

Mathematics of Computation



EDITED BY

James H. Bramble
Bille C. Carlson
Walter Gautschi, *Managing Editor*
Donald Goldfarb
Eugene Isaacson
Heinz-Otto Kreiss
James N. Lyness
Harald Niederreiter
Syvert P. Nørsett
Andrew M. Odlyzko
Frank W. J. Olver
John E. Osborn
Stanley Osher
Beresford Parlett
Carl Pomerance
René Schoof
Larry L. Schumaker
Ridgway Scott
Daniel Shanks
Frank Stenger
Hans J. Stetter
G. W. Stewart
Vidar Thomée
Lars B. Wahlbin
Hugh C. Williams
John W. Wrench, Jr.

April 1988

Volume 50, Number 182, Pages 361–662

**Published by the American Mathematical Society
Providence, Rhode Island USA**

ISSN 0025-5718

Editorial Committee

WALTER GAUTSCHI, Chairman. Dept. of Computer Sciences, Purdue Univ., West Lafayette, IN 47907

DONALD GOLDFARB, Dept. of Industrial Engineering and Operations Research, Seely W. Mudd Building, Columbia Univ. in the City of New York, New York, NY 10027

JOHN E. OSBORN, Dept. of Mathematics, Univ. of Maryland, College Park, MD 20742

HUGH C. WILLIAMS, Dept. of Computer Science, Univ. of Manitoba, Winnipeg, Manitoba, Canada R3T 2N2

Technical Editor

ERIKA GAUTSCHI, Dept. of Computer Sciences, Purdue Univ., West Lafayette, IN 47907

Board of Associate Editors

JAMES H. BRAMBLE, Dept. of Mathematics, Cornell Univ., Ithaca, NY 14853

BILLE C. CARLSON, Dept. of Mathematics, Iowa State Univ., Ames, IA 50011

EUGENE ISAACSON, Courant Institute of Mathematical Sciences, New York Univ., 251 Mercer Street, New York, NY 10012

HEINZ-OTTO KREISS, Dept. of Applied Mathematics, California Institute of Technology, Pasadena, CA 91125

JAMES N. LYNESS, Argonne National Laboratory, 9700 South Cass Avenue, Argonne, IL 60439

HARALD NIEDERREITER, Mathematical Institute, Austrian Academy of Sciences, Dr.-Ignaz-Seipel-Platz 2, A-1010 Vienna, Austria

SYVERT P. NØRSETT, Div. of Numerical Mathematics, The University of Trondheim and The Norwegian Institute of Technology, Alfred Getz vei 1, N-7034 Trondheim-NTH, Norway

ANDREW M. ODLYZKO, AT&T Bell Laboratories, 600 Mountain Avenue, Murray Hill, NJ 07974

FRANK W. J. OLVER, Inst. for Physical Science and Technology, Univ. of Maryland, College Park, MD 20742

STANLEY OSHER, Dept. of Mathematics, Univ. of California, Los Angeles, CA 90024

BERESFORD PARLETT, Dept. of Mathematics, Univ. of California, Berkeley, CA 94720

CARL POMERANCE, Dept. of Mathematics, The Univ. of Georgia, Athens, GA 30602

RENÉ SCHOOF, Universiteit van Amsterdam, Mathematisch Instituut, Roetersstraat 15, 1018 WB Amsterdam, The Netherlands

LARRY L. SCHUMAKER, Center for Approximation Theory, Dept. of Mathematics, Texas A&M Univ., College Station, TX 77843-3368

RIDGWAY SCOTT, Dept. of Mathematics, Pennsylvania State Univ., University Park, PA 16802

DANIEL SHANKS, Dept. of Mathematics, Univ. of Maryland, College Park, MD 20742

FRANK STENGER, Dept. of Mathematics, Univ. of Utah, Salt Lake City, UT 84112

HANS J. STETTER, Institut für Numerische Mathematik, Technische Universität Wien, Wiedner Hauptstrasse 6-10, A-1040, Wien, Austria

G. W. STEWART, Dept. of Computer Science, Univ. of Maryland, College Park, MD 20742

VIDAR THOMÉE, Mathematics Dept., Chalmers Univ. of Technology, S-412 96 Göteborg, Sweden

