VOLUME 70 NUMBER 236 OCTOBER 2001

MATHEMATICS OF COMPUTATION

AMERICAN MATHEMATICAL SOCIETY

EDITED BY

Randolph E. Bank
David W. Boyd
Susanne C. Brenner
Richard P. Brent
Joe P. Buhler
Carsten Carstensen
Arjeh M. Cohen
Ronald F. A. Cools
Howard Elman
Richard S. Falk
Andrew J. Granville
Daniel W. Lozier
Zhi-Quan Luo
Roswitha März
Harald Niederreiter
Ricardo Horacio Nochetto
Stanley Osher
Haesun Park
Joseph E. Pasciak
Lothar Reichel
René Schoof
Chi-Wang Shu
Frank Stenger
Denis Talay
Nico M. Temme
Lars B. Wahlbin, *Managing Editor*
Joseph D. Ward
Hugh C. Williams
Jinchao Xu

PROVIDENCE, RHODE ISLAND USA

ISSN 0025-5718

Available electronically at
www.ams.org/mcom/

Mathematics of Computation

This journal publishes research articles in computational mathematics. Areas covered include numerical analysis, with emphasis on the mathematical analysis and development of methods, computational number theory and algebra, and related fields. Table errata and reviews of books in areas related to computational mathematics are also included.

Submission information. See **Information for Authors** at the end of this issue.

Publisher Item Identifier. The Publisher Item Identifier (PII) appears at the top of the first page of each article published in this journal. This alphanumeric string of characters uniquely identifies each article and can be used for future cataloging, searching, and electronic retrieval.

Postings to the AMS website. Articles are posted to the AMS website individually after proof is returned from authors and before appearing in an issue.

Subscription information. *Mathematics of Computation* is published quarterly. Beginning in January 1996 *Mathematics of Computation* is accessible from `www.ams.org/publications/`. Subscription prices for Volume 70 (2001) are as follows: for paper delivery, $366 list, $293 institutional member, $329 corporate member, $238 member of CBMS organizations; $220 individual member; for electronic delivery, $329 list, $263 institutional member, $296 corporate member, $214 member of CBMS organizations, $197 individual member. Upon request, subscribers to paper delivery of this journal are also entitled to receive electronic delivery. If ordering the paper version, add $12 for surface delivery outside the United States and India; $18 to India. Expedited delivery to destinations in North America is $17; elsewhere $56.

Back number information. For back issues see the *AMS Catalog of Publications*.

Subscriptions and orders should be addressed to the American Mathematical Society, P.O. Box 845904, Boston, MA 02284-5904. *All orders must be accompanied by payment.* Other correspondence should be addressed to P.O. Box 6248, Providence, RI 02940-6248.

Copying and reprinting. Material in this journal may be reproduced by any means for educational and scientific purposes without fee or permission with the exception of reproduction by services that collect fees for delivery of documents and provided that the customary acknowledgment of the source is given. This consent does not extend to other kinds of copying for general distribution, for advertising or promotional purposes, or for resale. Requests for permission for commercial use of material should be addressed to the Assistant to the Publisher, American Mathematical Society, P.O. Box 6248, Providence, RI 02940-6248. Requests can also be made by e-mail to `reprint-permission@ams.org`.

Excluded from these provisions is material in articles for which the author holds copyright. In such cases, requests for permission to use or reprint should be addressed directly to the author(s). (Copyright ownership is indicated in the notice in the lower right-hand corner of the first page of each article.)

Mathematics of Computation is published quarterly by the American Mathematical Society at 201 Charles Street, Providence, RI 02904-2294. Periodicals postage is paid at Providence, Rhode Island. Postmaster: Send address changes to Mathematics of Computation, American Mathematical Society, P. O. Box 6248, Providence, RI 02940-6248.

© 2001 by the American Mathematical Society. All rights reserved.

This journal is indexed in *Mathematical Reviews*, *Zentralblatt MATH*, *Science Citation Index*®, *Science Citation Index*™*–Expanded*, *ISI Alerting Services*℠, *CompuMath Citation Index*®, and *Current Contents*®*/Physical, Chemical & Earth Sciences.*

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

10 9 8 7 6 5 4 3 2 1 06 05 04 03 02 01

INDEX TO VOLUME 70 (2001)

Bai, Fengshan. *See* Li, Tiejun

Bailey, David H., and Broadhurst, David J. *Parallel integer relation detection: Techniques and applications*, 1719

Bao, Weizhu. *See* Han, Houde

Battiato, Stefan, and Borho, Walter. *Breeding amicable numbers in abundance. II*, 1329

Batut, Christian. *Classification of quintic eutactic forms*, 395

Beale, J. Thomas. *A convergent boundary integral method for three-dimensional water waves*, 977

Bernstein, Daniel J. *Enumerating solutions to $p(a) + q(b) = r(c) + s(d)$*, 389

Beśka, Marek, and Dziedziul, Karol. *Saturation theorems for interpolation and the Bernstein-Schnabl operator*, 705

Bini, Dario, Del Corso, Gianna M., Manzini, Giovanni, and Margara, Luciano. *Inversion of circulant matrices over $\mathbf{Z}_m$*, 1169

Boe, Brian D. *Geometry of the Jantzen region in Lusztig's conjecture*, 1265

Bojanov, Borislav D., and Dimitrov, Dimitar K. *Gaussian extended cubature formulae for polyharmonic functions*, 671

Borho, Walter. *See* Battiato, Stefan

Bos, L., Taylor, M. A., and Wingate, B. A. *Tensor product Gauss-Lobatto points are Fekete points for the cube*, 1543

Bramble, James H., and Zhang, Xuejun. *Uniform convergence of the multigrid V-cycle for an anisotropic problem*, 453

Brezzi, Franco, and Marini, Donatella. *Error estimates for the three-field formulation with bubble stabilization*, 911

Brin, Leon Q. *Numerical testing of the stability of viscous shock waves*, 1071

Broadhurst, David J. *See* Bailey, David H.

Browkin, Jerzy. *Continued fractions in local fields, II*, 1281

Buhmann, M. D. *A new class of radial basis functions with compact support*, 307

Cai, DongSheng. *See* Miyazaki, Yoshinori

Canuto, Claudio, and Masson, Roland. *Stabilized wavelet approximations of the Stokes problem*, 1397

Carstensen, Carsten, and Funken, Stefan A. *A posteriori error control in low-order finite element discretisations of incompressible stationary flow problems*, 1353

Charnes, C., and Dempwolff, U. *The eight dimensional ovoids over $GF(5)$*, 853

Clark, David A., and Jarvis, Norman C. *Dense admissible sequences*, 1713

Cohen, Albert, Dahmen, Wolfgang, and DeVore, Ronald. *Adaptive wavelet methods for elliptic operator equations: Convergence rates*, 27

Cools, Ronald, and Lyness, James N. *Three- and four-dimensional K-optimal lattice rules of moderate trigonometric degree*, 1549

Cutter, Pamela A. *Finding prime pairs with particular gaps*, 1737

Daboussi, Hedi, and Rivat, Joël. *Explicit upper bounds for exponential sums over primes*, 431

Dahmen, Wolfgang. *See* Cohen, Albert

Dai, Y. H., and Yuan, Y. *A three-parameter family of nonlinear conjugate gradient methods*, 1155

Davie, A. M., and Gaines, J. G. *Convergence of numerical schemes for the solution of parabolic stochastic partial differential equations*, 121

Dedieu, Jean-Pierre, and Shub, Mike. *On simple double zeros and badly conditioned zeros of analytic functions of n variables*, 319

Dégot, Jérôme. *A condition number theorem for underdetermined polynomial systems*, 329

Del Corso, Gianna M. *See* Bini, Dario

Demkowicz, L. *See* Monk, P.

Dempwolff, U. *See* Charnes, C.

Descombes, Stéphane. *Convergence of a splitting method of high order for reaction-diffusion systems*, 1481

DeVore, Ronald. *See* Cohen, Albert

Dimitrov, Dimitar K. *See* Bojanov, Borislav D.

