Théorie des nombres

computing. This book is aimed at undergraduate mathematics and computer science students interested in developing a feeling for what mathematics is all about, where mathematics can be helpful, and what kinds of questions mathematicians work on. The authors discuss a number of selected results and methods of discrete mathematics, mostly from the areas of combinatorics and graph theory, with a little number theory, probability and combinatorial geometry. Wherever possible, the authors use proofs and problem solving to help students understand the solutions to problems. In addition, there are numerous examples, figures, and exercises spread throughout the book.

Ordre, treillis

G. GIERZ, K.H. HOFMANN, K. KEIMEL, J.D. LAWSON, M.W. MISLOVE, D.S. SCOTT. — **Continuous lattices and domains.** — Encyclopedia of mathematics and its applications, vol. 93. — Un vol. relié, 16×24, de XXXVI, 591 p. — ISBN 0-521-80338-1. — Prix: £75.00. — Cambridge University Press, Cambridge, 2003.

Information content and programming semantics are just two of the applications of the mathematical concepts of order, continuity and domains. The authors develop the mathematical foundations of partially ordered sets with completeness properties of various degrees, in particular directed complete ordered sets and complete lattices. Uniquely, they focus on partially ordered sets that have an extra order relation, modelling the notion that one element 'finitely approximates' another, something closely related to intrinsic topologies linking order and topology. Extensive use is made of topological ideas, both by defining useful topologies on the structures themselves and by developing close connections with numerous aspects of topology. The theory so developed not only has applications to computer science but also within mathematics to such areas as analysis, the spectral theory of algebras and the theory of computability. This authoritative, comprehensive account of the subject will be essential for all those working in the area.

George GRÄTZER. — **General lattice theory.** — Second edition. — Un vol. broché, 17×24, de XIX, 663 p. — ISBN 3-7643-6996-5. — Prix: SFr. 118.00. — Birkhäuser, Basel, 2003.

In the present edition of this widely known monograph, the work has been significantly updated and expanded. It contains an extensive new bibliography of 530 items and has been supplemented by eight appendices authored by an exceptional group of experts. The first appendix, written by the author, briefly reviews developments in lattice theory, specifically, the major results of the last 20 years and solutions of the problems proposed in the first edition. The other subjects concern distributive lattices and duality (Brian A. Davey and Hilary A. Priestley), continuous geometries (Friedrich Wehrung), projective lattice geometries (Marcus Greferath and Stefan E. Schmidt), varieties (Peter Jipsen and Henry Rose), free lattices (Ralph Freese), formal concept analysis (Bernhard Ganter and Rudolf Wille), and congruence lattices (Thomas Schmidt in collaboration with the author).

Théorie des nombres

M.A. BENNETT, B.C. BERNDT, N. BOSTON, H.G. DIAMOND, A.J. HILDEBRAND, W. PHILIPP, (Editors). — **Number theory for the millennium.** — Trois vol. brochés, 16×23,5, de respectivement 461 p., 447 p., 450 p. — ISBN 1-56881-126-8 (vol. 1), 1-56881-146-2 (vol. 2), 1-56881-152-7 (vol. 3). — Prix: US$ 50.00. par volume. — A. K. Peters, Natick, Massachusetts, 2002.

These proceedings review some of the major number theory achievements of the 20th century. In addition to survey papers by invited speakers the volume contains numerous original

research papers, many of which will serve as a starting point for further work. This conference builds on a strong tradition of international meetings in number theory at the University of Illinois in Urbana. The timing at the turn of the century provided an opportunity to invite a large number of researchers and an incentive to solicit substantial contributions from their current work. The Millennium Conference on Number Theory was held May 21-26, 2000 on the campus of the University of Illinois at Urbana-Champaign. A total of 276 mathematicians from 30 countries were present at the meeting.

M.A. BENNETT, B.C. BERNDT, N. BOSTON, H.G. DIAMOND, A.J. HILDEBRAND, W. PHILIPP, (Editors). — **Surveys in number theory: papers from the Millenial Conference on Number Theory.** — Un vol. broché, 15,5×23, de VII, 363 p. — ISBN 1-56881-162-4. — Prix: US$ 30.00. — A.K. Peters, Natick, Massachusetts, 2003.

The Millenial Conference was held on May 21-26, 2000 on the campus of the University of Illinois at Urbana-Champaign. The proceedings of this conference, containing 72 papers based on lectures given at that conference, have been published separately in three volumes under the title *Number Theory for the Millennium.* The present volume contains fourteen of these papers which represent broad surveys of topics in number theory or related areas. Presented and compiled by a group of international experts, these papers provide a current view of the state of the art and an outlook into the future of number theory research.

