
VOLUME 71 NUMBER 240



OCTOBER 2002

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
Daniel W. Lozier
Zhi-Quan Luo
Roswitha März
Harald Niederreiter
Ricardo Horacio Nochetto
Stanley Osher
Haesun Park
Joseph E. Pasciak
Lothar Reichel
René Schoof
Igor E. Shparlinski
Chi-Wang Shu, *Managing Editor*
Frank Stenger
Denis Talay
Nico M. Temme
Lars B. Wahlbin
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 71 (2002) are as follows: for paper delivery, \$388 list, \$310 institutional member, \$349 corporate member, \$252 member of CBMS organizations; \$233 individual member; for electronic delivery, \$349 list, \$279 institutional member, \$314 corporate member, \$227 member of CBMS organizations, \$209 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 www.ams.org/bookstore.

Subscriptions and orders should be addressed to the American Mathematical Society, P.O. Box 845904, Boston, MA 02284-5904 USA. *All orders must be accompanied by payment.* Other correspondence should be addressed to 201 Charles Street, Providence, RI 02904-2294 USA.

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 Acquisitions Department, American Mathematical Society, 201 Charles Street, Providence, RI 02904-2294 USA. 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 USA. Periodicals postage is paid at Providence, Rhode Island. Postmaster: Send address changes to Mathematics of Computation, American Mathematical Society, 201 Charles Street, Providence, RI 02904-2294 USA.

© 2002 by the American Mathematical Society. All rights reserved.

This journal is indexed in *Mathematical Reviews*, *Zentralblatt MATH*, *Science Citation Index*[®], *Science Citation Index*TM-Expanded, *ISI Alerting Services*SM, *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 07 06 05 04 03 02

INDEX TO VOLUME 71 (2002)

- Abbott, John. *Sparse squares of polynomials*, 407
- Albert, Samuel, Cockburn, Bernardo, French, Donald A., and Peterson, Todd E. *A posteriori error estimates for general numerical methods for Hamilton-Jacobi equations. Part I: The steady state case*, 49
- Alfa, Attahiru Sule, Xue, Jungong, and Ye, Qiang. *Accurate computation of the smallest eigenvalue of a diagonally dominant M-matrix*, 217
- Arnold, Douglas N., Boffi, Daniele, and Falk, Richard S. *Approximation by quadrilateral finite elements*, 909
- Babuška, Ivo, and Chleboun, Jan. *Effects of uncertainties in the domain on the solution of Neumann boundary value problems in two spatial dimensions*, 1339
- Bakaev, Nikolai, and Ostermann, Alexander. *Long-term stability of variable stepsize approximations of semigroups*, 1545
- Bartels, Sören. *See Carstensen, Carsten*
- Bartels, Sören, and Carstensen, Carsten. *Each averaging technique yields reliable a posteriori error control in FEM on unstructured grids. Part II: Higher order FEM*, 971
- Ben-Israel, Adi. *See Levin, Yuri*
- Bermúdez, Alfredo, and Rodríguez, Rodolfo. *Analysis of a finite element method for pressure/potential formulation of elastoacoustic spectral problems*, 537
- Bernardi, Christine, and Hecht, Frédéric. *Error indicators for the mortar finite element discretization of the Laplace equation*, 1371
- Boffi, Daniele. *See Arnold, Douglas N.*
- Boros, George, and Moll, Victor H. *Landen transformations and the integration of rational functions*, 649
- Borwein, Peter, and Hare, Kevin G. *Some computations on the spectra of Pisot and Salem numbers*, 767
- Boyd, David W. *On a problem of Byrnes concerning polynomials with restricted coefficients, II*, 1205
- Bramble, James H., Pasciak, Joseph E., and Steinbach, Olaf. *On the stability of the L^2 projection in $H^1(\Omega)$* , 147
- Brenner, Susanne C. *Convergence of the multigrid V-cycle algorithm for second-order boundary value problems without full elliptic regularity*, 507
- Caldwell, Chris K., and Gallot, Yves. *On the primality of $n! \pm 1$ and $2 \times 3 \times 5 \times \cdots \times p \pm 1$* , 441
- Calvo, M. P., and Palencia, C. *Avoiding the order reduction of Runge-Kutta methods for linear initial boundary value problems*, 1529
- Campillo, A., and Farrán, J. I. *Symbolic Hamburger-Noether expressions of plane curves and applications to AG codes*, 1759
- Carstensen, Carsten. *Merging the Bramble-Pasciak-Steinbach and the Crouzeix-Thomé criterion for H^1 -stability of the L^2 -projection onto finite element spaces*, 157
- . *See Bartels, Sören*
- Carstensen, Carsten, and Bartels, Sören. *Each averaging technique yields reliable a posteriori error control in FEM on unstructured grids. Part I: Low order conforming, nonconforming, and mixed FEM*, 945
- Castillo, Paul, Cockburn, Bernardo, Schötzau, Dominik, and Schwab, Christoph. *Optimal a priori error estimates for the hp-version of the local discontinuous Galerkin method for convection-diffusion problems*, 455
- Chleboun, Jan. *See Babuška, Ivo*
- Cockburn, Bernardo. *See Albert, Samuel*
- . *See Castillo, Paul*
- Cohen, Myra B., Colbourn, Charles J., Ives, Lee A., and Ling, Alan C. H. *Kirkman triple systems of order 21 with nontrivial automorphism group*, 873
- Colbourn, Charles J. *See Cohen, Myra B.*
- Coorevits, Patrice, Hild, Patrick, Lhalouani, Khalid, and Sassi, Taoufik. *Mixed finite element methods for unilateral problems: convergence analysis and numerical studies*, 1
- Darusis, Leyla, González-Vera, Pablo, and Njåstad, Olav. *Szegő quadrature formulas for certain Jacobi-type weight functions*, 683
- De Bonis, M. C., Della Vecchia, B., and Mastroianni, G. *Approximation of the Hilbert transform on the real line using Hermite zeros*, 1169
- Della Vecchia, B. *See De Bonis, M. C.*

