiregular polyhedra.

G. Teschl (Wien)

O. A. Ivanov: Easy as π?. An Introduction to Higher Mathematics. Translated by R. G. Burns. Springer, New York u.a., 1999, XVIII+187 S., ISBN 0-387-98521-2 P/b DM 58,–.

Hier liegt ein sehr bemerkenswertes Buch vor: der Autor versucht, zentrale mathematische Problemstellungen und Methoden aus nahezu allen mathematischen Disziplinen einem mathematisch bereits sehr gut ausgebildeten Leserkreis vom höheren Standpunkt, in vernetzter Form und ohne die für Studienanfänger natürlich notwendigen Detailschritte neuerlich vorzustellen. Konkret liegen dem Band langjährige Erfahrungen mit Lehrveranstaltungen für Lehramtstudenten knapp vor und nach dem Studienabschluß zugrunde; für einen kompletten Durchgang wird man wohl eine 5-stündige Semestereinheit benötigen. Die besondere Aufmerksamkeit des Autors dieser Zielgruppe gegenüber zeigt sich auch im sehr geschickten didaktischen Konzept: jeweils ausgehend von einfach formulierbaren, zweckmäßigen exemplarischen Beispielen wird auf die Vermittlung des für Mathematiklehrer nötigen, sowohl breiten als auch tiefen Verständnisses für mathematische Zusammenhänge und für die zentralen mathematischen Ideen hingearbeitet. Sehr viele Beispiele, zum überwiegenden Teil zumindest ansatzweise durchgerechnet, ermöglichen dem Leser das Vertrautwerden mit bzw. das Wiederholen der wesentlichen und universellen Grundprinzipien der modernen höheren Mathematik.

An Stelle einer Inhalsangabe muß die Aufzählung der Kapitelüberschriften genügen, eine dem Buch gerecht werdende detaillierte Aufzählung der außerordentlich vielen und vor allem unterschiedlichen Schwerpunkte würde den Besprechungsrahmen sprengen: 1. Induction, 2. Combinatorics, 3. Geometric Transformations, 4. Inequalities, 5. Sets, Equations, and Polynomials, 6. Graphs, 7. The Pigeonhole Principle, 8. The Quaternions, 9. The Derivative, 10. The Foundations of Analysis.

Wenn auch Vorlesungsskripten für Studenten die Basis dieses Buches bildeten, so liegt keineswegs ein triviales oder übliches Werk vor. Meines Erachtens können auch mathematische Profis diesen Band mit großem Gewinn — inhaltlicher und didaktischer Art — lesen!

P. Paukowitsch (Wien)

Jänich K: Lineare Algebra. Achte Auflage. Mit zahlreichen Abbildungen. (Springer-Lehrbuch.) Springer, Berlin u.a., 2000, XII+271 S. ISBN 3-540-66888-8 P/b DM 39,90.

In Mathematikerkreisen, vor allem bei an der Lehre nicht sonderlich interessierten Personen, werden sehr häufig Einführungstexte zu weitgehend standardisierten Lehrinhalten, insbesondere zur Linearen Algebra, als uninteressante und überflüssige Belastungen der Lehrbuchflut angesehen. Eine derartige negative Beurteilung ist bei dem vorliegenden Jänich-Band zur Linearen Algebra ganz sicher nicht angebracht! Sicherlich kommen nur die üblichen Inhalte vor; aber es kommt bei einem Lehrbuch für Studienanfänger vor allem eben auf das *wie* an (natürlich nicht nur bei dieser Zielgruppe)! Im Haupttext stellt der Autor das mathematisch Wesentliche dar, knapp und ohne zwar wichtige, den Anfänger aber zunächst irritierende Details. Solche finden sich im Nebentext, dazu kommen Erläuterungen und Motivationen zu den unterschiedlichen Typen von Routinebeweisen – die notwendige Routine muß der Erstsemestrige im Regelfall aber erst erwerben! Jedes Kapitel wird durch jeweils einen Zusatzabschnitt *für Physiker* und einen solchen *für Mathematiker* erweitert, dazu kommen Übungsaufgaben (wieder aufgeteilt für die beiden genannten Gruppen) sowie insgesamt 111 Testaufgaben (zu diesen finden sich am Buchende die Lösungen). Den Geometer erfreut natürlich die konsequente Grundhaltung des Autors, algebraische Sachverhalte zu geometrisieren und anhand sinnvoller Figuren zu visualisieren – auch ein didaktisches Prinzip, welches von manchen Mathematikern, als nicht den höheren Sphären entsprechend, abgelehnt wird.

Inhaltlich genügt hier die Aufzählung der Kapitelüberschriften: Mengen und Abbildungen, Vektorräume, Dimensionen, Lineare Abbildungen, Matrizenrechnung, die Determinante, Lineare Gleichungssysteme, Euklidische Vektorräume, Eigenwerte, die Hauptachsen-Transformation, Klassifikation von Matrizen. Natürlich kann einem das eine oder andere abgehen: so fehlen die Komplikationen beim Bearbeiten unendlichdimensionaler Vektorräume, und im Rahmen der Euklidischen Vektorräume werden nur die selbstadjungierten linearen Abbildungen, in der Matrixsprache also nur die symmetrischen Matrizen, behandelt. Diese kleinen Bemerkungen dienen aber nur dem Zweck, nicht in den Verdacht kommen zu wollen, nur positiv referiert zu haben! Nochmals: hier liegt ein inhaltlich und didaktisch wirklich vorbildliches Lehrbuch für Studenten und Dozenten vor — weitere Auflagen kommen sicher!