Doche, Christophe. *On the spectrum of the Zhang-Zagier height*, 419

Dontchev, A. L., and Hager, William W. *The Euler approximation in state constrained optimal control*, 173

Dziedziul, Karol. *See* Beśka, Marek
E, Weinan. *See* Liu, Jian-Guo
Fan, Haitao. *Existence of discrete shock profiles of a class of monotonicity preserving schemes for conservation laws*, 1043
Fang, Kai-Tai. *See* Liang, Jia-Juan
Faßbender, H. *The parameterized SR algorithm for symplectic (butterfly) matrices*, 1515
Fieker, Claus. *Computing class fields via the Artin map*, 1293
Flynn, E. Victor, Leprévost, Franck, Schaefer, Edward F., Stein, William A., Stoll, Michael, and Wetherell, Joseph L. *Empirical evidence for the Birch and Swinnerton-Dyer conjectures for modular Jacobians of genus 2 curves*, 1675
Friedlander, John B., Pomerance, Carl, and Shparlinski, Igor E. *Period of the power generator and small values of Carmichael's function*, 1591
Friedlander, John B., and Shparlinski, Igor E. *On the distribution of the power generator*, 1575
de Frutos, Javier, and Muñoz-Sola, Rafael. *On error estimates for Galerkin spectral discretizations of parabolic problems with nonsmooth initial data*, 525
Fukuda, Takashi, and Komatsu, Keiichi. *On Iwasawa λ_3-invariants of cyclic cubic fields of prime conductor*, 1707
Funken, Stefan A. *See* Carstensen, Carsten
Gaal, Peter, and Golomb, Solomon W. *Exhaustive determination of* (1023, 511, 255)*-cyclic difference sets*, 357
Gaines, J. G. *See* Davie, A. M.
Ganesh, M., and Steinbach, O. *Boundary element methods for potential problems with nonlinear boundary conditions*, 1031
Garefalakis, Theodoulos, and Panario, Daniel. *The index calculus method using non-smooth polynomials*, 1253
Gatica, Gabriel N., and Meddahi, Salim. *A dual-dual mixed formulation for nonlinear exterior transmission problems*, 1461
Gil, Amparo, Segura, Javier, and Temme, Nico M. *On nonoscillating integrals for computing inhomogeneous Airy functions*, 1183
Golomb, Solomon W. *See* Gaal, Peter
Gosse, Laurent, and Tzavaras, Athanasios E. *Convergence of relaxation schemes to the equations of elastodynamics*, 555
Grantham, Jon. *Frobenius pseudoprimes*, 873
Gutzmer, Tim, and Melenk, Jens Markus. *Approximation orders for natural splines in arbitrary dimensions*, 699
Haber, Seymour. *See* Jang, Aeyoung Park
Hager, William W. *See* Dontchev, A. L.
Halpern, L. *A spectral method for the Stokes problem in three-dimensional unbounded domains*, 1417
Han, Houde, and Bao, Weizhu. *Error estimates for the finite element approximation of linear elastic equations in an unbounded domain*, 1437
Heo, Sangwoo, and Xu, Yuan. *Constructing fully symmetric cubature formulae for the sphere*, 269
Hickernell, Fred J. *See* Liang, Jia-Juan
Hoffmann, W., Schatz, A. H., Wahlbin, L. B., and Wittum, G. *Asymptotically exact a posteriori estimators for the pointwise gradient error on each element in irregular meshes. Part 1: A smooth problem and globally quasi-uniform meshes*, 897
Hou, Thomas Y., and Zhang, Pingwen. *A new stabilizing technique for boundary integral methods for water waves*, 951
Houston, Paul, and Süli, Endre. *Adaptive Lagrange–Galerkin methods for unsteady convection-diffusion problems*, 77
Ikebe, Yasuhiko. *See* Miyazaki, Yoshinori
Jang, Aeyoung Park, and Haber, Seymour. *Numerical indefinite integration of functions with singularities*, 205
Jarvis, Norman C. *See* Clark, David A.
Jia, Zhongxiao, and Stewart, G. W. *An analysis of the Rayleigh–Ritz method for approximating eigenspaces*, 637
Johnson, Michael J. *The L_2-approximation order of surface spline interpolation*, 719

Joux, Antoine, and Lercier, Reynald. *"Chinese & Match", an alternative to Atkin's "Match and Sort" method used in the SEA algorithm*, 827
Jüttler, B. *Hermite interpolation by Pythagorean hodograph curves of degree seven*, 1089
Katsaounis, Theodoros, and Makridakis, Charalambos. *Finite volume relaxation schemes for multidimensional conservation laws*, 533
Kauthen, J.-P. *The numerical solution of integral-algebraic equations of index 1 by polynomial spline collocation methods*, 1503
Kikuchi, Yasushi. *See* Miyazaki, Yoshinori
Kohatsu-Higa, Arturo. *Weak approximations. A Malliavin calculus approach*, 135
Kokkorakis, G. C., and Roumeliotis, J. A. *Power series expansions for Mathieu functions with small arguments*, 1221
Komatsu, Keiichi. *See* Fukuda, Takashi
Korotov, Sergey, Křížek, Michal, and Neittaanmäki, Pekka. *Weakened acute type condition for tetrahedral triangulations and the discrete maximum principle*, 107
Křížek, Michal. *See* Korotov, Sergey
Lage, C. *See* Sauter, S. A.
Laubin, Pascal. *Optimal order collocation for the mixed boundary value problem on polygons*, 607
Leprévost, Franck. *See* Flynn, E. Victor
Lercier, Reynald. *See* Joux, Antoine
Li, Runze. *See* Liang, Jia-Juan
Li, Tiejun, and Bai, Fengshan. *Minimizing multi-homogeneous Bézout numbers by a local search method*, 767
Liang, Jia-Juan, Fang, Kai-Tai, Hickernell, Fred J., and Li, Runze. *Testing multivariate uniformity and its applications*, 337
Liberman, Elsa. *A posteriori error estimator for a mixed finite element method for Reissner-Mindlin plate*, 1383
Liu, Jian-Guo, and E, Weinan. *Simple finite element method in vorticity formulation for incompressible flows*, 579
Liu, Jian-Guo, and Xin, Zhouping. *Convergence of the point vortex method for 2-D vortex sheet*, 595
Luca, Florian. *On a conjecture of Erdős and Stewart*, 893
Lyness, James N. *See* Cools, Ronald
Makridakis, Charalambos. *See* Katsaounis, Theodoros
Manzini, Giovanni. *See* Bini, Dario
Margara, Luciano. *See* Bini, Dario
Marini, Donatella. *See* Brezzi, Franco
Masson, Roland. *See* Canuto, Claudio
Mastroianni, G., and Monegato, G. *Error estimates in the numerical evaluation of some BEM singular integrals*, 251
Meddahi, Salim. *See* Gatica, Gabriel N.
Melenk, Jens Markus. *See* Gutzmer, Tim
Melman, A. *Extreme eigenvalues of real symmetric Toeplitz matrices*, 649
Mhaskar, H. N., Narcowich, F. J., and Ward, J. D. *Spherical Marcinkiewicz-Zygmund inequalities and positive quadrature*, 1113
Miyazaki, Yoshinori, Kikuchi, Yasushi, Cai, DongSheng, and Ikebe, Yasuhiko. *Error analysis for the computation of zeros of regular Coulomb wave function and its first derivative*, 1195
Monegato, G. *See* Mastroianni, G.
Monk, P., and Demkowicz, L. *Discrete compactness and the approximation of Maxwell's equations in* $\mathbb{R}^3$, 507
Muñoz-Sola, Rafael. *See* de Frutos, Javier
Narcowich, F. J. *See* Mhaskar, H. N.
Neittaanmäki, Pekka. *See* Korotov, Sergey
Niederreiter, Harald, and Shparlinski, Igor E. *On the distribution of inversive congruential pseudorandom numbers in parts of the period*, 1569
Nilssen, Trygve K., Tai, Xue-Cheng, and Winther, Ragnar. *A robust nonconforming* H^2*-element*, 489
Northshield, Sam. *On iterates of Möbius transformations on fields*, 1305