LARS B. WAHLBIN, Dept. of Mathematics, Cornell Univ., Ithaca, NY 14853

JOHN W. WRENCH, JR., 6310 Jefferson Blvd., Frederick, MD 21701

SUBSCRIPTION INFORMATION: MATHEMATICS OF COMPUTATION is published quarterly, with issues numbered serially since Volume 1, Number 1. Subscription prices for Volumes 50 and 51 (1988) are \$181.00 list; \$145.00 institutional member; \$118.00 member of CBMS organizations; \$109.00 individual AMS member. A late charge of 10% of the subscription price will be imposed upon orders received from nonmember institutions and organizations after January 1 of the subscription year. Subscribers outside the United States and India must pay a postage surcharge of \$8.00; subscribers in India must pay a postage surcharge of \$18.00. Combination paper and microfiche subscription prices are \$241.00 list; \$193.00 institutional member. Microfiche of each issue will be mailed the fastest way before the issue is mailed by the printer.

BACK NUMBER INFORMATION: Back number prices *per volume* are for Volumes 1-21, \$82.00 list, \$66.00 member; for Volumes 22-33, \$124.00 list, \$99.00 institutional member; for Volumes 34-43, \$82.00 list, \$64.00 institutional member; Volumes 44-45, \$113.00 list, \$90.00 institutional member; Volumes 46-47, \$127.00 list, \$102.00 institutional member; Volumes 48-49, \$135.00 list, \$108.00 institutional member. Back volumes may be purchased on microfilm or microfiche from University Microfilms International, 300 North Zeeb Road, Ann Arbor, MI 48106.

UNPUBLISHED MATHEMATICAL TABLES: The editorial office of the journal maintains a repository of Unpublished Mathematical Tables (UMT). When a table is deposited in the UMT repository a brief summary of its contents is published in the section *Reviews and Descriptions of Tables and Books*. Upon request, the chairman of the editorial committee will supply copies of any table for a nominal cost per page. All tables and correspondence concerning the UMT should be sent to Walter Gautschi, Chairman, Editorial Committee, Mathematics of Computation, Department of Computer Sciences, Purdue University, West Lafayette, IN 47907.

Orders for subscriptions and publications of the American Mathematical Society should be addressed to the AMS, P.O. Box 1571, Annex Station, Providence, RI 02901-9930. *All orders must be accompanied by payment.* Other correspondence should be addressed to P.O. Box 6248, Providence, RI 02940.

MATHEMATICS OF COMPUTATION is published quarterly by the American Mathematical Society, 201 Charles Street, Providence, RI 02940. Second-class postage is paid at Providence, Rhode Island, and additional mailing offices. Postmaster: Send address changes to Mathematics of Computation, American Mathematical Society, P.O. Box 6248, Providence, RI 02940.

Copyright © 1988, American Mathematical Society. All rights reserved.
Printed in the United States of America.

The paper used in this journal is acid-free and falls within the guidelines established to ensure permanence and durability. ♾

MATHEMATICS OF COMPUTATION

TABLE OF CONTENTS

April 1988

Kenneth Eriksson and Claes Johnson , An Adaptive Finite Element Method for Linear Elliptic Problems	361
Sunil Kumar , Superconvergence of a Collocation-Type Method for Simple Turning Points of Hammerstein Equations	385
Andrew R. Conn, Nicholas I. M. Gould, and Philippe L. Toint , Testing a Class of Methods for Solving Minimization Problems with Simple Bounds on the Variables	399
D. Bini and V. Pan , Efficient Algorithms for the Evaluation of the Eigenvalues of (Block) Banded Toeplitz Matrices	431
James W. Demmel , The Probability That A Numerical Analysis Problem Is Difficult	449
F. W. J. Olver , Error Bounds for Linear Recurrence Relations	481
Jean-Francis Loiseau, Jean-Pierre Codaccioni, and Regis Cáboz , Hyperelliptic Integrals and Multiple Hypergeometric Series	501
Henry L. Gray and Nien fan Zhang , On a New Definition of the Fractional Difference	513
Shu Tezuka , On Optimal GFSR Pseudorandom Number Generators	531
Emma Lehmer , Connection Between Gaussian Periods and Cyclic Units ...	535
René Schoof and Lawrence C. Washington , Quintic Polynomials and Real Cyclotomic Fields with Large Class Numbers	543
Harvey Cohn and Jesse Deutsch , An Explicit Modular Equation in Two Variables for $\mathbb{Q}(\sqrt{3})$	557
Johannes Buchmann and H. C. Williams , On the Infrastructure of the Principal Ideal Class of an Algebraic Number Field of Unit Rank One	569
Pascual Llorente and Jordi Quer , On Totally Real Cubic Fields with Discriminant $D < 10^7$	581
Francis Buekenhout and Sarah Rees , The Subgroup Structure of the Mathieu Group M_{12}	595
E. Seah and D. R. Stinson , On the Enumeration of One-Factorizations of Complete Graphs Containing Prescribed Automorphism Groups	607
A. J. Stephens and H. C. Williams , Some Computational Results on a Problem Concerning Powerful Numbers	619
S. Battiato and W. Borho , Are There Odd Amicable Numbers Not Divisible by Three?	633