P. Paukowitsch (Wien)

B. Kisačanin: Mathematical Problems and Proofs. Plenum Press, New York, London, 1998, XIV+220 S. ISBN 0-306-45967-1 H/b $ 55,–.

Methodisch wendet sich der Autor an alle jene, welche ein mathematisches Buch in althergebrachter Weise mit Papier und Bleistift er- oder bearbeiten wollen (obwohl erst 32 jährig!). Inhaltlich werden die mathematischen Probleme und ihre Aufbereitung für interessierte Studienanfänger, eventuell auch für sehr begabte angehende Maturanten, sehr verständlich dargestellt und didaktisch vorzüglich vermittelt. Anhand von jeweils einfachen exemplarischen Aufgaben wird zunächst der problemlösende Aspekt der Mathematik vorgestellt und dann der weite Bogen zur Abstraktion gespannt: ausgehend von diesen Beispielen werden unterschiedliche und zum Teil sehr komplexe mathematische Lehrsätze formuliert und dann Wege zu eleganten Beweisen aufgezeigt. Insgesamt finden sich über 150 durchgerechnete Aufgaben und Lehrsätze.

Die folgenden vier mathematischen Disziplinen werden behandelt: Mengenlehre, Kombinatorik, Zahlentheorie und Geometrie. Der erste Abschnitt ist kurz gefaßt. Das zweite Kapitel widmet sich neben kombinatorischen Problemen weiters der Beweismethode, kombinatorische Identitäten zunächst zu erahnen, dann zu beweisen und schließlich zum eigentlichen Beweis einzusetzen. Der dritte Abschnitt führt über Primzahlaussagen und Teilbarkeitsalgorithmen zu den bekannten zahlentheoretischen Funktionen, zu Lösungssätzen von linearen Kongruenzen und Aussagen über pythagoräische Tripel. Der Geometrieteil enthält Aussagen über mit Dreiecken verknüpfte geometrische Objekte sowie Lehrsätze über Vierecke, insbesondere Sehnenvierecke. Zu den angeführten unterschiedlichen Beweismethoden gehört unter anderem auch der sachgemäße Einsatz komplexer Zahlen in der ebenen Geometrie. Vom Anhang scheinen mir besonders der Teil über die vollständige Induktion — wegen der vielen instruktiven Beispiele aus unterschiedlichen mathematischen Disziplinen — sowie der Teil über bekannte mathematische Konstanten und deren Herleitung von großem allgemeinen Interesse zu sein. Ein sehr interessantes und empfehlenswertes, ziemlich universelles Lehrbuch für Studenten und Dozenten!

P. Paukowitsch (Wien)

H. O. Peitgen, H. Jürgens, D. Saupe, E. Maletsky, T. Perciante: Fractals for the Classroom: Strategic Activities Volume Three. National Council of Teachers of Mathematics — Springer, New York u.a., 1999, XIV+107 S., ISBN 0-387-98420-8 P/b DM 49,–.

Dieser dritte und abschließende Band zur schüleradäquaten Aufbereitung von — entsprechend dem vorliegenden Konzept der Autoren mathematisch natürlich einfachen — Problemstellungen zur Fraktalen Geometrie enthält die Kapitel 7 und 8 des gesamten Werkes: *Iterierte Funktionensysteme* und *Geometrische Genetische Codes* lauten die Überschriften. Nach jeweils einer kurzen begrifflichen

Einführung werden anhand von sehr ausführlichen und im Unterricht direkt einsetzbaren Arbeitsblättern die mathematischen Inhalte, Testaufgaben und Taschenrechnerprogramme auf Schülerniveau präsentiert; die Lösungen finden sich am Buchende. Konkret nehmen die Autoren exemplarisch Bezug auf das Iterieren von affinen Abbildungen sowie auf das Bestimmen der Matrixbeschreibungen zu unterschiedlichen selbstähnlichen Vorgängen. Insgesamt liegt in der dreibändigen Serie ein sehr guter Beitrag zur experimentellen mathematischen Forschung auf Schülerniveau vor.

P. Paukowitsch (Wien)

J. L. Walker: Codes and Curves. (Student Mathematical Library — IAS/Park City Mathematical Subseries, Vol. 6.) American Mathematical Society, Providence, Rhode Island — Institut for Advanced Study, 2000, XII+66 S. ISBN 0-8218-2628-X P/b $ 15,–.

In dieser Serie werden Vortragsreihen publiziert, die – meist im Rahmen von Sommerschulen in Park City oder Princeton – Brücken zwischen mathematischen Forschern und high school-Lehrern oder Didaktikern schlagen sollen. Dadurch soll diesen Gruppen ermöglicht werden, einander über aktuelle Fragen und Probleme zu informieren und so mögliche Kontakte aufzubauen.