Omar, Sami. *Localization of the first zero of the Dedekind zeta function*, 1607
Panario, Daniel. *See* Garefalakis, Theodoulos
Papageorgiou, A. *Fast convergence of quasi-Monte Carlo for a class of isotropic integrals*, 297
Pauli, Sebastian, and Roblot, Xavier-François. *On the computation of all extensions of a p-adic field of a given degree*, 1641
Peyre, Emmanuel, and Tschinkel, Yuri. *Tamagawa numbers of diagonal cubic surfaces, numerical evidence*, 367
Pomerance, Carl. *See* Friedlander, John B.
van der Poorten, A. J., te Riele, H. J. J., and Williams, H. C. *Computer verification of the Ankeny–Artin–Chowla conjecture for all primes less than* 100 000 000 000, 1311
Ramm, Alexander G., and Smirnova, Alexandra B. *On stable numerical differentiation*, 1131
Richstein, Jörg. *Verifying the Goldbach conjecture up to* $4 \cdot 10^{14}$, 1745
te Riele, H. J. J. *See* van der Poorten, A. J.
Rivat, Joël. *See* Daboussi, Hedi
Roberts, David P. *Density of cubic field discriminants*, 1699
Roblot, Xavier-François. *See* Pauli, Sebastian
Roumeliotis, J. A. *See* Kokkorakis, G. C.
Ryan, Pat. *Eigenvalue and eigenfunction error estimates for finite element formulations of linear hydroelasticity*, 471
Santos-León, J. C. *Error bounds for interpolatory quadrature rules on the unit circle*, 281
Sauter, S. A., and Lage, C. *Transformation of hypersingular integrals and black-box cubature*, 223
Schaefer, Edward F. *See* Flynn, E. Victor
Schatz, A. H. *See* Hoffmann, W.
Segura, Javier. *Bounds on differences of adjacent zeros of Bessel functions and iterative relations between consecutive zeros*, 1205
_____. *See* Gil, Amparo
Selmane, Schehrazad. *Quadratic extensions of totally real quintic fields*, 837
_____. *Tenth degree number fields with quintic fields having one real place*, 845
Shail, R. *A class of infinite sums and integrals*, 789
Shparlinski, Igor E. *On the uniformity of distribution of the RSA pairs*, 801
_____. *See* Friedlander, John B.
_____. *See* Niederreiter, Harald
Shub, Mike. *See* Dedieu, Jean-Pierre
Siksek, Samir. *Sieving for rational points on hyperelliptic curves*, 1661
Smirnova, Alexandra B. *See* Ramm, Alexander G.
Stein, Greg. *Using the theory of cyclotomy to factor cyclotomic polynomials over finite fields*, 1237
Stein, William A. *See* Flynn, E. Victor
Steinbach, O. *See* Ganesh, M.
Stewart, G. W. *See* Jia, Zhongxiao
Stoll, Michael. *See* Flynn, E. Victor
Süli, Endre. *See* Houston, Paul
Tai, Xue-Cheng. *See* Nilssen, Trygve K.
Taylor, M. A. *See* Bos, L.
Temme, Nico M. *See* Gil, Amparo
Teske, Edlyn. *On random walks for Pollard's rho method*, 809
Thaine, F. *Jacobi sums and new families of irreducible polynomials of Gaussian periods*, 1617
Tiihonen, T. *Shape calculus and finite element method in smooth domains*, 1
Toselli, Andrea, Widlund, Olof B., and Wohlmuth, Barbara I. *An iterative substructuring method for Maxwell's equations in two dimensions*, 935
Tschinkel, Yuri. *See* Peyre, Emmanuel
Tzavaras, Athanasios E. *See* Gosse, Laurent
Urban, Karsten. *Wavelet bases in* $\mathbf{H}(\mathrm{div})$ *and* $\mathbf{H}(\mathbf{curl})$, 739
Wahlbin, L. B. *See* Hoffmann, W.
Ward, J. D. *See* Mhaskar, H. N.
Wasilkowski, G. W., and Woźniakowski, H. *On the complexity of stochastic integration*, 685
Wetherell, Joseph L. *See* Flynn, E. Victor

Widlund, Olof B. *See* Toselli, Andrea
Williams, H. C. *See* van der Poorten, A. J.
Wingate, B. A. *See* Bos, L.
Winther, Ragnar. *See* Nilssen, Trygve K.
Wittum, G. *See* Hoffmann, W.
Wohlmuth, Barbara I. *See* Toselli, Andrea
Woźniakowski, H. *See* Wasilkowski, G. W.
Xin, Zhouping. *See* Liu, Jian-Guo
Xu, Jinchao, and Zhou, Aihui. *A two-grid discretization scheme for eigenvalue problems*, 17
Xu, Yuan. *See* Heo, Sangwoo
Yuan, Y. *See* Dai, Y. H.
Zhang, Pingwen. *See* Hou, Thomas Y.
Zhang, Xuejun. *See* Bramble, James H.
Zhang, Zhenxiang. *Finding strong pseudoprimes to several bases*, 863
Zhou, Aihui. *See* Xu, Jinchao

INDEX OF REVIEWS BY AUTHOR OF WORK REVIEWED

Author	*Review Number*	*Classification*	*Page*
Ascher, Uri M., & Petzold, Linda R.	5	65-01, 65L05, 65L06, 65L10, 65L12, 65L99	1340
Blake, Ian, Seroussi, Gadiel, & Smart, Nigel	14	94-02, 94A60, 14H52	1755
Budd, C. J., & Iserles, A. (Editors)	6	65L05, 37Mxx	1342
Chen, Zhongying	4	See Li, Ronghua	1338
Conn, Andrew R., Gould, Nicholas I. M., & Toint, Philippe L.	12	90C30, 90C25, 65K05	1753
Gould, Nicholas I. M.	12	See Conn, Andrew R.	1753
Humphries, A. R.	7	See Stuart, A. M.	1344
6 See Budd, C. J.		1342	
Kailath, T., & Sayed, A. H. (Editors)	13	65F05, 65F25, 65F35	1754
Konyagin, Sergei, & Shparlinski, Igor	9	11L05, 11L40, 65C10, 94A60, 94B05	1348
Li, Ronghua, Chen, Zhongying, & Wu, Wei	4	65-02, 65N06, 65N30	1338
Meurant, Gerard	8	65-02, 65Fxx	1346
Petzold, Linda R.	5	See Ascher, Uri M.	1340
Rabier, Patrick J., & Rheinboldt, Werner C.	11	70F25, 34A09, 65L80	1751
Rheinboldt, Werner C.	11	See Rabier, Patrick J.	1751
13 See Kailath, T.		1754	
Schwab, Ch.	2	65N30, 74S05, 76M10	1335
Seroussi, Gadiel	14	See Blake, Ian	1755
Sethian, J. A.	1	35L60, 65M06, 74S20, 76M20, 78A05, 80A22	449
Shparlinski, Igor	9	See Konyagin, Sergei	1348
Smart, Nigel	14	See Blake, Ian	1755
Smart, Nigel P.	10	11-02, 11Dxx	1349
Stuart, A. M., & Humphries, A. R.	7	37Mxx, 65Pxx	1344
Toint, Philippe L.	12	See Conn, Andrew R.	1753
Trefethen, Lloyd N.	3	41A10, 42A10, 65M70, 65T40	1337
Wu, Wei	4	See Li, Ronghua	1338

INDEX OF REVIEWS BY SUBJECT OF WORK REVIEWED

Author	Review Number	Title	Page
11-XX Number theory			
11-02 *Research exposition (monographs, survey articles)*			
Smart, Nigel P.	10	The algorithmic resolution of Diophantine equations	1349
11Dxx *Diophantine equations*			
Smart, Nigel P.	10	The algorithmic resolution of Diophantine equations	1349
11L05 *Gauss and Kloosterman sums; generalizations*			
Konyagin, Sergei, & Shparlinski, Igor	9	Character sums with exponential functions and their applications	1348
11L40 *Estimates on character sums*			
Konyagin, Sergei, & Shparlinski, Igor	9	Character sums with exponential functions and their applications	1348
14-XX Algebraic geometry			
14H52 *Elliptic curves*			
Blake, Ian, Seroussi, Gadiel, & Smart, Nigel	14	Elliptic curves in cryptography	1755
34-XX Ordinary differential equations			
34A09 *Implicit equations, differential-algebraic equations*			
Rabier, Patrick J., & Rheinboldt, Werner C.	11	Nonholonomic motion of rigid mechanical systems from a DAE viewpoint	1751
35-XX Partial differential equations			
35L60 *Nonlinear first-order PDE of hyperbolic type*			
Sethian, J. A.	1	Level set methods and fast marching methods: evolving interfaces in computational geometry, fluid mechanics, computer vision, and materials science	449
37-XX Dynamical systems and ergodic theory			
37Mxx *Approximation methods and numerical treatment of dynamical systems*			
Budd, C. J., & Iserles, A. (Editors)	6	Geometric integration: numerical solution of differential equations	1342
Stuart, A. M., & Humphries, A. R.	7	Dynamical systems and numerical analysis	1344
41-XX Approximations and expansions			
41A10 *Approximation by polynomials*			
Trefethen, Lloyd N.	3	Spectral methods in Matlab	1337
42-XX Fourier analysis			
42A10 *Trigonometric approximation*			
Trefethen, Lloyd N.	3	Spectral methods in Matlab	1337