- Deutsch, Jesse Ira. *A computational approach to Hilbert modular group fixed points*, 1271
- Dräxler, Peter, and Kögerler, Klara. *An algorithm for finding all preprojective components of the Auslander-Reiten quiver*, 743
- Druskin, Vladimir, and Moskow, Shari. *Three-point finite-difference schemes, Padé and the spectral Galerkin method. I. One-sided impedance approximation*, 995
- Dubner, H., Forbes, T., Lygeros, N., Mizony, M., Nelson, H., and Zimmermann, P. *Ten consecutive primes in arithmetic progression*, 1323
- Dubner, Harvey. *Repunit R49081 is a probable prime*, 833
- Dubner, Harvey, and Gallot, Yves. *Distribution of generalized Fermat prime numbers*, 825
- Dusart, Pierre. *Estimates of $\theta(x; k, l)$ for large values of x* , 1137
- E, Weinan, and Liu, Jian-Guo. *Projection method III: Spatial discretization on the staggered grid*, 27
- Emmerich, Frank. *Average equidistribution and statistical independence properties of digital inverse pseudorandom numbers over parts of the period*, 781
- Enge, Andreas. *Computing discrete logarithms in high-genus hyperelliptic Jacobians in provably subexponential time*, 729
- Enge, Andreas, and Stein, Andreas. *Smooth ideals in hyperelliptic function fields*, 1219
- Entacher, Karl, Schell, Thomas, and Uhl, Andreas. *Efficient lattice assessment for LCG and GLP parameter searches*, 1231
- Estep, Donald J., and Stuart, Andrew M. *The dynamical behavior of the discontinuous Galerkin method and related difference schemes*, 1075
- Everest, G., Gaál, I., Györy, K., and Röttger, C. *On the spatial distribution of solutions of decomposable form equations*, 633
- Falk, Richard S. *See Arnold, Douglas N.*
- Fang, Kai-Tai, Ma, Chang-Xing, and Winker, Peter. *Centered L_2 -discrepancy of random sampling and Latin hypercube design, and construction of uniform designs*, 275
- Farmer, D. W., and James, K. *The irreducibility of some level 1 Hecke polynomials*, 1263
- Farrán, J. I. *See Campillo, A.*
- Fok, Johnson C. M., Guo, Benyu, and Tang, Tao. *Combined Hermite spectral-finite difference method for the Fokker-Planck equation*, 1497
- Forbes, T. *See Dubner, H.*
- Forbes, Tony. *Fifteen consecutive integers with exactly four prime factors*, 449
- Fournier, Nicolas, and Méléard, Sylvie. *A stochastic particle numerical method for 3D Boltzmann equations without cutoff*, 583
- Freistühler, Heinrich, and Rohde, Christian. *Numerical computation of viscous profiles for hyperbolic conservation laws*, 1021
- French, Donald A. *See Albert, Samuel*
- Friedlander, John B., Pomerance, Carl, and Shparlinski, Igor E. *Corrigendum to "Period of the power generator and small values of Carmichael's function"*, 1803
- Gaál, I. *See Everest, G.*
- Gaál, István, and Pohst, Michael. *On the resolution of relative Thue equations*, 429
- Galbraith, S. D., Paulus, S. M., and Smart, N. P. *Arithmetic on superelliptic curves*, 393
- Gallot, Yves. *See Caldwell, Chris K.*
- . *See Dubner, Harvey*
- Gao, Shuhong, and Lauder, Alan G. B. *Hensel lifting and bivariate polynomial factorisation over finite fields*, 1663
- von zur Gathen, Joachim, and Gerhard, Jürgen. *Polynomial factorization over \mathbb{F}_2* , 1677
- Gatica, Gabriel N., and Heuer, Norbert. *Conjugate gradient method for dual-dual mixed formulations*, 1455
- Gerhard, Jürgen. *See von zur Gathen, Joachim*
- Girault, V., and Scott, L. R. *Hermite interpolation of nonsmooth functions preserving boundary conditions*, 1043
- Göbel, Manfred. *Finite SAGBI bases for polynomial invariants of conjugates of alternating groups*, 761
- González, C., Ostermann, A., Palencia, C., and Thalhammer, M. *Backward Euler discretization of fully nonlinear parabolic problems*, 125
- González Vasco, Maria Isabel, and Shparlinski, Igor E. *Security of the most significant bits of the Shamir message passing scheme*, 333