Im konkreten Fall bemüht sich die Autorin, einem mathematisch gebildeten, aber nicht spezialisierten Publikum einen Einblick in algebraisch-geometrische Codes zu vermitteln. Um verständlich zu bleiben, werden natürlich etliche Vereinfachungen in Kauf genommen, was bei Vorträgen durchaus angebracht ist. Im vorliegenden Büchlein wird der Leser auf 44 Seiten von den Grundbegriffen der linearen Codes samt Schranken für deren Kenngrößen bzw. von den Grundbegriffen ebener algebraischer Kurven (projektiver Abschluß, Geschlecht, Divisoren, Riemann-Roch) bis zu den dualen Goppa-Codes hingeführt. Auf weiteren 15 Seiten sind Grundbegriffe der Algebra (Gruppe, Ring, Körper, Homomorphismus) sowie der endlichen Körper zusammengefaßt.

Welchem Typ von Leser ein solches Büchlein ein erfolgreiches “Hineinschnuppern” in die algebraisch-geometrischen Codes ermöglicht, kann der Rezensent nicht beurteilen.

G. Lettl (Graz)

Internationale Mathematische Nachrichten

AMS-Preise 2001

Der "Steele Prize for Mathematical Exposition" wurde *Richard P. Stanley* (MIT) für sein zweibändiges Werk "Enumerative Combinatorics" verliehen. Den "Steele Prize for Seminal Contribution to Research" erhielten *Leslie F. Greencard* (Courant Institute, New York) und *Vladimir Rokhlin* (Yale University) für ihre Arbeit "A fast algorithm for particle simulations", J. Comput. Phys. **73** (1987), 325–348. *Harry Kesten* (Cornell University) wurde mit dem "Steele Prize for Lifetime Achievement" ausgezeichnet.

Den "Veblen Prize" erhielten *Jeff Cheeger* (Courant Institute, New York) für seine Arbeiten zur Differentialgeometrie, *Yakov Eliashberg* (Stanford University) für seine Arbeiten zur symplektischer und Kontakt-Geometrie und *Michael J. Hopkins* (MIT) für seine Arbeiten zur der Homptopietheorie.

Der "Satter Prize" wurde *Karen E. Smith* (University of Michigan) für ihre hervorragenden Arbeiten in der Kommutativen Algebra und *Sijue Wu* (University of Maryland) für die Lösung eines Problems der Wasserwellengleichung verliehen.

Den "Morgan Prize 2000" erhielt *Jacob Lurie*.

(Notices AMS)

Staudt-Preis

Don B. Zagier (Bonn) wurde für seine bahnbrechenden Arbeiten zur Zahlentheorie mit dem Staudt-Preis 2001 ausgezeichnet. Der mit DM 120.000,– dotierte Preis wurde 1991 erstmals vergeben und wird nur alle drei Jahre verliehen. Frühere Preisträger sind Hans Grauert, Stefan Hildebrandt und Martin Kneser.

(DMV-Mitteilungen)

Der 3ECM — Barcelona 2000

Wie die Zeit vergeht! Nach der Premiere in Paris (1992) und der zweiten Vorstellung in Budapest (1996) wurde nun in Barcelona schon der dritte ECM (European

Congress of Mathematics) abgehalten. Es wurde wiederum eine erfolgreiche Veranstaltung. Etwa 1200 Teilnehmer waren gekommen, besonders viele aus Spanien (natürlich) und aus Osteuropa, einige (nicht ganz ein Dutzend) auch aus Österreich, darunter Klaus Schmidt (invited speaker) und Bruno Buchberger (round table), aber kein (offizieller) Delegierter (für die Sitzungen).

Die Veranstalter haben offensichtlich mit viel Enthusiasmus – und einigem Erfolg – versucht, die Politik und die Öffentlichkeit auf den Kongress aufmerksam zu machen und für Mathematik zu werben. So wurden zum Beispiel in den Zügen der zum Kongresspalast führenden U-Bahn-Linien die besten Beiträge zum Plakatwettbewerb der EMS angebracht (die allerdings, soweit wir beobachten konnten, von den Fahrgästen weitgehend ignoriert wurden). Und an der Placa Espanya, einem der Verkehrsknoten von Barcelona – für die folgende Woche *unsere* Metrostation – wies ein riesiges Plakat (angebracht auf einem der venezianisch angehauchten Türme, die zur Prunkstraße zum Mont Juic leiten) auf den Kongress hin. Von dort ging es neben einem Spalier von Springbrunnen und vorbei an Messe- und weiteren Kongressbauten (teilweise Relikte der Weltaustellung 1929) zur Kongresshalle.