Paul ERDŐS, János SURÁNYI. — **Topics in the theory of numbers.** — Undergraduate texts in mathematics. — Un vol. relié, 16×24, de XVIII, 287 p. — ISBN 0-387-95320-5. — Prix: €49.95. — Springer, New York, 2003.

This rather unique book is a guided tour through number theory. While most introductions to number theory provide a systematic and exhaustive treatment of the subject, the authors have chosen instead to illustrate the many varied subjects by associating recent discoveries, interesting methods, and unsolved problems. In particular, we read about combinatorial problems in number theory, a branch of mathematics co-founded and popularized by Paul Erdős. János Surányi's vast teaching experience successfully complements Paul Erdős's ability to initiate new directions of research by suggesting new problems and approaches.

Georges GRAS. — **Class field theory: from theory to practice.** — Springer monographs in mathematics. — Un vol. relié, 16×24, de XIII, 491 p. — ISBN 3-540-44133-6. — Prix: €79.95. — Springer, Berlin, 2003.

Global class field theory is a major achievement of algebraic number theory, based on the functorial properties of the reciprocity map and the existence theorem. The author works out the consequences and the practical use of these results by giving detailed studies and illustrations of classical subjects (classes, idèles, ray class fields, symbols, reciprocity laws, Hasse's principles, the Grunwald-Wang theorem, Hilbert's towers,...). He also proves some new or less-known results (reflection theorem, structure of the Abelian closure of a number field) and lays emphasis on the invariant T_p of Abelian p-ramification, which is related to important Galois cohomology properties and p-adic conjectures. This book, intermediary between the classical literature published in the sixties and the recent computational literature, gives much material in an elementary way, and is suitable for students, researchers, and all who are fascinated by this theory.

Friedrich von HAESELER. — **Automatic sequences.** — De Gruyter expositions in mathematics, vol. 36. — Un vol. relié, 18×24,5, de 191 p. — ISBN 3-11-015629-6. — Prix: €78.50. — Walter de Gruyter, Berlin, 2003.

Automatic sequences are sequences which are, in a well-defined manner, produced by a finite automaton. The concept of automatic sequences has applications in algebra, number the-

ory, finite automata, formal languages, and combinatorics of words. The goal of this text is to provide a unified approach to automatic sequences over a group. The text deals with several aspects of automatic sequences: substitutions and finite automata, a general notion of automaticity, elementary properties of automatic sequences, automatic functions and their properties, an algebraic approach to automatic sequences.

G. J. O. JAMESON. — **The prime number theorem.** — London Mathematical Society student texts, vol. 53. — Un vol. broché, 15×22,5, de X, 252 p. — ISBN 0-521-89110-8 (relié: 0-521-81411-1). — Prix: £18.95 (relié: £50.00). — Cambridge University Press, Cambridge, 2003.

The prime number theorem gives an asymptotic expression for the number of primes less than a given number. It is unquestionably one of the great theorems of mathematics. This book aims to give a simple and clear exposition of the theorem and its proof, treating it as a subject in its own right rather than a fringe topic of a wider subject. The book gives an easy-paced and thorough account of the concepts and methods needed. Topics are introduced in a natural order, avoiding unmotivated definitions. The main prerequisites are standard undergraduate courses on real and complex analysis.

Serge PERRINE. — **La théorie de Markoff et ses développements.** — Un vol. relié, 17,5×25, de VII, 326 p. — ISBN 2-909467-05-8. — Tessier & Ashpool, Guildford, Surrey et Chantilly, Oise, 2002.

Un formalisme général: Sur les suites et les fractions continues. Sur les matrices de suites. Sur les formes quadratiques. L'équation de Markoff généralisée. Quelques conséquences. — Bouquets, forêts et arbres: Le principe d'analyse. Les involutions conservant l'équation. Les bouquets de solutions. Finitude du nombre de bouquets. Équations équilibrées et triplets de Cohn. Le lien entre bouquets et arbres — Analyse du spectre de Markoff: Première décomposition. Seconde décomposition. Dépendance mutuelle des suites *X2* et *T*. Recollement des arborescences. — Vers les courbes elliptiques: Approche par les corps quadratiques. Équations pointues et dégénérées. Équation d'un réseau. Lien avec les courbes elliptiques. Compléments sur la surface cubique. Compléments géométriques. — Tores percés conformes: Géométrie du demi plan de Poincaré. Construction de tores percés conformes. Représentations paramétriques. Cône attaché à un tore percé. Étude des tores percés paraboliques. Réduction des tores percés paraboliques. Perspectives. — La théorie de Markoff classique: Présentation matricielle de la théorie. D'autres présentations matricielles. Identification du groupe concerné. Relation avec le groupe libre $\mathbf{F}_2$. Equivalence des couples de générateurs. Conséquences pour le groupe Aut($\mathbf{F}_2$). Présentations du groupe Aut($\mathbf{F}_2$). L'interprétation de l'arbre de Markoff. Applications à $GL(2,\mathbf{Z})$. — Géométrie conforme des surfaces: La notion de surface de Riemann. Des exemples de surfaces de Riemann. Revêtements universels et groupes de Poincaré. Groupes fuchsiens. La théorie de Teichmüller. Quelques applications. Cas du tore $\mathbf{T}$. Cas du tore percé à une piqûre $\mathbf{T}\backslash\{p\}$. Approche par les fibrés vectoriels.