- González-Vera, Pablo. *See* Daruis, Leyla
- Gosse, Laurent. *Localization effects and measure source terms in numerical schemes for balance laws*, 553
- Gragg, William B. *See* Wang, Tai-Lin
- Granville, Andrew, and Pomerance, Carl. *Two contradictory conjectures concerning Carmichael numbers*, 883
- Gray, Norman. *Automatic reduction of elliptic integrals using Carlson's relations*, 311
- Guimond, Louis-Sébastien, and Patera, Jiří. *Proving the deterministic period breaking of linear congruential generators using two tile quasicrystals*, 319
- Guo, Benyu. *See* Fok, Johnson C. M.
- Györy, K. *See* Everest, G.
- Han, Bin, and Jia, Rong-Qing. *Quincunx fundamental refinable functions and quincunx biorthogonal wavelets*, 165
- Hare, Kevin G. *See* Borwein, Peter
- Havu, Ville, and Pitkäranta, Juhani. *Analysis of a bilinear finite element for shallow shells I: Approximation of inextensional deformations*, 923
- Hecht, Frédéric. *See* Bernardi, Christine
- Heuer, Norbert. *See* Gatica, Gabriel N.
- Hickernell, Fred J., and Wang, Xiaoqun. *The error bounds and tractability of quasi-Monte Carlo algorithms in infinite dimension*, 1641
- Hild, Patrick. *See* Coorevits, Patrice
- Holden, Joshua. *Comparison of algorithms to calculate quadratic irregularity of prime numbers*, 863
- Hough, David M. *Asymptotic estimation of Gaussian quadrature error for a nonsingular integral in potential theory*, 717
- Ives, Lee A. *See* Cohen, Myra B.
- James, K. *See* Farmer, D. W.
- Jia, Rong-Qing. *See* Han, Bin
- Joe, S. *See* Sloan, I. H.
- Katz, I. Norman. *See* Markman, Jerry
- Kim, Hyun Kwang, and Kim, Jung Soo. *Evaluation of zeta function of the simplest cubic field at negative odd integers*, 1243
- Kim, Jung Soo. *See* Kim, Hyun Kwang
- Kögerler, Klara. *See* Dräxler, Peter
- Kohl, Timothy, and Replogle, Daniel R. *Computation of several cyclotomic Swan subgroups*, 343
- Kohnen, Winfried, and Kuß, Michael. *Some numerical computations concerning spinor zeta functions in genus 2 at the central point*, 1597
- Krejić, Nataša, and Lužanin, Zorana. *Newton-like method with modification of the right-hand-side vector*, 237
- Kumada, Toshihiro, Leeb, Hannes, Kurita, Yoshiharu, and Matsumoto, Makoto. *Corrigenda to "New primitive t -nomials ($t = 3, 5$) over $GF(2)$ whose degree is a Mersenne exponent," and some new primitive pentanomials*, 1337
- Kuo, F. Y. *See* Sloan, I. H.
- Kurita, Yoshiharu. *See* Kumada, Toshihiro
- Kuß, Michael. *See* Kohnen, Winfried
- Lauder, Alan G. B. *See* Gao, Shuhong
- Leeb, Hannes. *Asymptotic properties of the spectral test, diaphony, and related quantities*, 297
 ———. *See* Kumada, Toshihiro
- Levin, Yuri, and Ben-Israel, Adi. *Directional Newton methods in n variables*, 251
- Lhalouani, Khalid. *See* Coorevits, Patrice
- Ling, Alan C. H. *See* Cohen, Myra B.
- Liu, Jian-Guo. *See* E, Weinan
- Louboutin, Stéphane. *Computation of class numbers of quadratic number fields*, 1735
- Lužanin, Zorana. *See* Krejić, Nataša
- Lygeros, N. *See* Dubner, H.
- Ma, Chang-Xing. *See* Fang, Kai-Tai