65-XX Numerical analysis

65-01 *Instructional exposition (textbooks, tutorial papers, etc.)*

Ascher, Uri M., & Petzold, Linda R.	5	Computer methods for ordinary differential equations and differential-algebraic equations	1340

65-02 *Research exposition (monographs, survey articles)*

Li, Ronghua, Chen, Zhongying, & Wu, Wei	4	Generalized difference methods for differential equations. Numerical analysis of finite volume methods	1338
Meurant, Gerard	8	Computer solution of large linear systems	1346

65C10 *Random number generation*

Konyagin, Sergei, & Shparlinski, Igor	9	Character sums with exponential functions and their applications	1348

65Fxx *Numerical linear algebra*

Meurant, Gerard	8	Computer solution of large linear systems	1346

65F05 *Direct methods for linear systems and matrix inversion*

Kailath, T., & Sayed, A. H. (Editors)	13	Fast reliable algorithms for matrices with structure	1754

65F25 *Orthogonalization*

Kailath, T., & Sayed, A. H. (Editors)	13	Fast reliable algorithms for matrices with structure	1754

65F35 *Matrix norms, conditioning, scaling*

Kailath, T., & Sayed, A. H. (Editors)	13	Fast reliable algorithms for matrices with structure	1754

65K05 *Mathematical programming algorithms*

Conn, Andrew R., Gould, Nicholas I. M., & Toint, Philippe L.	12	Trust-region methods	1753

65L05 *Initial value problems*

Ascher, Uri M., & Petzold, Linda R.	5	Computer methods for ordinary differential equations and differential-algebraic equations	1340
Budd, C. J., & Iserles, A. (Editors)	6	Geometric integration: numerical solution of differential equations	1342

65L06 *Multistep, Runge-Kutta and extrapolation methods*

Ascher, Uri M., & Petzold, Linda R.	5	Computer methods for ordinary differential equations and differential-algebraic equations	1340

65L10 *Boundary value problems*

Ascher, Uri M., & Petzold, Linda R.	5	Computer methods for ordinary differential equations and differential-algebraic equations	1340

65L12 *Finite difference methods*

Ascher, Uri M., & Petzold, Linda R.	5	Computer methods for ordinary differential equations and differential-algebraic equations	1340

65L80 *Methods for differential-algebraic equations*

Rabier, Patrick J., & Rheinboldt, Werner C. 11 Nonholonomic motion of rigid mechanical systems from a DAE viewpoint 1751

65L99 *None of the above, but in this section*

Ascher, Uri M., & Petzold, Linda R. 5 Computer methods for ordinary differential equations and differential-algebraic equations 1340

65M06 *Finite difference methods*

Sethian, J. A. 1 Level set methods and fast marching methods: evolving interfaces in computational geometry, fluid mechanics, computer vision, and materials science 449

65M70 *Spectral, collocation and related methods*

Trefethen, Lloyd N. 3 Spectral methods in Matlab 1337

65N06 *Finite difference methods*

Li, Ronghua, Chen, Zhongying, & Wu, Wei 4 Generalized difference methods for differential equations. Numerical analysis of finite volume methods 1338

65N30 *Finite elements, Rayleigh-Ritz and Galerkin methods, finite methods*

Li, Ronghua, Chen, Zhongying, & Wu, Wei 4 Generalized difference methods for differential equations. Numerical analysis of finite volume methods 1338

Schwab, Ch. 2 *p*- and *hp*-finite element methods. Theory and applications in solid and fluid mechanics 1335

65Pxx *Numerical problems in dynamical systems*

Stuart, A. M., & Humphries, A. R. 7 Dynamical systems and numerical analysis 1344

65T40 *Trigonometric approximation and interpolation*

Trefethen, Lloyd N. 3 Spectral methods in Matlab 1337

70-XX Mechanics of particles and systems

70F25 *Nonholonomic systems*

Rabier, Patrick J., & Rheinboldt, Werner C. 11 Nonholonomic motion of rigid mechanical systems from a DAE viewpoint 1751

74-XX Mechanics of deformable solids

74S05 *Finite element methods*

Schwab, Ch. 2 *p*- and *hp*-finite element methods. Theory and applications in solid and fluid mechanics 1335

74S20 *Finite difference methods*

Sethian, J. A. 1 Level set methods and fast marching methods: evolving interfaces in computational geometry, fluid mechanics, computer vision, and materials science 449

76-XX Fluid mechanics

76M10 *Finite element methods*

Schwab, Ch.	2	p- and hp-finite element methods. Theory and applications in solid and fluid mechanics	1335

76M20 *Finite difference methods*

Sethian, J. A.	1	Level set methods and fast marching methods: evolving interfaces in computational geometry, fluid mechanics, computer vision, and materials science	449

78-XX Optics, electromagnetic theory

78A05 *Geometric optics*

Sethian, J. A.	1	Level set methods and fast marching methods: evolving interfaces in computational geometry, fluid mechanics, computer vision, and materials science	449

80-XX Classical thermodynamics, heat transfer

80A22 *Stefan problems, phase changes, etc.*

Sethian, J. A.	1	Level set methods and fast marching methods: evolving interfaces in computational geometry, fluid mechanics, computer vision, and materials science	449

90-XX Operations research, mathematical programming

90C25 *Convex programming*

Conn, Andrew R., Gould, Nicholas I. M., & Toint, Philippe L.	12	Trust-region methods	1753

90C30 *Nonlinear programming*

Conn, Andrew R., Gould, Nicholas I. M., & Toint, Philippe L.	12	Trust-region methods	1753

94-XX Information and communication, circuits

94-02 *Research exposition (monographs, survey articles)*

Blake, Ian, Seroussi, Gadiel, & Smart, Nigel	14	Elliptic curves in cryptography	1755

94A60 *Cryptography*

Blake, Ian, Seroussi, Gadiel, & Smart, Nigel	14	Elliptic curves in cryptography	1755
Konyagin, Sergei, & Shparlinski, Igor	9	Character sums with exponential functions and their applications	1348

94B05 *Linear codes, general*

Konyagin, Sergei, & Shparlinski, Igor	9	Character sums with exponential functions and their applications	1348

VOLUME 70 2001

MATHEMATICS OF COMPUTATION

AMERICAN MATHEMATICAL SOCIETY

EDITED BY
Randolph E. Bank
David W. Boyd
Susanne C. Brenner
Richard P. Brent
Joe P. Buhler
Carsten Carstensen
Arjeh M. Cohen
Ronald F. A. Cools
Howard Elman
Richard S. Falk
Andrew J. Granville
Daniel W. Lozier
Zhi-Quan Luo
Roswitha März
Harald Niederreiter
Ricardo Horacio Nochetto
Stanley Osher
Haesun Park
Joseph E. Pasciak
Lothar Reichel
René Schoof
Chi-Wang Shu
Frank Stenger
Denis Talay
Nico M. Temme
Lars B. Wahlbin, *Managing Editor*
Joseph D. Ward
Hugh C. Williams
Jinchao Xu

PROVIDENCE, RHODE ISLAND USA

ISSN 0025-5718

Mathematics of Computation

This journal publishes research articles in computational mathematics. Areas covered include numerical analysis, with emphasis on the mathematical analysis and development of methods, computational number theory and algebra, and related fields. Table errata and reviews of books in areas related to computational mathematics are also included.

Submission information. See **Information for Authors** at the end of this issue.

Publisher Item Identifier. The Publisher Item Identifier (PII) appears at the top of the first page of each article published in this journal. This alphanumeric string of characters uniquely identifies each article and can be used for future cataloging, searching, and electronic retrieval.

Postings to the AMS website. Articles are posted to the AMS website individually after proof is returned from authors and before appearing in an issue.

Subscription information. *Mathematics of Computation* is published quarterly. Beginning in January 1996 *Mathematics of Computation* is accessible from `www.ams.org/publications/`. Subscription prices for Volume 70 (2001) are as follows: for paper delivery, $366 list, $293 institutional member, $329 corporate member, $238 member of CBMS organizations; $220 individual member; for electronic delivery, $329 list, $263 institutional member, $296 corporate member, $214 member of CBMS organizations, $197 individual member. Upon request, subscribers to paper delivery of this journal are also entitled to receive electronic delivery. If ordering the paper version, add $12 for surface delivery outside the United States and India; $18 to India. Expedited delivery to destinations in North America is $17; elsewhere $56.