Reviews and Descriptions of Tables and Books	639
Oden and Carey 13 , Chavent and Jaffre 14 , Reinhardt 15 , Elschner 16 , Čížek 17 , Abramowitz and Stegun, Editors 18 , Bauer and Eidel 19a, b, c , Fibonacci (Sigler) 20 , van der Burgh and Mattheij, Editors 21 , Collatz, Meinardus and Nürnberger, Editors 22 , Keast and Fairweather, Editors 23 , Jamieson, Gannon and Douglass, Editors 24 , Deuffhard and Engquist, Editors 25	
Table Errata	653
Bateman Manuscript Project 610 , Oberhettinger and Badii 611 , Fibonacci 612	
Corrigenda	655
Rabinowitz, Dueck and Williams	
Author Index	659

Information for Contributors

Authors are encouraged to prepare articles electronically with the $\mathcal{A}\mathcal{M}\mathcal{S}$ - $\mathcal{T}\mathcal{E}\mathcal{X}$ software package in the AMS pre-print style and to provide the article in this electronic form for typesetting. While this procedure may not reduce the interval between submission and publication of an article, generally much more accurate copy will be returned for proofreading. Production time for manuscripts prepared with other systems, even $\mathcal{T}\mathcal{E}\mathcal{X}$ itself without $\mathcal{A}\mathcal{M}\mathcal{S}$ - $\mathcal{T}\mathcal{E}\mathcal{X}$, currently prevents cost-effective use of the existing electronic form. Before sending an $\mathcal{A}\mathcal{M}\mathcal{S}$ - $\mathcal{T}\mathcal{E}\mathcal{X}$ manuscript for typesetting, contact the AMS Composition department for details.

Manuscripts prepared by some means other than $\mathcal{A}\mathcal{M}\mathcal{S}$ - $\mathcal{T}\mathcal{E}\mathcal{X}$ should be doubled-spaced and produced in the format used by the journal. For journal abbreviations, see the latest *Mathematical Reviews* volume index. An author should submit the original and two copies of the manuscript and retain one copy. The author may suggest an appropriate editor for his paper. It is recommended that the author acquaint himself with the pertinent material contained in "A Manual for Authors of Mathematical Papers," which is available from the American Mathematical Society. All contributions intended for publication and all books for review should be addressed to Walter Gautschi, Chairman, Editorial Committee, Mathematics of Computation, Department of Computer Sciences, Purdue University, West Lafayette, Indiana 47907. The date received, which is published with the final version of an accepted paper, is the date received in the office of the Chairman of the Editorial Committee, and it is the responsibility of the author to submit manuscripts directly to this office.

Each article submitted for publication must be accompanied by a brief and reasonably self-contained abstract, and by 1980 *Mathematics Subject Classification* (1985 *Revision*) numbers. If a list of key words and phrases is included, it will be printed as a footnote on the first page. A list of the classification numbers may be found in the 1984 Subject Index to *Mathematical Reviews*. Authors are also encouraged to supply electronic addresses when available. These will be printed after the postal address at the end of each article.