- Markman, Jerry, and Katz, I. Norman. *Convergence of an iterative algorithm for solving Hamilton-Jacobi type equations*, 77
- März, Roswitha, and Rodríguez-Santiesteban, Antonio R. *Analyzing the stability behaviour of solutions and their approximations in case of index-2 differential-algebraic systems*, 605
- Mastroianni, G. *See* De Bonis, M. C.
- Matsumoto, Makoto. *See* Kumada, Toshihiro
- Matthews, Keith. *Thue's theorem and the diophantine equation $x^2 - Dy^2 = \pm N$* , 1281
- de la Maza, Ana-Cecilia. *Bounds for the smallest norm in an ideal class*, 1745
- Meini, Beatrice. *Efficient computation of the extreme solutions of $X + A^*X^{-1}A = Q$ and $X - A^*X^{-1}A = Q$* , 1189
- Méléard, Sylvie. *See* Fournier, Nicolas
- Meuser, Diane, and Robinson, Margaret. *The Igusa local zeta functions of elliptic curves*, 815
- Mhaskar, H. N., Narcowich, F. J., and Ward, J. D. *Corrigendum to "Spherical Marcinkiewicz-Zygmund inequalities and positive quadrature"*, 453
- Mizony, M. *See* Dubner, H.
- Moll, Victor H. *See* Boros, George
- Moskow, Shari. *See* Druskin, Vladimir
- Narcowich, F. J. *See* Mhaskar, H. N.
- Nelson, H. *See* Dubner, H.
- Neymeyr, Klaus. *A geometric theory for preconditioned inverse iteration applied to a subspace*, 197
- Njåstad, Olav. *See* Daruis, Leyla
- Nochetto, Ricardo H., and Wahlbin, Lars B. *Positivity preserving finite element approximation*, 1405
- Ostermann, A. *See* González, C.
- Ostermann, Alexander. *See* Bakaev, Nikolai
- Oudshoorn, W. R., and van der Put, M. *Lie symmetries and differential Galois groups of linear equations*, 349
- Palencia, C. *See* Calvo, M. P.
- . *See* González, C.
- Pasciak, Joseph E. *See* Bramble, James H.
- Paszkievicz, A., and Schinzel, A. *On the least prime primitive root modulo a prime*, 1307
- . *Numerical calculation of the density of prime numbers with a given least primitive root*, 1781
- Patera, Jiří. *See* Guimond, Louis-Sébastien
- Paulus, S. M. *See* Galbraith, S. D.
- Peterson, Todd E. *See* Albert, Samuel
- Pitkäranta, Juhani. *See* Havu, Ville
- Pohst, Michael. *See* Gaál, István
- Pomerance, Carl. *See* Friedlander, John B.
- . *See* Granville, Andrew
- van der Put, M. *See* Oudshoorn, W. R.
- Replogle, Daniel R. *See* Kohl, Timothy
- Reztsov, A. V. *See* Sloan, I. H.
- Richter, Gerard R. *On the stability of a family of finite element methods for hyperbolic problems*, 527
- Robinson, Margaret. *See* Meuser, Diane
- Rodríguez, Rodolfo. *See* Bermúdez, Alfredo
- Rodríguez-Santiesteban, Antonio R. *See* März, Roswitha
- Rohde, Christian. *See* Freistühler, Heinrich
- Röttger, C. *See* Everest, G.
- Sassi, Taoufik. *See* Coorevits, Patrice
- Schaback, Robert, and Wendland, Holger. *Inverse and saturation theorems for radial basis function interpolation*, 669
- Schell, Thomas. *See* Entacher, Karl
- Schinzel, A. *See* Paszkievicz, A.
- Schötzau, Dominik. *See* Castillo, Paul
- Schwab, Christoph. *See* Castillo, Paul