Es hat sich wieder erwiesen, daß es bei großen Kongressen sehr günstig ist, wenn sich alles – so wie hier – in einem einzigen Gebäude abspielt. Eine riesige Halle im Erdgeschoß war zentraler Treffpunkt. Sie beherbergte die Stände der großen Buchausstellung (wie immer ein Anziehungspunkt mit vielen Sonderangeboten, Katalogen und Ansichtsexemplaren von Zeitschriften), die Poster-Ausstellung, die zentrale Information und eine Boutique. Hier fanden die Kaffee-Pausen statt, hier wurden die Computer mit Internetanschluss ständig umlagert, (aber es gab etwas wenige Sitz- und Schreibgelegenheiten), hier wurde am Sonntag die Anmeldung flott erledigt, und von hier konnte man rasch in den darüberliegenden Saal für die Hauptvorträge und in die Seminarräume gelangen (leider hat eine solche Lösung – Mieten eines Kongressgebäudes – auch Nachteile: keine Bibliothek, kein Sekretariat und sie ist ziemlich teuer).

Die – wie üblich musikalisch umrahmte – Eröffnung begann mit interessierten und freundlichen Worten der zuständigen Politiker (teilweise mit mathematischen Background), die in den folgenden Statements der Veranstalter für sie vorbereiteten und an sie gerichteten Worte gingen dann trotzdem ins Leere: Die drei Vertreter der Politik eilten gleich nach ihren Ansprachen geschlossen zu weiteren Terminen. Bei der anschließenden Bekanntgabe der Preisträger (siehe Liste) war Jacques-Lious Lions ein engagierter Zeremonienmeister, der die Leistung der jungen Mathematiker lobte und bedauerte, dass es nicht genug Preise gebe, um sie alle zu würdigen, der aber dagegen den formellen Teil – die Verlesung der Würdigungen (citations) – nur merklich gelangweilt absolvierte.

Die Auswahl der Preisträger wurde übrigens in einem offenen Brief von dem *EMS Committee for Women and Mathematics* kritisiert: Die Herkunft der Preisträger ist regional unausgeglichen, die Verteilung der Themen erscheint einseitig und es

wurde keine einzige Frau ausgezeichnet. Auch in Anbetracht der Schwierigkeit jeder vergleichenden Würdigung von Leistungen in unterschiedlichen Gebieten erscheint diese Kritik nicht ganz unbegründet. Allerdings dürfte der Grund nicht in ungerechtfertigter Diskriminierung durch das Preiskomitee liegen, sondern an den Nomierungen.

Das gesellschaftliche Programm war etwas knapp bemessen: Ein Bankett in der Mittagspause nach der Eröffnung und ein Abend-Empfang im Palau Real – das war alles. Deshalb hatten wir zwar genügend Zeit (der Aufforderung des Bürgermeisters folgend), das abendliche und nächtliche Barcelona touristisch und kulinarisch zu erkunden, es bewirkte aber auch, dass sich der Kongress – nach einem dichten, wenig Zeit lassenden Tagesprogramm – jeden Abend auflöste, und die Teilnehmer sich über die Stadt verteilten.

Die Organisation verlief weitgehend reibungslos, wenn man von Warteschlangen beim Kaffee-Stand absieht, der nur in den kurzen Coffee-Breaks geöffnet war. Klagen gab es allerdings über das Reisebüro, dem die Abwicklung der Buchungen übertragen worden war, und das offenbar kräftige Aufschläge auf die Hotelpreise kassierte.

Natürlich wurde auch diesmal die bewährte und interessante Einrichtung der Roundtable-Gespräche fortgesetzt. Der Ablauf scheint einigermaßen institutionalisiert zu sein: Zunächst gibt es Statements, eher Kurzreferate, des Moderators und der drei Teilnehmer des Panels (viermal 15 Minuten, etwa die Hälfte der zur Verfügung stehenden Zeit), dann folgen Wortmeldungen aus dem Publikum, eventuell auch Antworten aus dem Panel. Ein brauchbarer Kompromiss, da eine echte Diskussion nur selten durchführbar ist.

Dem Motto des Jahres – 2000 ist das Jahr der Mathematik – entsprechend kam häufig das Bild unserer Disziplin in der Öffentlichkeit zur Sprache. Nicht nur beim einschlägigen Thema *How to Increase Public Awareness of Mathematics* (ein Gespräch, das von einem engagierten, mathematisch interessierten spanischen Wissenschaftsjournalisten vorbereitet worden war, der am Freitag vor Kongressbeginn plötzlich und unerwartet gestorben war), sondern wohl auch im parallel dazu abgehaltenen Roundtable *Mathematics Teaching at the Tertiary Level*, sowie bei der Frage *What is Mathematics Today?* und der Abschlussveranstaltung *Shaping the 21st Century*, bei der allerdings lange Zeit das Thema verfehlt wurde. Auch wenn die Situation von Land zu Land anders ist (in Frankreich zum Beispiel anscheinend merklich besser): Wirklich zufrieden mit dem Image der Mathematik und des Mathematikers zeigte sich niemand. Die Einstellung zur Mathematik – und darin herrschte im wesentlichen Übereinstimmung – wird vor allem in der Schule durch die Mathematik-Lehrer geformt: Also brauchen wir gut ausgebildete Lehrer, die selbst von Mathematik fasziniert sind. Konkrete Lösungsvorschläge blieben (erwartungsgemäß?) aus.