Back number information. For back issues see the *AMS Catalog of Publications*.

Subscriptions and orders should be addressed to the American Mathematical Society, P.O. Box 845904, Boston, MA 02284-5904. *All orders must be accompanied by payment.* Other correspondence should be addressed to P.O. Box 6248, Providence, RI 02940-6248.

Copying and reprinting. Material in this journal may be reproduced by any means for educational and scientific purposes without fee or permission with the exception of reproduction by services that collect fees for delivery of documents and provided that the customary acknowledgment of the source is given. This consent does not extend to other kinds of copying for general distribution, for advertising or promotional purposes, or for resale. Requests for permission for commercial use of material should be addressed to the Assistant to the Publisher, American Mathematical Society, P.O. Box 6248, Providence, RI 02940-6248. Requests can also be made by e-mail to `reprint-permission@ams.org`.

Excluded from these provisions is material in articles for which the author holds copyright. In such cases, requests for permission to use or reprint should be addressed directly to the author(s). (Copyright ownership is indicated in the notice in the lower right-hand corner of the first page of each article.)

Mathematics of Computation is published quarterly by the American Mathematical Society at 201 Charles Street, Providence, RI 02904-2294. Periodicals postage is paid at Providence, Rhode Island. Postmaster: Send address changes to Mathematics of Computation, American Mathematical Society, P. O. Box 6248, Providence, RI 02940-6248.

© 2001 by the American Mathematical Society. All rights reserved.

This journal is indexed in *Mathematical Reviews*, *Zentralblatt MATH*, *Science Citation Index*®, *Science Citation Index*™*–Expanded*, *ISI Alerting Services*℠, *CompuMath Citation Index*®, and *Current Contents*®*/Physical, Chemical & Earth Sciences.*

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

10 9 8 7 6 5 4 3 2 1 06 05 04 03 02 01

MATHEMATICS OF COMPUTATION

CONTENTS

Vol. 70, No. 233 January 2001

T. Tiihonen, Shape calculus and finite element method in smooth domains 1
Jinchao Xu and Aihui Zhou, A two-grid discretization scheme for eigenvalue problems ... 17
Albert Cohen, Wolfgang Dahmen, and Ronald DeVore, Adaptive wavelet methods for elliptic operator equations: Convergence rates ... 27
Paul Houston and Endre Süli, Adaptive Lagrange–Galerkin methods for unsteady convection-diffusion problems ... 77
Sergey Korotov, Michal Křížek, and Pekka Neittaanmäki, Weakened acute type condition for tetrahedral triangulations and the discrete maximum principle ... 107
A. M. Davie and J. G. Gaines, Convergence of numerical schemes for the solution of parabolic stochastic partial differential equations ... 121
Arturo Kohatsu-Higa, Weak approximations. A Malliavin calculus approach ... 135
A. L. Dontchev and William W. Hager, The Euler approximation in state constrained optimal control ... 173
Aeyoung Park Jang and Seymour Haber, Numerical indefinite integration of functions with singularities ... 205
S. A. Sauter and C. Lage, Transformation of hypersingular integrals and black-box cubature ... 223
G. Mastroianni and G. Monegato, Error estimates in the numerical evaluation of some BEM singular integrals ... 251
Sangwoo Heo and Yuan Xu, Constructing fully symmetric cubature formulae for the sphere ... 269
J. C. Santos-León, Error bounds for interpolatory quadrature rules on the unit circle ... 281
A. Papageorgiou, Fast convergence of quasi-Monte Carlo for a class of isotropic integrals ... 297
M. D. Buhmann, A new class of radial basis functions with compact support ... 307
Jean-Pierre Dedieu and Mike Shub, On simple double zeros and badly conditioned zeros of analytic functions of n variables ... 319
Jérôme Dégot, A condition number theorem for underdetermined polynomial systems ... 329
Jia-Juan Liang, Kai-Tai Fang, Fred J. Hickernell, and Runze Li, Testing multivariate uniformity and its applications ... 337
Peter Gaal and Solomon W. Golomb, Exhaustive determination of (1023, 511, 255)-cyclic difference sets ... 357
Emmanuel Peyre and Yuri Tschinkel, Tamagawa numbers of diagonal cubic surfaces, numerical evidence ... 367
Daniel J. Bernstein, Enumerating solutions to $p(a) + q(b) = r(c) + s(d)$. 389
Christian Batut, Classification of quintic eutactic forms ... 395
Christophe Doche, On the spectrum of the Zhang-Zagier height ... 419

Hedi Daboussi and Joël Rivat, Explicit upper bounds for exponential sums over primes 431
Reviews and Descriptions of Tables and Books 449
J. A. Sethian **1**

Vol. 70, No. 234 **April 2001**

James H. Bramble and Xuejun Zhang, Uniform convergence of the multigrid V-cycle for an anisotropic problem 453
Pat Ryan, Eigenvalue and eigenfunction error estimates for finite element formulations of linear hydroelasticity 471
Trygve K. Nilssen, Xue-Cheng Tai, and Ragnar Winther, A robust nonconforming H^2-element 489
P. Monk and L. Demkowicz, Discrete compactness and the approximation of Maxwell's equations in $\mathbb{R}^3$ 507
Javier de Frutos and Rafael Muñoz-Sola, On error estimates for Galerkin spectral discretizations of parabolic problems with nonsmooth initial data 525
Theodoros Katsaounis and Charalambos Makridakis, Finite volume relaxation schemes for multidimensional conservation laws 533
Laurent Gosse and Athanasios E. Tzavaras, Convergence of relaxation schemes to the equations of elastodynamics 555
Jian-Guo Liu and Weinan E, Simple finite element method in vorticity formulation for incompressible flows 579
Jian-Guo Liu and Zhouping Xin, Convergence of the point vortex method for 2-D vortex sheet 595
Pascal Laubin, Optimal order collocation for the mixed boundary value problem on polygons 607
Zhongxiao Jia and G. W. Stewart, An analysis of the Rayleigh–Ritz method for approximating eigenspaces 637
A. Melman, Extreme eigenvalues of real symmetric Toeplitz matrices 649
Borislav D. Bojanov and Dimitar K. Dimitrov, Gaussian extended cubature formulae for polyharmonic functions 671
G. W. Wasilkowski and H. Woźniakowski, On the complexity of stochastic integration 685
Tim Gutzmer and Jens Markus Melenk, Approximation orders for natural splines in arbitrary dimensions 699
Marek Beśka and Karol Dziedziul, Saturation theorems for interpolation and the Bernstein-Schnabl operator 705
Michael J. Johnson, The L_2-approximation order of surface spline interpolation 719
Karsten Urban, Wavelet bases in $\mathbf{H}(\mathrm{div})$ and $\mathbf{H}(\mathbf{curl})$ 739
Tiejun Li and Fengshan Bai, Minimizing multi-homogeneous Bézout numbers by a local search method 767
R. Shail, A class of infinite sums and integrals 789

Igor E. Shparlinski, On the uniformity of distribution of the RSA pairs . 801
Edlyn Teske, On random walks for Pollard's rho method 809
Antoine Joux and Reynald Lercier, "Chinese & Match", an alternative to Atkin's "Match and Sort" method used in the SEA algorithm 827
Schehrazad Selmane, Quadratic extensions of totally real quintic fields .. 837
Schehrazad Selmane, Tenth degree number fields with quintic fields having one real place 845
C. Charnes and U. Dempwolff, The eight dimensional ovoids over GF(5) 853
Zhenxiang Zhang, Finding strong pseudoprimes to several bases 863
Jon Grantham, Frobenius pseudoprimes 873
Florian Luca, On a conjecture of Erdős and Stewart 893