- Scott, L. R. *See* Girault, V.
- Semaev, Igor A. *Special prime numbers and discrete logs in finite prime fields*, 363
- Shparlinski, Igor E. *See* Friedlander, John B.
- . *See* González Vasco, Maria Isabel
- Sidi, Avram. *New convergence results on the generalized Richardson extrapolation process GREP⁽¹⁾ for logarithmic sequences*, 1569
- Simalarides, Anastasios. *Upper bounds for the prime divisors of Wendt's determinant*, 415
- Simon, Denis. *Solving norm equations in relative number fields using S -units*, 1287
- Sloan, I. H., Kuo, F. Y., and Joe, S. *On the step-by-step construction of quasi-Monte Carlo integration rules that achieve strong tractability error bounds in weighted Sobolev spaces*, 1609
- Sloan, I. H., and Reztsov, A. V. *Component-by-component construction of good lattice rules*, 263
- Smart, N. P. *See* Galbraith, S. D.
- Stefanelli, Ulisse. *Analysis of a variable time-step discretization of the three-dimensional Frémond model for shape memory alloys*, 1431
- Stein, Andreas. *See* Enge, Andreas
- Stein, Andreas, and Teske, Edlyn. *The parallelized Pollard kangaroo method in real quadratic function fields*, 793
- . *Explicit bounds and heuristics on class numbers in hyperelliptic function fields*, 837
- Steinbach, Olaf. *See* Bramble, James H.
- Stinson, D. R. *Some baby-step giant-step algorithms for the low hamming weight discrete logarithm problem*, 379
- Stuart, Andrew M. *See* Estep, Donald J.
- Suda, Reiji, and Takami, Masayasu. *A fast spherical harmonics transform algorithm*, 703
- Tai, Xue-Cheng, and Tseng, Paul. *Convergence rate analysis of an asynchronous space decomposition method for convex minimization*, 1105
- Tai, Xue-Cheng, and Xu, Jinchao. *Global and uniform convergence of subspace correction methods for some convex optimization problems*, 105
- Takami, Masayasu. *See* Suda, Reiji
- Tang, Tao. *See* Fok, Johnson C. M.
- Teske, Edlyn. *See* Stein, Andreas
- Thalhammer, M. *See* González, C.
- Tseng, Paul. *See* Tai, Xue-Cheng
- Uhl, Andreas. *See* Entacher, Karl
- Wahlbin, Lars B. *See* Nochetto, Ricardo H.
- Wang, Tai-Lin, and Gragg, William B. *Convergence of the shifted QR algorithm for unitary Hessenberg matrices*, 1473
- Wang, Xiaoqun. *See* Hickernell, Fred J.
- Ward, J. D. *See* Mhaskar, H. N.
- Wendland, Holger. *See* Schaback, Robert
- Winker, Peter. *See* Fang, Kai-Tai
- Xu, Jinchao. *See* Tai, Xue-Cheng
- Xue, Jungong. *See* Alfa, Attahiru Sule
- Ye, Qiang. *See* Alfa, Attahiru Sule
- Zhang, Zhenxiang. *A one-parameter quadratic-base version of the Baillie-PSW probable prime test*, 1699
- Zhang, Zhimin. *Derivative superconvergent points in finite element solutions of harmonic functions—A theoretical justification*, 1421
- Zimmermann, P. *See* Dubner, H.
- Zulehner, Walter. *Analysis of iterative methods for saddle point problems: a unified approach*, 479