P.S.: Am Ende unseres Berichts aus Budapest vor vier Jahren stand der Hinweis auf den nächsten Kongress in Barcelona. Damals hatten wir über den Termin im

Juli – mitten in der Hauptsaison, zur heißesten Zeit – geklagt. Glücklicherweise wurden unsere Befürchtungen nicht wahr: Natürlich, es war Hauptsaison, aber – Petrus meinte es offensichtlich gut mit den Mathematikern – moderat warm. Auch das klimatisierte Kongress-Gebäude war kein Eiskasten, auch wenn manchmal etwas zu kühle Zugluft zu spüren war (dass unsere Furcht aber nicht unbegründet war, haben uns Berichte von Satelliten-Veranstaltungen in Spanien bewiesen, die in der Woche davor unter extremer Hitze gelitten hatten). Diesmal muss eine solche Vorschau übrigens unterbleiben, denn mangels Bewerbern konnte für 2004 noch kein Kongress-Ort bekanntgegeben werden.

EMS-Preisträger (je 6000 Euro) und die Titel ihrer Vorträge:

Semyon Alesker (Israel): Valuations on convex sets.

Raphael Cerf (Frankreich): Towards a microscopic theory of phase coexistence.

Dennis Gaitsgory (USA): Towards the geometrization of the local Langlands correspondence.

Emmanuel Grenier (Frankreich): Some results on the stability of boundary layers.

Dominic Joyce (Großbritannien): (war verhindert, Arbeitsgebiet Differentialgeometrie).

Vincent Lafforgue (Frankreich): Banach *KK*-theory and the Baum-Connes conjecture.

Michael McQuillan (Großbritannien): Non-Commutative Mori Theory.

Stefan Yu. Nemirovski (Russland): Geometric methods in complex analysis.

Paul Seidel (Frankreich): Vanishing cycles and mutation.

Wendelin Werner (Frankreich): Critical exponents, conformal invariance and planar Brownian motion.

Felix Klein Preis (5000 Euro):

David C. Dobson (USA): Modelling and optimal design of photonic structures.

Ferran Sunyer i Balaguer Preis

Juan-Pablo Ortega (Spanien) und *Tudor Ratiu* (Rumänien): Symmetry and singularities in conservative dynamics.

Hauptvorträge:

Andrew J. Wiles (Princeton): Galois representation and automorphic forms.

Robbert Dijkgraaf (Amsterdam): The mathematics of M-theory.

Carlos Simó (Barcelona): New families of solutions in N-body problems.

Marie-France Vignéras (Paris): Local Langlands correspondence for $GL(n, Q_p)$ modulo $l \neq p$.

Hendrik W. Lenstra (Berkeley and Leiden): Flags and lattice basis reduction.

Yves Meyer (Cachan): The role of oscillations in non-linear problems.

Hans Föllmer (Berlin): Probabilistic aspects of financial risk.

Olag Viro (Uppsala and St. Petersburg): Dequantization of real algebraic geometry on a logarithmic paper.

Yuri I. Manin (Bonn): Moduli, motives, mirrors.

Minisymposien:

Computer Algebra,
Curves over finite fields and codes,
Free boundary problems,
Mathematical finance: theory and practice,
Mathematics in modern genetics,
Quantum chaology,
Quantum computing,
String theory and M-theory,
Simplectic and contact geometry and Hamiltonian dynamics,
Wavelet applications in signal processing.

Round tables:

Mathematics teaching on the tertiary level,
The impact of mathematical research on industry and viceversa,
How to increase public awareness of mathematics,
What is mathematics today?
Building networks of cooperation in mathematics,
The impact of new technologies on mathematical research,
Shaping the 21th century.

Für weitere Informationen über die EMS (zum Beispiel genaueres Programm, Teilnehmerlisten, andere Aktivitäten) weisen wir auf die Homepage der EMS hin: *http://www.emis.de* .

Christa Binder und Peter Schmitt

MCM2001 — 3rd IMACS Seminar on Monte Carlo Methods
Sept. 10–14, 2001, Salzburg University

The purpose of this conference is to provide a forum for the presentation of recent advances in the analysis, implementation and applications of Monte Carlo simulation techniques and, in particular to stimulate the exchange of information between specialists in these areas. This conference is the third in a series, the previous meetings being held in Bruxelles and Varna.

For further information see *http://mcm2001.sbg.ac.at* or contact Karl Entacher, e-mail *mcm2001@cosy.sbg.ac.at* .

4th MATHMOD Vienna — 4th IMACS Symposium on Mathematical Modelling, February 5–7, 2003, Vienna

The international symposium on Mathematical Modelling will take place at Vienna University of Technology. Scientists and engineers using or developing models or interested in the development or application of various modelling tools will find an opportunity to present ideas, methods and results and discuss their experiences or problems with experts of various areas of specialisation.

The scope of the conference covers theoretic and applied aspects of the various types of mathematical modelling (equations of various types, automata, Petri nets, bond graphs, qualitative and fuzzy models, etc.) for systems of dynamic nature (deterministic, stochastic, continuous, discrete or hybrid with respect to time, etc.). Comparison of modelling approaches, model simplification, modelling uncertainties, port-based modelling and the impact of items such as these on problem solution, numerical techniques, validation, automation of modelling and software support for modelling, co-simulation, etc. will be discussed in special sessions as well as applications of modelling in control, design or analysis of systems in engineering and other fields of application.