Copying and Reprinting

Individual readers of this publication, and nonprofit libraries acting for them, are permitted to make fair use of the material, such as to copy an article for use in teaching or research. Permission is granted to quote brief passages from this publication in reviews provided the customary acknowledgement of the source is given.

Republication, systematic copying, or multiple reproduction of any material in this publication (including abstracts) is permitted only under license from the American Mathematical Society. Requests for such permission should be addressed to the Executive Director, American Mathematical Society, P.O. Box 6248, Providence, Rhode Island 02940.

The appearance of the code on the first page of an article in this journal indicates the copyright owner's consent for copying beyond that permitted by Sections 107 or 108 of the U.S. Copyright Law, provided that the fee of \$1.00 plus \$.25 per page for each copy be paid directly to Copyright Clearance Center, Inc., 21 Congress Street, Salem, Massachusetts 01970. This consent does not extend to other kinds of copying, such as copying for general distribution, for advertising or promotion purposes, for creating new collective works, or for resale.

DANIEL SHANKS, DEDICATION
Special Issue
Mathematics of Computation

This special issue of *Mathematics of Computation* (Volume 48, Number 177, January 1987) is dedicated to Daniel Shanks on the occasion of his 70th birthday. Since 1959, when Shanks joined the Editorial Committee for this journal, he has been a guiding force in shaping the computational number theory component of the journal, and has had an immense influence in the field. This volume contains papers by some of the top researchers in the field and covers such topics as elliptic curves, primality testing, congruences, class groups, and cyclotomic fields. Although a numbered issue of the *Mathematics of Computation* journal, it will serve as a stand alone reference work for computational number theory.

Contents

- William W. Adams**, *Characterizing Pseudoprimes for third-order linear recurrences*
Leonard M. Adelman, Dennis R. Estes, and Kevin S. McCurley, *Solving bivariate quadratic congruences in random polynomial time*
Richard Blecksmith, John Brillhart, and Irving Gerst, *Parity results for certain partition functions and identities similar to theta function identities*
Johannes Buchmann, *The computation of the fundamental unit of totally complex quartic orders*
Johannes Buchmann and H. C. Williams, *On principal ideal testing in totally complex quartic fields and the determination of certain cyclotomic constants*
Nicholas Buck, Lones Smith, Blair K. Spearman, and Kenneth S. Williams, *The cyclotomic numbers of order fifteen*
Duncan A. Buell, *Class groups of quadratic fields. II*
David G. Cantor, *Computing in the Jacobian of a hyperelliptic curve*
H. Cohen and A. K. Lenstra, *Implementation of a new primality test*
H. Cohen and J. Martinet, *Class groups of number fields: numerical heuristics*
Harvey Cohn and Jesse Deutsch, *Application of symbolic manipulation to Hecke transformations of modular forms in two variables*
T. W. Cusick and Lowell Schoenfeld, *A table of fundamental pairs of units in totally real cubic fields*

- Daniel Gordon, Douglas Grenier, and Audrey Terras**, *Hecke operators and the fundamental domain for $(\text{SL}(3, \mathbb{Z}))$*
Marie-Nicole Gras, *Special units in real cyclic sextic fields*
R. K. Guy, C. B. Lacampagne, and J. L. Selfridge, *Primes at a glance*
Neal Koblitz, *Elliptic curve cryptosystems*
D. H. Lehmer and Emma Lehmer, *Cyclotomic resultants*
H. W. Lenstra, Jr. and R. J. Schoof, *Primitive normal bases for finite fields*
R. A. Mollin, *Class numbers of quadratic fields determined by solvability of diophantine equations*
Peter L. Montgomery, *Speeding the Pollard and elliptic curve methods of factorization*
Morris Newman and Robert C. Thompson, *Numerical values of Goldberg's coefficients in the series for $\log(e^x e^y)$*
A. M. Odlyzko, *On the distribution of spacings between zeros of the zeta function*
M. Pohst, *On computing isomorphisms of equation orders*
Carl Pomerance, *Very short primality proofs*
Herman J. J. te Riele, *On the sign of the difference $\pi(x) - li(x)$*
Robert D. Silverman, *The multiple polynomial quadratic sieve*
Jonathan W. Tanner and Samuel S. Wagstaff, Jr., *New congruences for the Bernoulli numbers*
Heinz M. Tschöpe and Horst G. Zimmer, *Computation of the Néron-Tate height on elliptic curves*
Lawrence C. Washington, *Class numbers of the simplest cubic fields*
H. C. Williams, *Effective primality tests for some integers of the forms $A5^n - 1$ and $A7^n - 1$*
H. C. Williams and M. C. Wunderlich, *On the parallel generation of the residues for the continued fraction factoring algorithm*
Don Zagier, *Large integral points on elliptic curves*