Igor SHPARLINSKI. — **Cryptographic applications of analytic number theory: complexity lower bounds and pseudorandomness.** — Progress in computer science and applied logic, vol. 22. — Un vol. relié, 16×24, de VIII, 411 p. — ISBN 3-7643-6654-0. — Prix: SFr. 148.00. — Birkhäuser, Basel, 2003.

The book introduces new ways of using analytic number theory in cryptography and related areas, such as complexity theory and pseudorandom number generation. *Key topics and features:* Various lower bounds on the complexity of some number theoretic and cryptographic problems, associated with classical schemes such as RSA, Diffie-Hellman, DSA as well as with

relatively new schemes like XTR and NTRU. — A series of very recent results about certain important characteristics (period, distribution, linear complexity) of several commonly used pseudorandom number generators, such as the RSA generator, Blum-Blum-Shub generator, Naor-Reingold generator, inversive generator, and others. — One of the principal tools is bounds of exponential sums, which are combined with other number theoretic methods such as lattice reduction and sieving. — A number of open problems of different levels of difficulty and proposals for further research. — An extensive and up-to-date bibliography.

Corps et polynômes

Toma ALBU. — **Cogalois theory.** — Pure and applied mathematics, vol. 252. — Un vol. relié, 15,5×23,5, de XII, 341 p. — ISBN 0-8247-0949-7. — Prix: US$ 150.00. — Marcel Dekker, New York, 2003.

This volume offers a systematic, comprehensive investigation of field extensions, finite or not, that possess a cogalois correspondence. The subject, called cogalois theory, is somewhat dual to the very classical Galois theory dealing with field extensions possessing a Galois correspondence. — *Contents:* Finite cogalois theory: Preliminaries. Kneser extensions. Cogalois extensions. Strongly Kneser extensions. Galois G-cogalois extensions. Radical extensions and crossed homomorphisms. Examples of G-cogalois extensions. G-cogalois extensions and primitive elements. Applications to algebraic number fields. Connections with graded algebras and Hopf algebras. — Infinite cogalois theory: Infinite Kneser extensions. Infinite G-cogalois extensions. Infinite Kummer theory. Infinite Galois theory and Pontryagin duality. Infinite Galois G-cogalois extensions.

Christian U. JENSEN, Arne LEDET, Noriko YUI. — **Generic polynomials: constructive aspects of the inverse Galois problem.** — Mathematical Science Research Institute publications, vol. 45. — Un vol. relié, 16×24, de IX, 258 p. — ISBN 0-521-81998-9. — Prix: £45.00. — Cambridge University Press, Cambridge, 2002.

This book describes a constructive approach to the inverse Galois problem: Given a finite group G and a field K, determine whether there exists a Galois extension of K whose Galois group is isomorphic to G. Further, if there is such a Galois extension, find an explicit polynomial over K whose Galois group is the prescribed group G. The main theme of the book is an exposition of a family of "generic" polynomials for certain finite groups, which give all Galois extensions having the required group as their Galois group. The existence of such generic polynomials is discussed, and where they do exist, a detailed treatment of their construction is given. The book also introduces the notion of "generic dimension" to address the problem of the smallest number of parameters required by a generic polynomial.

Teo MORA. — **Solving polynomial equation systems I: the Kronecker-Duval philosophy.** — Encyclopedia of mathematics and its applications, vol. 88. — Un vol. relié, 16×24, de XIII, 423 p. — ISBN 0-521-81154-6. — Prix: £60.00. — Cambridge University Press, Cambridge, 2003.

Polynomial equations have been long studied, both theoretically and with a view to solving them. Until recently, manual computation was the only solution method and the theory was developed to accommodate it. With the advent of computers, the situation changed dramatically. Many classical results can be more usefully recast within a different framework