For further information see *http://simtech.tuwien.ac.at/MATHMOD* or contact Prof. Inge Troch, e-mail *inge.troch@tuwien.ac.at* .

Travel Grants for Young Mathematicians to Attend the International Congress of Mathematicians

The International Mathematical Union will award travel grants to young mathematicians to help them to attend the ICM-2002, Beijing, China, August 20-28, 2002. The grants are intended for young mathematicians from developing countries (not necessarily members of IMU). Please notice that mathematicians from Eastern European countries, even those with strict monetary regulations, are not part of this program, but shall also be specially considered directly by the Local Organizing Committee.

The age-limit for the grantees is 35 years on the occasion of the Congress. The candidates should present evidence of research work at the post-doctoral level, and they should be able to benefit from the interaction with mathematicians from other countries attending the Congress.

In addition to the name and address of the candidate, including e-mail address and fax number when available, the applications should contain a brief curriculum vitae, including date of birth, plus a list of publications (papers published or definitively accepted for publication).

The Local Organizing Committee of the International Congress of Mathematicians will provide a special allowance to the grantees to cover their registration, board and lodging.

Applications for the travel grant may be sent directly to the Secretary of the Union. Applications may also be submitted through the National Committees for Mathematics, which in such a case will send all the relevant information about the candidates to the Secretary.

All applications should reach the Secretary by January 31, 2002:

Phillip A. Griffiths (Secretary)
Institute for Advanced Study
Einstein Drive, Princeton, NJ 08540, USA
Tel: (609) 734-8200
Fax: (609) 683-7605
e-mail *imu@ias.edu*

Summer School in "Symplectic Geometry", Paris, July 12–19, 2001

This school is devoted to the recent advances in the topology of symplectic varieties and their groups of symplectomorphisms. It is intended to Ph. D. students, post-docs and researchers in close fields.

It is the first of four summer schools organized by the Institut de mathematiques de Jussieu. It will propose to young researchers a synthetic view of the progresses in symplectic geometry and give them the opportunity of meeting the first specialists in the field.

For further information and registration see *http://www.math.jussieu.fr/geosym/* .

Nachrichten der Österreichischen Mathematischen Gesellschaft

Mitteilungen des ÖMG-Vorsitzenden

Wenn Sie Gelegenheit haben, die ÖMG-homepage *http://www.mat.univie.ac.at/∼oemg/Tagungen/2001/index.html* anzuklicken, finden Sie dort eine ständig wachsende, ausführliche Beschreibung des 15. ÖMG-Kongresses, der vom 17. bis 21. September 2001 an der Universität Wien stattfinden wird. Hier will ich nur auf einige Höhepunkte und Singularitäten eigens aufmerksam gemacht werden. Auf die diesmal besonders stattliche Liste der Hauptvorträge gehe ich dabei gar nicht ein – die Namen sprechen für sich! Auch das Ausflugsprogramm und die Minisymposien sind recht ambitioniert.

Unter den 17 Sektionen fällt eine etwas aus dem Rahmen: Sie ist nicht einem Fachgebiet wie etwa der Algebra oder der Differentialgeometrie gewidmet, sondern dem Erwin-Schrödinger-Institut (ESI). Damit greifen wir eine Idee der DMV-Kongresse auf. Dort wird jedes Jahr ein Institut (oder eine Forschungseinrichtung) gesondert und ausführlich präsentiert. Für unseren ersten Schritt in diese Richtung ist das ESI geradezu prädestiniert – es ist ein Lichtblick in der österreichischen Wissenschaftsszene, eine Neugründung, die sich rasch einen hervorragenden, weltweit beachteten Namen gemacht hat und jährlich hunderte von Besuchern anzieht. Durch die ungemein fruchtbare Zusammenarbeit von Mathematikern und Physikern, die schlanke Verwaltung und die häufigen, an der Weltspitze orientierten wissenschaftlichen Evaluationen wurde das ESI zu einer geradezu exemplarischen Einrichtung.

Am Abend des Eröffnungstages, dem 17. September (einem Montag), wird eine Wiener Vorlesung der Mathematik gewidmet sein. Diese prestigeträchtige und sehr großzügig beworbene Veranstaltungsreihe ist wohl das intellektuelle Flaggschiff der Stadt Wien und hat im Lauf der Jahre ein unverwechselbares Profil errungen. Der Titel der Vorlesung lautet: „Reine Kunst und Angewandte Mathematik“. Drei angewandte Mathematiker der Spitzenklasse, nämlich Neunzert, Bulirsch und Peitgen werden jeweils über Zusammenhänge mit der bildenden Kunst, der Literatur und der Musik referieren, woran sich hoffentlich lebhafte Diskussionen entzünden werden.

Auch zum Abschluss, am Freitag nachmittag, wird zur Diskussion gebeten. Wie schon im Vorjahr sollen Lehrer und Schüler über die neuen Berufsbilder in der

Mathematik informiert werden. Während aber beim letzten Mal die Vortragenden junge WissenschaftlerInnen waren, wird das Panel diesmal aus arrivierten Persönlichkeiten der Wirtschaft bestehen, die alle ihre Karriere mit dem Studium der Mathematik begonnen haben und nun bei führenden Industrieunternehmen, Banken und Versicherungen an leitenden Stellen tätig sind. Hoffentlich wird es auch diesmal wieder gelingen, ein zahlreiches junges Publikum anzulocken.