1980 Mathematics Subject Classification 11
 ISSN 0025-5718

448 pages (softcover), January 1987
Individual member \$29, List price \$48.
 Institutional member \$38
 To order, please specify SHANKS/MC

Shipping/Handling: 1st book \$2, each add'l \$1,
 \$25 max. By air, 1st book \$5, each add'l \$3,
 \$100 max.

Prepayment required. Order from AMS, P.O. Box
 1571, Annex Station, Providence, RI 02901-9930,
 or call 800-556-7774 to use VISA or MasterCard.



(Continued from back cover)

Reviews and Descriptions of Tables and Books	639
Oden and Carey 13 , Chavent and Jaffre 14 , Reinhardt 15 , Elschner 16 , Čížek 17 , Abramowitz and Stegun, Editors 18 , Bauer and Eidel 19a, b, c , Fibonacci (Sigler) 20 , van der Burgh and Mattheij, Editors 21 , Collatz, Meinardus and Nürnberger, Editors 22 , Keast and Fairweather, Editors 23 , Jamieson, Gannon and Douglass, Editors 24 , Deuffhard and Engquist, Editors 25	
Table Errata	653
Bateman Manuscript Project 610 , Oberhettinger and Badii 611 , Fibonacci 612	
Corrigenda	655
Rabinowitz, Dueck and Williams	
Author Index	659

No microfiche supplement in this issue

MATHEMATICS OF COMPUTATION

TABLE OF CONTENTS

April 1988

Kenneth Eriksson and Claes Johnson , An Adaptive Finite Element Method for Linear Elliptic Problems	361
Sunil Kumar , Superconvergence of a Collocation-Type Method for Simple Turning Points of Hammerstein Equations	385
Andrew R. Conn, Nicholas I. M. Gould, and Philippe L. Toint , Testing a Class of Methods for Solving Minimization Problems with Simple Bounds on the Variables	399
D. Bini and V. Pan , Efficient Algorithms for the Evaluation of the Eigenvalues of (Block) Banded Toeplitz Matrices	431
James W. Demmel , The Probability That A Numerical Analysis Problem Is Difficult	449
F. W. J. Olver , Error Bounds for Linear Recurrence Relations	481
Jean-Francois Loiseau, Jean-Pierre Codaccioni, and Regis Cáböz , Hyperelliptic Integrals and Multiple Hypergeometric Series	501
Henry L. Gray and Nien fan Zhang , On a New Definition of the Fractional Difference	513
Shu Tezuka , On Optimal GFSR Pseudorandom Number Generators	531
Emma Lehmer , Connection Between Gaussian Periods and Cyclic Units ...	535
René Schoof and Lawrence C. Washington , Quintic Polynomials and Real Cyclotomic Fields with Large Class Numbers	543
Harvey Cohn and Jesse Deutsch , An Explicit Modular Equation in Two Variables for $\mathbb{Q}(\sqrt{3})$	557
Johannes Buchmann and H. C. Williams , On the Infrastructure of the Principal Ideal Class of an Algebraic Number Field of Unit Rank One	569
Pascual Llorente and Jordi Quer , On Totally Real Cubic Fields with Discriminant $D < 10^7$	581
Francis Buekenhout and Sarah Rees , The Subgroup Structure of the Mathieu Group M_{12}	595
E. Seah and D. R. Stinson , On the Enumeration of One-Factorizations of Complete Graphs Containing Prescribed Automorphism Groups	607
A. J. Stephens and H. C. Williams , Some Computational Results on a Problem Concerning Powerful Numbers	619
S. Battiato and W. Borho , Are There Odd Amicable Numbers Not Divisible by Three?	633

(Continued on inside back cover)