INDEX OF REVIEWS BY AUTHOR OF WORK REVIEWED

<i>Author</i>	<i>Review Number</i>	<i>Classification</i>	<i>Page</i>
BAI, ZHAOJUN, DEMMEL, JAMES, DONGARRA, JACK, RUHE, AXEL, & VAN DER VORST, HENK (EDITORS)	3	65-02, 65F15	1330
BUSENHART, HEDWIG ULMER	1	See KREISS, HEINZ-OTTO	1329
3 See BAI, ZHAOJUN		1330	
DEVORE, RONALD A., ISERLES, ARIEH, & SÚLI, ENDRE (EDITORS)	2	65-02	1329
3 See BAI, ZHAOJUN		1330	
2 See DEVORE, RONALD A.		1329	
KAMINSKI, D.	7	See PARI, R. B.	1799
KREISS, HEINZ-OTTO, & BUSENHART, HEDWIG ULMER	1	35F10, 35K15, 65M06, 65M12	1329
LAM, KWOK-YAN, SHPARLINSKI, IGOR, WANG, HUAXIONG, & XING, CHAOPING (EDITORS)	6	11Yxx, 11Txx, 94Axx, 68P25	1334
PARI, R. B., & KAMINSKI, D.	7	41A60, 33-02, 33Cxx, 30E15	1799
3 See BAI, ZHAOJUN		1330	
SAPIRO, GUILLERMO	4	35Q80, 49-01, 53-01, 65D99, 68U10	1331
6 See LAM, KWOK-YAN		1334	
2 See DEVORE, RONALD A.		1329	
3 See BAI, ZHAOJUN		1330	
6 See LAM, KWOK-YAN		1334	
6 See LAM, KWOK-YAN		1334	
YAP, CHEE KENG	5	68W30, 11Yxx, 12Y05, 13Pxx	1333

INDEX OF REVIEWS BY SUBJECT OF WORK REVIEWED

<i>Author</i>	<i>Review Number</i>	<i>Title</i>	<i>Page</i>
11-XX Number theory			
11Txx <i>Finite fields and commutative rings (number-theoretic aspects)</i>			
LAM, KWOK-YAN, SHPARLINSKI, IGOR, WANG, HUAXIONG, & XING, CHAOPING (EDITORS)	6	Cryptography and computational number theory	1334
11Yxx <i>Computational number theory</i>			
LAM, KWOK-YAN, SHPARLINSKI, IGOR, WANG, HUAXIONG, & XING, CHAOPING (EDITORS)	6	Cryptography and computational number theory	1334
YAP, CHEE KENG	5	Fundamental problems of algorithmic algebra	1333

12-XX Field theory and polynomials

12Y05 *Computational aspects of field theory and polynomials*

YAP, CHEE KENG 5 [Fundamental problems of algorithmic algebra](#) 1333

13-XX Commutative rings and algebras

13Pxx *Computational aspects of commutative algebra*

YAP, CHEE KENG 5 [Fundamental problems of algorithmic algebra](#) 1333

30-XX Functions of a complex variable

30E15 *Asymptotic representations in the complex domain*

PARI, R. B., & KAMINSKI, D. 7 [Asymptotics and Mellin–Barnes integrals](#) 1799

33-XX Special functions

33-02 *Research exposition (monographs, survey articles)*

PARI, R. B., & KAMINSKI, D. 7 [Asymptotics and Mellin–Barnes integrals](#) 1799

33Cxx *Hypergeometric functions*

PARI, R. B., & KAMINSKI, D. 7 [Asymptotics and Mellin–Barnes integrals](#) 1799

35-XX Partial differential equations

35F10 *Initial value problems for linear first-order PDE, linear evolution equations*