Mathematisch interessierten Schülerinnen und Schülern – und wohl auch einem weiteren Publikum – werden im kleinen Festsaal der Universität gleich zwei Ausstellungen geboten. Da ist einmal die von Robert Mischak und Gerd Baron veranstaltete „Jagd auf Zahlen und Figuren“, die im Lauf der letzten Jahre regelmäßig in Wien und anderen Landeshauptstädten präsentiert wurde und Schüler anregt, in einer Art Rätselrally ein Problem nach dem anderen in Teamarbeit zu knacken. Außerdem bieten wir, erstmals in Österreich, die Ausstellung „Mathematik zum Anfassen“, die unter der Leitung von Albrecht Beutelspacher in den lezten Jahren in Deutschland große Resonanz gefunden hat. (Beutelspacher ist dafür im Vorjahr mit dem Kommunikator-Preis ausgezeichnet worden, für besondere Verdienste um die Vermittlung von Wissenschaft). Übrigens werden einige der Objekte – so etwa die Riesenseifenhaut – in Wien einen festen Platz finden, und zwar im Kindermuseum Zoom, das ab Oktober im Museumsquartier zu besuchen sein wird.

Daneben wird im Arkadenhof der Universität während des Kongresses und noch einige Wochen danach eine weitere Ausstellung zu sehen sein. Sie heißt „Kalter Abschied aus Europa – der Exodus der Mathematik“ und befaßt sich mit den Leistungen und Schicksalen der Wiener MathematikerInnnen der Zwischenkriegszeit, von denen so viele emigrieren mussten. Die Mathematik dieser Zeit zeichnet sich ja nicht nur durch hervorragende Qualität aus, sondern auch durch ungewöhnlich enge Querverbindungen zu anderen Fächern, wie etwa der Philosophie, der Literatur, der Physik und den Wirtschaftswissenschaften. Damit arbeiten Universität und ÖMG ein besonders dramatische Kapitel der Vergangenheit auf. Einer der letzten Überlebenden der damals vertriebenen Mathematiker, Franz Alt, wird als Ehrengast an der Eröffnung teilnehmen. ”It feels like the crowning end of a long journey“, schreibt er uns dazu.

Bei der Vorbereitung dieser Ausstellung habe ich auch begonnen, mich mit jenen Emigranten zu befassen, die als ”second generation“ beschrieben werden – geboren in Wien, aber vertrieben, bevor sie hier ihr Studium beginnen konnten. Sowohl die Qualität als auch die Quantität dieser ”second generation“ sind überwältigend, und ich bin sicher, dass meine Liste noch längst nicht vollständig ist. Hier ist sie:

> J.M. Blatt, Peter Braunfeld, Erwin Trebitsch, Gertrude Ehrlich, Herbert Federer, Lisl Gaal, Felix Haas, Walter Karplus, Walter Kochen, Kurt Kreith, Walter Littman, Fritz Mautner, Hans Offenberger, Edgar Reich, Hans Reiter, Walter Rudin, Frank Spitzer, J.G. Schaeffer,

Hans Schneider, Binyamin Schwarz, Josef Silberstein, Theodor Sterling, Hans Weinberger und John Wermer.

Ich wäre dankbar für jede Hilfe bei der Vervollständigung dieser Liste.

Und ich hoffe zuversichtlich, Sie beim Kongress willkommen heißen zu können! Die Anmeldefrist läuft bis 30. Juni.

Karl Sigmund

Vorträge im Rahmen der ÖMG in Wien

18.–19. 1. 2001. Colloquium on Operator Theory and its Applications, in Honour of Israel Gohberg

M.A. Kaashoek (Amsterdam): A band method approach to a commutant lifting problem.

A. Böttcher (Chemnitz): The finite section method for Toeplitz operators – from Gohberg's pioneering work to the present.

D. Alpay (Beer Sheva): Some finite-dimensional backward shift-invariant subspaces in the ball and a related interpolation problem.

A. Ran (Amsterdam): How about stability?

I. Gohberg (Tel Aviv): Orthogonal systems and convolution operators.

M. Deistler (TU Wien): Identification of linear systems.

H. Bart (Rotterdam): Logarithmic residues in the Banach algebra generated by the compact operators and the identity.

G. Heinig (Kuweit): The Toeplitz-plus-Hankel structure from an algebraic view point.

V. Adamyan (Odessa): Principal minors of the perturbation determinat for groups of unitary operators.

B. Silbermann (Chemnitz): Functions of shifts and their discretizations.

A. Dijksma (Groningen): Factorization and basis properties od selfadjoint operator functions.

23. 3. 2001: Festkolloquium anläßlich des 60. Geburtstages von Inge Troch und Hans-Jörg Dirschmid

Jan C. Willems (Groningen): Modeling, Modularity and Moduls.