Vol. 70, No. 235 **July 2001**

W. Hoffmann, A. H. Schatz, L. B. Wahlbin, and G. Wittum, Asymptotically exact a posteriori estimators for the pointwise gradient error on each element in irregular meshes. Part 1: A smooth problem and globally quasi-uniform meshes 897
Franco Brezzi and Donatella Marini, Error estimates for the three-field formulation with bubble stabilization 911
Andrea Toselli, Olof B. Widlund, and Barbara I. Wohlmuth, An iterative substructuring method for Maxwell's equations in two dimensions 935
Thomas Y. Hou and Pingwen Zhang, A new stabilizing technique for boundary integral methods for water waves 951
J. Thomas Beale, A convergent boundary integral method for three-dimensional water waves 977
M. Ganesh and O. Steinbach, Boundary element methods for potential problems with nonlinear boundary conditions 1031
Haitao Fan, Existence of discrete shock profiles of a class of monotonicity preserving schemes for conservation laws 1043
Leon Q. Brin, Numerical testing of the stability of viscous shock waves .. 1071
B. Jüttler, Hermite interpolation by Pythagorean hodograph curves of degree seven 1089
H. N. Mhaskar, F. J. Narcowich, and J. D. Ward, Spherical Marcinkiewicz-Zygmund inequalities and positive quadrature 1113
Alexander G. Ramm and Alexandra B. Smirnova, On stable numerical differentiation 1131
Y. H. Dai and Y. Yuan, A three-parameter family of nonlinear conjugate gradient methods 1155
Dario Bini, Gianna M. Del Corso, Giovanni Manzini, and Luciano Margara, Inversion of circulant matrices over $\mathbf{Z}_m$ 1169
Amparo Gil, Javier Segura, and Nico M. Temme, On nonoscillating integrals for computing inhomogeneous Airy functions 1183

Yoshinori Miyazaki, Yasushi Kikuchi, DongSheng Cai, and Yasuhiko Ikebe, Error analysis for the computation of zeros of regular Coulomb wave function and its first derivative 1195

Javier Segura, Bounds on differences of adjacent zeros of Bessel functions and iterative relations between consecutive zeros 1205

G. C. Kokkorakis and J. A. Roumeliotis, Power series expansions for Mathieu functions with small arguments 1221

Greg Stein, Using the theory of cyclotomy to factor cyclotomic polynomials over finite fields 1237

Theodoulos Garefalakis and Daniel Panario, The index calculus method using non-smooth polynomials 1253

Brian D. Boe, Geometry of the Jantzen region in Lusztig's conjecture 1265

Jerzy Browkin, Continued fractions in local fields, II 1281

Claus Fieker, Computing class fields via the Artin map 1293

Sam Northshield, On iterates of Möbius transformations on fields 1305

A. J. van der Poorten, H. J. J. te Riele, and H. C. Williams, Computer verification of the Ankeny–Artin–Chowla conjecture for all primes less than 100 000 000 000 1311

Stefan Battiato and Walter Borho, Breeding amicable numbers in abundance. II 1329

Reviews and Descriptions of Tables and Books 1335

Ch. Schwab **2**, Lloyd N. Trefethen **3**, Ronghua Li, Zhongying Chen, and Wei Wu **4**, Uri M. Ascher and Linda R. Petzold **5**, C. J. Budd and A. Iserles, Editors **6**, A. M. Stuart and A. R. Humphries **7**, Gerard Meurant **8**, Sergei Konyagin and Igor Shparlinski **9**, Nigel P. Smart **10**

Vol. 70, No. 236 **October 2001**

Carsten Carstensen and Stefan A. Funken, A posteriori error control in low-order finite element discretisations of incompressible stationary flow problems 1353

Elsa Liberman, A posteriori error estimator for a mixed finite element method for Reissner-Mindlin plate 1383

Claudio Canuto and Roland Masson, Stabilized wavelet approximations of the Stokes problem 1397

L. Halpern, A spectral method for the Stokes problem in three-dimensional unbounded domains 1417

Houde Han and Weizhu Bao, Error estimates for the finite element approximation of linear elastic equations in an unbounded domain 1437

Gabriel N. Gatica and Salim Meddahi, A dual-dual mixed formulation for nonlinear exterior transmission problems 1461

Stéphane Descombes, Convergence of a splitting method of high order for reaction-diffusion systems 1481

J.-P. Kauthen, The numerical solution of integral-algebraic equations of index 1 by polynomial spline collocation methods 1503
H. Faßbender, The parameterized SR algorithm for symplectic (butterfly) matrices 1515
L. Bos, M. A. Taylor, and B. A. Wingate, Tensor product Gauss-Lobatto points are Fekete points for the cube 1543
Ronald Cools and James N. Lyness, Three- and four-dimensional K-optimal lattice rules of moderate trigonometric degree 1549
Harald Niederreiter and Igor E. Shparlinski, On the distribution of inversive congruential pseudorandom numbers in parts of the period .. 1569
John B. Friedlander and Igor E. Shparlinski, On the distribution of the power generator 1575
John B. Friedlander, Carl Pomerance, and Igor E. Shparlinski, Period of the power generator and small values of Carmichael's function 1591
Sami Omar, Localization of the first zero of the Dedekind zeta function .. 1607
F. Thaine, Jacobi sums and new families of irreducible polynomials of Gaussian periods 1617
Sebastian Pauli and Xavier-François Roblot, On the computation of all extensions of a p-adic field of a given degree 1641
Samir Siksek, Sieving for rational points on hyperelliptic curves 1661
E. Victor Flynn, Franck Leprévost, Edward F. Schaefer, William A. Stein, Michael Stoll, and Joseph L. Wetherell, Empirical evidence for the Birch and Swinnerton-Dyer conjectures for modular Jacobians of genus 2 curves 1675
David P. Roberts, Density of cubic field discriminants 1699
Takashi Fukuda and Keiichi Komatsu, On Iwasawa λ_3-invariants of cyclic cubic fields of prime conductor 1707
David A. Clark and Norman C. Jarvis, Dense admissible sequences .. 1713
David H. Bailey and David J. Broadhurst, Parallel integer relation detection: Techniques and applications 1719
Pamela A. Cutter, Finding prime pairs with particular gaps 1737
Jörg Richstein, Verifying the Goldbach conjecture up to $4 \cdot 10^{14}$ 1745
Reviews and Descriptions of Tables and Books 1751
Patrick J. Rabier and Werner C. Rheinboldt **11**, Andrew R. Conn, Nicholas I. M. Gould, and Philippe L. Toint **12**, T. Kailath and A. H. Sayed, Editors **13**, Ian Blake, Gadiel Seroussi, and Nigel Smart **14**

Editorial Information

As of May 31, 2001, the backlog for this journal was approximately 3 issues. This estimate is the result of dividing the number of manuscripts for this journal in the Providence office that have not yet gone to the printer on the above date by the average number of articles per issue over the previous twelve months, reduced by the number of issues published in six months (the time necessary for editing and composing a typical issue). In an effort to make articles available as quickly as possible, articles are posted to the AMS website individually after proof is returned from authors and before appearing in an issue.

A Consent to Publish and Copyright Agreement is required before a paper will be published in this journal. After a paper is accepted for publication, the Providence office will send out a Consent to Publish and Copyright Agreement to all authors of the paper. By submitting a paper to this journal, authors certify that the results have not been submitted to nor are they under consideration for publication by another journal, conference proceedings, or similar publication.

Information for Authors

Initial submission. Prior to February 1, 2002, an author should submit three paper copies of the manuscript. Initial submission by email is not allowed. The author may suggest an appropriate editor for his paper. All contributions intended for publication and all books for review should be addressed to Lars B. Wahlbin, Managing Editor, Mathematics of Computation, Center for Applied Mathematics, 657 Frank H. T. Rhodes Hall, Cornell University, Ithaca, NY 14853-3801. The date received, which is published with the final version of an accepted paper, is the date received in the office of the Managing Editor, and it is the responsibility of the author to submit manuscripts directly to this office.

After February 1, 2002, an author should submit the manuscript by e-mail to `mathcomp@dam.brown.edu`. The manuscript should be sent as a single postscript or pdf file. Files can be compressed using zip or gzip making the files smaller in size. If e-mail submission is not feasible, three paper copies should be submitted. If the office of the Managing Editor is not able to print the file received from an e-mail submission, the author will be contacted and asked to send three paper copies instead. The author may suggest an appropriate editor for his or her paper. All paper copies of contributions and all books for review should be addressed to Chi-Wang Shu, Managing Editor, Mathematics of Computation, Division of Applied Mathematics, Brown University, 182 George Street, Providence, RI 02912. The date received, which is published with the final version of an accepted paper, is the date received in the office of the Managing Editor, and it is the responsibility of the author to submit manuscripts directly to this office.

