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
Syvert P. Nørsett
Andrew M. Odlyzko
Frank W. J. Olver
John E. Osborn
Stanley Osher
Beresford Parlett
Philip Rabinowitz
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.

January 1987
Volume 48, Number 177, Pages 1–448

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
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
PHILIP RABINOWITZ, Dept. of Applied Mathematics, The Weizmann Institute of Science, Rehovot, Israel
LARRY L. SCHUMAKER, Center for Approximation Theory, Dept. of Mathematics, Texas A&M Univ., College Station, TX 77843-3368
RIDGWAY SCOTT, Dept. of Mathematics, Univ. of Michigan, Ann Arbor, MI 48109
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 48 and 49 (1987) are $174.00 list; $139.00 institutional member; $113.00 member of CBMS organizations; $104.00 individual AMS member. A late charge of 10% of the subscription price will be imposed upon orders received from nonmembers 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 $231.00 list; $185.00 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, $80.00 list, $64.00 member; for Volumes 22–33, $120.00 list, $96.00 institutional member; for Volumes 34–43, $80.00 list, $64.00 institutional member; Volumes 44–45, $113.00 list, $90.00 institutional member; Volumes 46–47, $123.00 list, $98.00 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 02904. 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 © 1987, 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
January 1987

William W. Adams, Characterizing Pseudoprimes for Third-Order Linear Recurrences 1

Leonard M. Adleman, Dennis R. Estes, and Kevin S. McCurley, Solving Bivariate Quadratic Congruences in Random Polynomial Time 17

Richard Blecksmith, John Brillhart, and Irving Gerst, Parity Results for Certain Partition Functions and Identities Similar to Theta Function Identities 29

Johannes Buchmann, The Computation of the Fundamental Unit of Totally Complex Quartic Orders 39

Johannes Buchmann and H. C. Williams, On Principal Ideal Testing in Totally Complex Quartic Fields and the Determination of Certain Cyclotomic Constants 55

Nicholas Buck, Lones Smith, Blair K. Spearman, and Kenneth S. Williams, The Cyclotomic Numbers of Order Fifteen 67

Duncan A. Buell, Class Groups of Quadratic Fields. II 85

David G. Cantor, Computing in the Jacobian of a Hyperelliptic Curve 95

H. Cohen and A. K. Lenstra, Implementation of a New Primality Test 103

H. Cohen and J. Martinet, Class Groups of Number Fields: Numerical Heuristics 123

Harvey Cohn and Jesse Deutsch, Application of Symbolic Manipulation to Hecke Transformations of Modular Forms in Two Variables 139

T. W. Cusick and Lowell Schoenfeld, A Table of Fundamental Pairs of Units in Totally Real Cubic Fields 147

Daniel Gordon, Douglas Grenier, and Audrey Terras, Hecke Operators and the Fundamental Domain for $SL(3, \mathbf{Z})$ 159

Marie-Nicole Gras, Special Units in Real Cyclic Sextic Fields 179

R. K. Guy, C. B. Lacampagne, and J. L. Selfridge, Primes at a Glance 183

Neal Koblitz, Elliptic Curve Cryptosystems 203

D. H. Lehmer and Emma Lehmer, Cyclotomic Resultants 211

H. W. Lenstra, Jr. and R. J. Schoof, Primitive Normal Bases for Finite Fields 217

R. A. Mollin, Class Numbers of Quadratic Fields Determined by Solvability of Diophantine Equations 233

Peter L. Montgomery, Speeding the Pollard and Elliptic Curve Methods of Factorization 243

Morris Newman and Robert C. Thompson, Numerical Values of Goldberg's Coefficients in the Series for $\log(e^x e^y)$ 265

A. M. Odlyzko, On the Distribution of Spacings Between Zeros of the Zeta Function 273

M. Pohst, On Computing Isomorphisms of Equation Orders 309

Carl Pomerance, Very Short Primality Proofs 315

Herman J. J. te Riele, On the Sign of the Difference $\pi(x) - \mathrm{li}(x)$ 323

Robert D. Silverman, The Multiple Polynomial Quadratic Sieve 329

Jonathan W. Tanner and Samuel S. Wagstaff, Jr., New Congruences for the Bernoulli Numbers 341

Heinz M. Tschöpe and Horst G. Zimmer, Computation of the Néron-Tate Height on Elliptic Curves 351

Lawrence C. Washington, Class Numbers of the Simplest Cubic Fields 371

H. C. Williams, Effective Primality Tests for Some Integers of the Forms $A5^n - 1$ and $A7^n - 1$ 385

H. C. Williams and M. C. Wunderlich, On the Parallel Generation of the Residues for the Continued Fraction Factoring Algorithm 405

Don Zagier, Large Integral Points on Elliptic Curves 425

Reviews and Descriptions of Tables and Books 437

Shanks **1**, Rosen **2**, Riesel **3**, Conway, Curtis, Nortin, Parker, and Wilson **4**, Bach **5**, Muskat and Williams **6**

Corrigendum 447

Costa Pereira

Supplement to "Implementation of a New Primality Test" by **H. Cohen and A. K. Lenstra** S1

Microfiche Supplements

Nicholas Buck, Lones Smith, Blair K. Spearman, and Kenneth S. Williams, The Cyclotomic Numbers of Order Fifteen

Morris Newman and Robert C. Thompson, Numerical Values of Goldberg's Coefficients in the Series for $\log(e^x e^y)$

Information for Contributors and information on Copying and Reprinting can be found after the supplements section at the end of this issue.