A. Prechtl (TU Wien): Physikalische Dimensionen mathematischer Begriffe.

K. Desoyer (TU Wien): Zur Optimierung der Querschnitte von Robotergliedern.

F. Rattay (TU Wien): Stochastische Resonanz — und was wir beim Hören mitbekommen.

F. Breitenecker (TU Wien): Simulation — quo vadis?

H. Langer (TU Wien): Lösungen der Riccati-Gleichung und indefinite Skalarprodukte.

Druckfehlerberichtigung

In den IMN 185 (Dez. 2000) wurde auf Seite 78 der Name *Franz Diboky* falsch abgedruckt.

Persönliches

Prof. *Heinz Engl* hat einen Ruf als *Dean of Science*, verbunden mit einer "tenured professorship", ans Rensselaer Polytechnic Institute (Troy, New York, USA) erhalten.

Prof. *Peter Gruber* wurde am 18. April 2001 das Ehrendoktorat der Universität Siegen verliehen.

Prof. *Otmar Scherzer* (Universität Bayreuth; früher Universität Linz, Institut für Industriemathematik), Förderungspreisträger der ÖMG und Träger des START-Preises, hat den Ruf auf ein Ordinariat für angewandte und computerorientierte Mathematik an der Universität Innsbruck angenommen.

Neue Mitglieder

Gernot Greschonig, Mag.rer.nat. — Sommerg. 3/23, A-1190 Wien. geb. 1971. 1999/2000 Vertragsass. Univ. Wien, seit Okt. 2000 Vertragsass. TU Wien. e-mail *gernot.greschonig@univie.ac.at*.

Wolfgang Hassler, Mag. Dr.rer.nat. — Mittergrabenweg 77, A-8010 Graz. geb. 1975. 1993 Matura, 1993–99 Hauptstudium Mathematik Univ. Graz, 1999/2000 Doktorat (Diss.: Faktorisierung in eindimensionalen Integritätsbereichen), Inst. f. Math. Univ. Graz. e-mail *Wolfgang.Hassler@kfunigraz.ac.at*.

Martin Predota, Dipl.Ing. — Ernst-Haeckel-Str. 46, A-8010 Graz. geb. 1974. 1999 Abschluß des Studiums Techn. Math. TU Graz, seit Okt. 2000 Angestellter am FWF-Projekt S8308-Mat, Arbeit an Diss. im Bereich Finanzmathematik bei Prof. R. Tichy. e-mail *predota@finanz.math.tu-graz.ac.at*.

Robert Resel, Mag.rer.nat. — Stromstr. 47/4/15, A-1200 Wien. geb. 1976. 1995–2001 Studium Math./P.P.P. Lehramt, Co-Autor von *Wege zur Mathematik* (gem.m. H.-C. Reichel), seit 1997 Tutor am Inst. f. Math. Univ. Wien, seit 2001 Doktoratsstudium. e-mail *a9502035@unet.univie.ac.at*.

Josef Schicho, Dr. — geb. 1964. 1982-95 Studium Math. Univ. Linz, 1992-97 Systemadministrator IKU Linz, seit 1997 Univ. Ass. IKU Linz, Institut RISC, Univ. Linz, A-4040 Linz. e-mail *schicho@risc.uni-linz.ac.at*.

Joachim Schwermer, Univ.-Prof. Dr. — geb. 1950. Universitätsprofessor am Inst. f. Math. Univ. Wien, Strudlhofg. 4, A-1090 Wien. e-mail *joachim.schwermer@univie.ac.at*.

Bernhard Spangl — Baumeisterg. 26/4/4, A-1160 Wien. geb. 1975. Seit 1994 Studium Techn. Math., TU Wien.

Karl Unterkofler, Univ. Doz., Dipl.-Ing., Dr. — geb. 1957. 1986 Diplom Techn. Physik, TU Graz, 1989 Doktorat Mathematische Physik TU Graz (bei W. Bulla), 1990-92 Schrödingerstipendiat Univ. of Missouri, Columbia, 2001 Habilitation Angewandte Mathematik an der TU Graz, derzeit Hochschullehrer für Mathematik an der FH-Vorarlberg, Achstr. 1, A-6850 Dornbirn. e-mail *karl.unterkofler@fh-vorarlberg.ac.at*.

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 2001:

K. Sigmund (Univ. Wien): Vorsitzender.
H. Engl (Univ. Linz): Stellvertretender Vorsitzender.
M. Drmota (TU Wien): Herausgeber der IMN.
W. Woess (TU Graz): Schriftführer.
P. Michor (Univ. Wien): Stellvertretender Schriftführer.
I. Troch (TU Wien): Kassierin.
W. Schachermayer (TU Wien): Stellvertretender Kassier.

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 (BMBWK Wien)
H.-C. Reichel (Univ. Wien): Vorsitzender der Didaktikkommission.
H. Sorger (Wien)
H. Stachel (TU Wien)
H. Strasser (WU Wien)
G. Teschl (Univ. Wien)
R. F. Tichy (TU Graz)
H. Troger (TU Wien)
H. K. Wolff (TU Wien)

Mitgliedsbeitrag:

Jahresbeitrag: 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.mat.univie.ac.at/∼oemg/