The first page must consist of a *descriptive title*, followed by an *abstract* that summarizes the article in language suitable for workers in the general field (algebra, analysis, etc.). The *descriptive title* should be short, but informative; useless or vague phrases such as "some remarks about" or "concerning" should be avoided. The *abstract* must be brief and reasonably self-contained. Included with the footnotes to the paper should be the 2000 *Mathematics Subject Classification* representing the primary and secondary subjects of the article. The classifications are accessible from `www.ams.org/msc/`. The list of classifications is also available in print starting with the 1999 annual index of *Mathematical Reviews*. The Mathematics Subject Classification footnote may be followed by a list of *key words and phrases* describing the subject matter of the article and taken from it. Journal abbreviations used in bibliographies are listed in the latest *Mathematical Reviews* annual index. The series abbreviations are also accessible from `www.ams.org/publications/`. To help in preparing and verifying references, the AMS offers MR Lookup, a Reference Tool for Linking, at `www.ams.org/mrlookup/`. When the manuscript is submitted, authors should supply the editor with electronic addresses if available. These will be printed after the postal address at the end of each article.

Electronically prepared manuscripts. For the final submission of accepted papers, the AMS encourages use of electronically prepared manuscripts, with a strong preference

for $\mathcal{A}\mathcal{M}\mathcal{S}$-LaTeX. To this end, the Society has prepared $\mathcal{A}\mathcal{M}\mathcal{S}$-LaTeX author packages for each AMS publication. Author packages include instructions for preparing electronic manuscripts, the *AMS Author Handbook*, samples, and a style file that generates the particular design specifications of that publication series. Articles properly prepared using the $\mathcal{A}\mathcal{M}\mathcal{S}$-LaTeX style file and the \label and \ref commands automatically enable extensive intra-document linking to the bibliography and other elements of the article for searching electronically on the Web. Because linking must often be added manually to electronically prepared manuscripts in other forms of TeX, using $\mathcal{A}\mathcal{M}\mathcal{S}$-LaTeX also reduces the amount of technical intervention once the files are received by the AMS. This results in fewer errors in processing and saves the author proofreading time. $\mathcal{A}\mathcal{M}\mathcal{S}$-LaTeX papers also move more efficiently through the production stream, helping to minimize publishing costs.

$\mathcal{A}\mathcal{M}\mathcal{S}$-LaTeX is the highly preferred format of TeX, but author packages are also available in $\mathcal{A}\mathcal{M}\mathcal{S}$-TeX. Those authors who make use of these style files from the beginning of the writing process will further reduce their own efforts. Manuscripts prepared electronically in LaTeX or plain TeX are normally not acceptable due to the high amount of technical time required to insure that the file will run properly through the AMS in-house production system. LaTeX users will find that $\mathcal{A}\mathcal{M}\mathcal{S}$-LaTeX is the same as LaTeX with additional commands to simplify the typesetting of mathematics, and users of plain TeX should have the foundation for learning $\mathcal{A}\mathcal{M}\mathcal{S}$-LaTeX.

Authors may retrieve an author package from the AMS website starting from `www.ams.org/tex/` or via FTP to `ftp.ams.org` (login as `anonymous`, enter username as password, and type `cd pub/author-info`). The *AMS Author Handbook* and the *Instruction Manual* are available in PDF format following the author packages link from `www.ams.org/tex/`. The author package can also be obtained free of charge by sending email to `pub@ams.org` (Internet) or from the Publication Division, American Mathematical Society, P.O. Box 6248, Providence, RI 02940-6248. When requesting an author package, please specify $\mathcal{A}\mathcal{M}\mathcal{S}$-LaTeX or $\mathcal{A}\mathcal{M}\mathcal{S}$-TeX, Macintosh or IBM (3.5) format, and the publication in which your paper will appear. Please be sure to include your complete mailing address.

The final version of the electronic manuscript should be sent to the Providence office immediately after the paper has been accepted for publication. The author should also send the final version of the paper manuscript to the Managing Editor, who will forward a copy to the Providence office. Editors will require authors to send their electronically prepared manuscripts to the Providence office in a timely fashion. Electronically prepared manuscripts can be sent via email to `pub-submit@ams.org` (Internet) or on diskette to the Electronic Prepress Department, American Mathematical Society, P.O. Box 6248, Providence, RI 02940-6248. When sending a manuscript electronically, please be sure to include a message indicating in which publication the paper has been accepted. No corrections will be accepted electronically. Authors must mark their changes on their proof copies and return them to the Providence office. Complete instructions on how to send files are included in the author package.

Electronic graphics. Comprehensive instructions on preparing graphics are available at `www.ams.org/jourhtml/graphics.html`. A few of the major requirements are given here.

Submit files for graphics as EPS (Encapsulated PostScript) files. This includes graphics originated via a graphics application as well as scanned photographs or other computer-generated images. If this is not possible, TIFF files are acceptable as long as they can be opened in Adobe Photoshop or Illustrator. No matter what method was used to produce the graphic, it is necessary to provide a paper copy to the AMS.

Authors using graphics packages for the creation of electronic art should also avoid the use of any lines thinner than 0.5 points in width. Many graphics packages allow the user to specify a "hairline" for a very thin line. Hairlines often look acceptable when proofed on a typical laser printer. However, when produced on a high-resolution laser imagesetter, hairlines become nearly invisible and will be lost entirely in the final printing process.

Screens should be set to values between 15% and 85%. Screens which fall outside of this range are too light or too dark to print correctly. Variations of screens within a graphic should be no less than 10%.

AMS policy on making changes to articles after posting. Articles are posted to the AMS website individually after proof is returned from authors and before appearing in an issue. To preserve the integrity of electronically published articles, once an article is individually posted to the AMS website but not yet in an issue, changes cannot be made in place in the paper. However, an "Added after posting" section may be added to the paper right before the References when there is a critical error in the content of the paper. The "Added after posting" section gives the author an opportunity to correct this type of critical error before the article is put into an issue for printing and before it is then reposted with the issue. The "Added after posting" section remains a permanent part of the paper. The AMS does not keep author-related information, such as affiliation, current address, and email address, up to date after a paper is initially posted.

Once the article is assigned to an issue, even if the issue has not yet been posted to the AMS website, corrections may be made to the paper by submitting a traditional errata article to the Editor. The errata article will appear in a future print issue and will link back and forth on the web to the original article online.

Secure manuscript tracking on the Web and via email. Authors can track their manuscripts through the AMS journal production process using the personal AMS ID and Article ID printed in the upper right-hand corner of the Consent to Publish form sent to each author who publishes in AMS journals. Access to the tracking system is available from `www.ams.org/mstrack/` or via email sent to `mstrack-query@ams.org`. To access by email, on the subject line of the message simply enter the AMS ID and Article ID. To track more than one manuscript by email, choose one of the Article IDs and enter the AMS ID and the Article ID followed by the word *all* on the subject line. An explanation of each production step is provided on the web through links from the manuscript tracking screen. Questions can be sent to `mcom-query@ams.org`.

TEX files available. Beginning with the January 1992 issue of the *Bulletin* and the January 1996 issues of *Transactions, Proceedings, Mathematics of Computation*, and the *Journal of the AMS*, TEX files can be downloaded from the AMS website, starting from `www.ams.org/journals/`. Authors without Web access may request their files at the address given below after the article has been published. For *Bulletin* papers published in 1987 through 1991 and for *Transactions, Proceedings, Mathematics of Computation*, and the *Journal of the AMS* papers published in 1987 through 1995, TEX files are available upon request for authors without Web access by sending email to `file-request@ams.org` or by contacting the Electronic Prepress Department, American Mathematical Society, P.O. Box 6248, Providence, RI 02940-6248. The request should include the title of the paper, the name(s) of the author(s), the name of the publication in which the paper has or will appear, and the volume and issue numbers if known. The TEX file will be sent to the author making the request after the article goes to the printer. If the requestor can receive Internet email, please include the email address to which the file should be sent. Otherwise please indicate a diskette format and postal address to which a disk should be mailed. **Note:** Because TEX production at the AMS sometimes requires extra fonts and macros that are not yet publicly available, TEX files cannot be guaranteed to run through the author's version of TEX without errors. The AMS regrets that it cannot provide support to eliminate such errors in the author's TEX environment.

Inquiries. Any inquiries concerning a paper that has been accepted for publication that cannot be answered via the manuscript tracking system mentioned above should be sent to `mcom-query@ams.org` or directly to the Electronic Prepress Department, American Mathematical Society, P.O. Box 6248, Providence, RI 02940-6248.