KREISS, HEINZ-OTTO, & BUSENHART, HEDWIG ULMER 1 [Time-dependent partial differential equations and their numerical solution](#) 1329

35K15 *Initial value problems for second-order, parabolic equations*

KREISS, HEINZ-OTTO, & BUSENHART, HEDWIG ULMER 1 [Time-dependent partial differential equations and their numerical solution](#) 1329

35Q80 *Applications of PDE in areas other than physics*

SAPIRO, GUILLERMO 4 [Geometric partial differential equations and image analysis](#) 1331

41-XX Approximations and expansions

41A60 *Asymptotic approximations, asymptotic expansions (steepest descent, etc.)*

PARI, R. B., & KAMINSKI, D. 7 [Asymptotics and Mellin–Barnes integrals](#) 1799

49-XX Calculus of variations and optimal control; optimization

49-01 *Instructional exposition (textbooks, tutorial papers, etc.)*

SAPIRO, GUILLERMO 4 [Geometric partial differential equations and image analysis](#) 1331

53-XX Differential geometry

53-01 *Instructional exposition (textbooks, tutorial papers, etc.)*

SAPIRO, GUILLERMO 4 [Geometric partial differential equations and image analysis](#) 1331

INDEX OF REVIEWS BY SUBJECT OF WORK REVIEWED

65-XX Numerical analysis

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

BAI, ZHAOJUN, DEMMEL, JAMES, 3 [Templates for the solution of algebraic](#)
DONGARRA, JACK, [eigenvalue problems, a practical guide](#) 1330
RUHE, AXEL, &
VAN DER VORST, HENK
(EDITORS)

DEVORE, RONALD A., 2 [Foundations of computational mathemat-](#)
ISERLES, ARIEH, & [ics](#) 1329
SÚLI, ENDRE (EDITORS)

65D99 *None of the above, but in this section*

SAPIRO, GUILLERMO 4 [Geometric partial differential equations and](#)
[image analysis](#) 1331

65F15 *Eigenvalues, eigenvectors*

BAI, ZHAOJUN, DEMMEL, JAMES, 3 [Templates for the solution of algebraic](#)
DONGARRA, JACK, [eigenvalue problems, a practical guide](#) 1330
RUHE, AXEL, &
VAN DER VORST, HENK
(EDITORS)

65M06 *Finite difference methods*

KREISS, HEINZ-OTTO, & 1 [Time-dependent partial differential equa-](#)
BUSENHART, HEDWIG ULMER [tions and their numerical solution](#) 1329

65M12 *Stability and convergence of numerical methods*

KREISS, HEINZ-OTTO, & 1 [Time-dependent partial differential equa-](#)
BUSENHART, HEDWIG ULMER [tions and their numerical solution](#) 1329

68-XX Computer science

68P25 *Data encryption*

LAM, KWOK-YAN, 6 [Cryptography and computational number](#)
SHPARLINSKI, IGOR, [theory](#) 1334
WANG, HUAXIONG, &
XING, CHAOPING (EDITORS)

68U10 *Image processing*

SAPIRO, GUILLERMO 4 [Geometric partial differential equations and](#)
[image analysis](#) 1331

68W30 *Symbolic computation and algebraic computation*

YAP, CHEE KENG 5 [Fundamental problems of algorithmic alge-](#)
[bra](#) 1333

94-XX Information and communication, circuits

94Axx *Communication, information*

LAM, KWOK-YAN, 6 [Cryptography and computational number](#)
SHPARLINSKI, IGOR, [theory](#) 1334
WANG, HUAXIONG, &
XING, CHAOPING (EDITORS)

INDEX OF TABLE ERRATA

INDEX OF TABLE ERRATA

<i>No.</i>	<i>Author</i>	<i>Title</i>	<i>Page</i>
636	GRADSHTEYN, I. S., & RYZHIK, I. M.	Table of integrals, series, and products	1335
637	GRADSHTEYN, I. S., & RYZHIK, I. M.	Table of integrals, series, and products	1335
638	ABRAMOWITZ, M., & STEGUN, I.	Handbook of mathematical functions with formulas, graphs, and mathematical tables . .	1801



