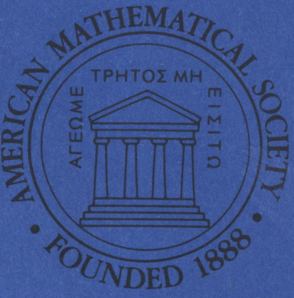
Mathematics of Computation



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

Published by the American Mathematical Society
Providence, Rhode Island USA
ISSN 0025-5718

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UNPUBLISHED MATHEMATICAL TABLES: The editorial office of the journal maintains a repository of Unpublished Mathematical Tables (UMT).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.

Mathematics of Computation

Special Issue

Dedicated to

DANIEL SHANKS

January 1987

VOLUME 48 · 1987 · NUMBERS 177–178

Providence, Rhode Island, USA
ISSN 0025–5718

Dedication

The editors of Mathematics of Computation are pleased to dedicate this issue to Daniel Shanks on the occasion of his seventieth birthday, January 17, 1987.

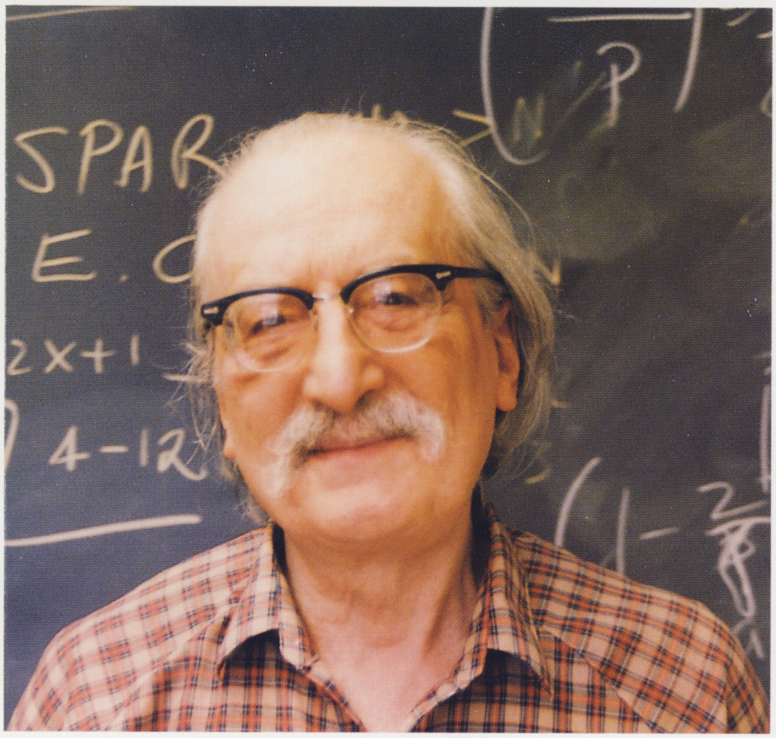
Dan joined the Editorial Committee in 1959 and has served, either on this committee or on The Board of Associate Editors, ever since. Indeed, when occasion has demanded, he has even acted in an ex officio capacity as the chairman of The Editorial Committee. He is also the custodian of the UMT File.

The extent of Dan's contribution to the computational number theory component of Mathematics of Computation is incalculable. Through his energy in finding new manuscripts, his enthusiasm in encouraging younger authors, and his innovative ideas, he is, to a very great degree, responsible for the flourishing state of this discipline. Some idea of his immense influence and wide range of interests can be gained by an examination of the table of contents of this issue.

In an effort to keep this dedication a surprise and to keep this issue from growing too large, the editors did not inform all of the people who would have liked to contribute articles to celebrate Dan's birthday. To those whose work does not appear here, we sincerely apologize.

The editors are pleased to acknowledge the tremendous amount of care and work put in by the authors of the articles contained in this volume. We would also like to thank the referees, whose patience, good humor, and professionalism, was a great help in putting up with what were frequently very close deadlines.

H. C. Williams
for the editors



DANIEL SHANKS

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.

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.

Information for Contributors

Authors are encouraged to prepare articles electronically with the AMS-TeX 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 TeX itself without AMS-TeX, currently prevents cost-effective use of the existing electronic form. Before sending an AMS-TeX manuscript for typesetting, contact the AMS Composition Department for details.

Manuscripts prepared by some means other than AMS-TeX should be double-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. Institutions sponsoring research reported in the journal are assessed page and microfiche charges.

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.

The research journals of the American Mathematical Society carry a page charge of $50.00 per page to help defray the cost of publication. This amount is charged to the institution or to a contract supporting the research reported in the published paper. The publication charge policy of the United States Federal Council for Science and Technology (FCST) is reported on page 112 of the February, 1975 issue of the NOTICES of the American Mathematical Society. In no case is the author personally responsible for paying the page charge, nor is acceptance of the author's paper for publication dependent upon payment of the page charge.

Copying and Reprinting

ABCDEFGHIJ 8987

(*Continued from back cover*)

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 $\log(e^x e^y)$

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

(Continued on inside back cover)