Editorial Committee

STANLEY OSHER, Department of Mathematics, University of California, P. O. Box 951555, Los Angeles, CA 90095-1555; *E-mail*: sjo@math.ucla.edu

RENÉ SCHOOF, Dipartimento di Matematica, 2a Università di Roma "Tor Vergata", I-00133 Roma, Italy; *E-mail*: schoof@wins.uva.nl

LARS B. WAHLBIN, Chairman. Center for Applied Mathematics, 657 Frank H. T. Rhodes Hall, Cornell University, Ithaca, NY 14853-3801; *E-mail*: awahlbin@cam.cornell.edu

JOSEPH D. WARD, Department of Mathematics, Texas A&M University, College Station, TX 77843-3368; *E-mail*: jward@math.tamu.edu

Board of Associate Editors

RANDOLPH E. BANK, Department of Mathematics, University of California San Diego, C-012, La Jolla, CA 92093-0001; *E-mail*: reb@sdna2.ucsd.edu

DAVID W. BOYD, Department of Mathematics, University of British Columbia, Vancouver, BC Canada V6T 1Z2; *E-mail*: boyd@math.ubc.ca

SUSANNE C. BRENNER, Department of Mathematics, University of South Carolina, Columbia, SC 29208; *E-mail*: brenner@math.sc.edu

RICHARD P. BRENT, Oxford University Computing Laboratory, Wolfson Building, Parks Road, Oxford OX1 3QD, England; *E-mail*: Richard.Brent@comlab.ox.ac.uk

JOE P. BUHLER, Mathematical Sciences, Research Institute, 1000 Centennial Drive, Berkeley, CA 94720-5070; *E-mail*: jpb@msri.org

CARSTEN CARSTENSEN, Mathematisches Seminar, Christian-Albrechts-Universität zu Kiel, Ludewig-Meyn-Straße 4, D-24098 Kiel, Germany; *E-mail*: cc@numerik.uni-kiel.de

ARJEH M. COHEN, Faculteit Wiskunde en Informatica, TU Eindhoven, Postbus 513, 5600 MB Eindhoven, Netherlands; *E-mail*: amc@win.tue.nl

RONALD F. A. COOLS, Department of Computer Science, Katholieke Universiteit Leuven, Celestijnenlaan 200A, B-3001 Heverlee, Belgium; *E-mail*: ronald.cools@cs.kuleuven.ac.be

HOWARD ELMAN, Department of Computer Science, University of Maryland, College Park, MD 20742-0001; *E-mail*: elman@cs.umd.edu

RICHARD S. FALK, Department of Mathematics, Rutgers University, Hill Center, 110 Frelinghuysen Road, Piscataway, NJ 08854-8019; *E-mail*: falk@math.rutgers.edu

ANDREW J. GRANVILLE, Department of Mathematics, University of Georgia, Athens, GA 30602-7403; *E-mail*: andrew@math.uga.edu

DANIEL W. LOZIER, National Institute of Standards and Technology, 100 Bureau Drive, Mail Stop 8910, Gaithersburg, MD 20899-8910; *E-mail*: dlozier@nist.gov

ZHI-QUAN LUO, Department of Electrical and Computer Engineering, McMaster University, Room CRL/225, Hamilton, ON Canada L8S 4K1; *E-mail*: luozq@mcmail.cis.mcmaster.ca

ROSWITHA MÄRZ, Institut für Mathematik, Humboldt-Universität zu Berlin, Unter den Linden 6, D-10099 Berlin, Germany; *E-mail*: maerz@mathematik.hu-berlin.de

HARALD NIEDERREITER, Department of Mathematics, National University of Singapore, 2 Science Drive 2, Singapore 117543, Republic of Singapore; *E-mail*: nied@math.nus.edu.sg

RICARDO HORACIO NOCHETTO, Department of Mathematics, University of Maryland, Mathematics Building 084, College Park, MD 20742-0001; *E-mail*: rhn@math.umd.edu

HAESUN PARK, Department of Computer Science, University of Minnesota, 4-192 EE/CS, 200 Union Street, Minneapolis, MN 55455; *E-mail*: hpark@cs.umn.edu

JOSEPH E. PASCIAK, Department of Mathematics, Texas A&M University, 507B Blocker Hall, MS 3368, College Station, TX 77843; *E-mail*: pasciak@math.tamu.edu

LOTHAR REICHEL, Department of Mathematics & Computer Science, Kent State University, P.O. Box 5190, Kent, OH 44242-0001; *E-mail*: reichel@mcs.kent.edu

CHI-WANG SHU, Applied Mathematics Division, Brown University, P.O. Box F, 182 George St., Providence, RI 02912-0001; *E-mail*: shu@cfm.brown.edu

FRANK STENGER, School of Computing, University of Utah, Salt Lake City, UT 84112-1102; *E-mail*: stenger@cs.utah.edu

DENIS TALAY, INRIA, 2004 Route des Lucioles, BP 93, 06902 Sophia Antipolis Cedex, France; *E-mail*: talay@sophia.inria.fr

NICO M. TEMME, Centrum voor Wiskunde en Informatica, P.O. Box 94079, 1090-GB Amsterdam, Netherlands; *E-mail*: nicot@cwi.nl

HUGH C. WILLIAMS, Department of Computer Science, University of Manitoba, Winnipeg, Manitoba R3T 2N2 Canada; *E-mail*: Hugh_Williams@csmail.cs.umanitoba.ca

JINCHAO XU, Department of Mathematics, Pennsylvania State University, McAllister Building, University Park, PA 16802-6401; *E-mail*: xu@math.psu.edu

(Continued from back cover)

David P. Roberts, Density of cubic field discriminants 1699
Takashi Fukuda and Keiichi Komatsu, On Iwasawa λ_3-invariants of cyclic cubic fields of prime conductor 1707
David A. Clark and Norman C. Jarvis, Dense admissible sequences .. 1713
David H. Bailey and David J. Broadhurst, Parallel integer relation detection: Techniques and applications 1719
Pamela A. Cutter, Finding prime pairs with particular gaps 1737
Jörg Richstein, Verifying the Goldbach conjecture up to $4 \cdot 10^{14}$ 1745
Reviews and Descriptions of Tables and Books 1751
Patrick J. Rabier and Werner C. Rheinboldt **11**, Andrew R. Conn, Nicholas I. M. Gould, and Philippe L. Toint **12**, T. Kailath and A. H. Sayed, Editors **13**, Ian Blake, Gadiel Seroussi, and Nigel Smart **14**

No microfiche supplement in this issue

MATHEMATICS OF COMPUTATION

CONTENTS

Vol. 70, No. 236 October 2001

Carsten Carstensen and Stefan A. Funken, A posteriori error control in low-order finite element discretisations of incompressible stationary flow problems 1353

Elsa Liberman, A posteriori error estimator for a mixed finite element method for Reissner-Mindlin plate 1383

Claudio Canuto and Roland Masson, Stabilized wavelet approximations of the Stokes problem 1397

L. Halpern, A spectral method for the Stokes problem in three-dimensional unbounded domains 1417

Houde Han and Weizhu Bao, Error estimates for the finite element approximation of linear elastic equations in an unbounded domain ... 1437

Gabriel N. Gatica and Salim Meddahi, A dual-dual mixed formulation for nonlinear exterior transmission problems 1461

Stéphane Descombes, Convergence of a splitting method of high order for reaction-diffusion systems 1481

J.-P. Kauthen, The numerical solution of integral-algebraic equations of index 1 by polynomial spline collocation methods 1503

H. Faßbender, The parameterized SR algorithm for symplectic (butterfly) matrices 1515

L. Bos, M. A. Taylor, and B. A. Wingate, Tensor product Gauss-Lobatto points are Fekete points for the cube 1543

Ronald Cools and James N. Lyness, Three- and four-dimensional K-optimal lattice rules of moderate trigonometric degree 1549

Harald Niederreiter and Igor E. Shparlinski, On the distribution of inversive congruential pseudorandom numbers in parts of the period 1569

John B. Friedlander and Igor E. Shparlinski, On the distribution of the power generator 1575

John B. Friedlander, Carl Pomerance, and Igor E. Shparlinski, Period of the power generator and small values of Carmichael's function 1591

Sami Omar, Localization of the first zero of the Dedekind zeta function 1607

F. Thaine, Jacobi sums and new families of irreducible polynomials of Gaussian periods 1617

Sebastian Pauli and Xavier-François Roblot, On the computation of all extensions of a p-adic field of a given degree 1641

Samir Siksek, Sieving for rational points on hyperelliptic curves 1661

(*Continued on inside back cover*)

0025-5718(200110)70:236*;1-J