MATHEMATICS OF COMPUTATION

A M E R I C A N M A T H E M A T I C A L S O C I E T Y

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
Daniel W. Lozier
Zhi-Quan Luo
Roswitha März
Harald Niederreiter
Ricardo Horacio Nochetto
Stanley Osher
Haesun Park
Joseph E. Pasciak
Lothar Reichel
René Schoof
Igor E. Shparlinski
Chi-Wang Shu, *Managing Editor*
Frank Stenger
Denis Talay
Nico M. Temme
Lars B. Wahlbin
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 71 (2002) are as follows: for paper delivery, \$388 list, \$310 institutional member, \$349 corporate member, \$252 member of CBMS organizations; \$233 individual member; for electronic delivery, \$349 list, \$279 institutional member, \$314 corporate member, \$227 member of CBMS organizations, \$209 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 www.ams.org/bookstore.

Subscriptions and orders should be addressed to the American Mathematical Society, P.O. Box 845904, Boston, MA 02284-5904 USA. *All orders must be accompanied by payment.* Other correspondence should be addressed to 201 Charles Street, Providence, RI 02904-2294 USA.

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 Acquisitions Department, American Mathematical Society, 201 Charles Street, Providence, RI 02904-2294 USA. 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 USA. Periodicals postage is paid at Providence, Rhode Island. Postmaster: Send address changes to Mathematics of Computation, American Mathematical Society, 201 Charles Street, Providence, RI 02904-2294 USA.

© 2002 by the American Mathematical Society. All rights reserved.

This journal is indexed in *Mathematical Reviews*, *Zentralblatt MATH*, *Science Citation Index*[®], *Science Citation Index*TM-Expanded, *ISI Alerting Services*SM, *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 07 06 05 04 03 02

MATHEMATICS OF COMPUTATION

CONTENTS

Vol. 71, No. 237

January 2002

Patrice Coorevits, Patrick Hild, Khalid Lhalouani, and Taoufik Sassi , Mixed finite element methods for unilateral problems: convergence analysis and numerical studies	1
Weinan E and Jian-Guo Liu , Projection method III: Spatial discretization on the staggered grid	27
Samuel Albert, Bernardo Cockburn, Donald A. French, and Todd E. Peterson , A posteriori error estimates for general numerical methods for Hamilton-Jacobi equations. Part I: The steady state case	49
Jerry Markman and I. Norman Katz , Convergence of an iterative algorithm for solving Hamilton-Jacobi type equations	77
Xue-Cheng Tai and Jinchao Xu , Global and uniform convergence of subspace correction methods for some convex optimization problems ..	105
C. González, A. Ostermann, C. Palencia, and M. Thalhammer , Backward Euler discretization of fully nonlinear parabolic problems ..	125
James H. Bramble, Joseph E. Pasciak, and Olaf Steinbach , On the stability of the L^2 projection in $H^1(\Omega)$	147
Carsten Carstensen , Merging the Bramble-Pasciak-Steinbach and the Crouzeix-Thomé criterion for H^1 -stability of the L^2 -projection onto finite element spaces	157
Bin Han and Rong-Qing Jia , Quincunx fundamental refinable functions and quincunx biorthogonal wavelets	165
Klaus Neymeyr , A geometric theory for preconditioned inverse iteration applied to a subspace	197
Attahiru Sule Alfa, Jungong Xue, and Qiang Ye , Accurate computation of the smallest eigenvalue of a diagonally dominant M -matrix	217
Nataša Krejić and Zorana Lužanin , Newton-like method with modification of the right-hand-side vector	237
Yuri Levin and Adi Ben-Israel , Directional Newton methods in n variables	251
I. H. Sloan and A. V. Reztsov , Component-by-component construction of good lattice rules	263
Kai-Tai Fang, Chang-Xing Ma, and Peter Winker , Centered L_2 -discrepancy of random sampling and Latin hypercube design, and construction of uniform designs	275
Hannes Leeb , Asymptotic properties of the spectral test, diaphony, and related quantities	297
Norman Gray , Automatic reduction of elliptic integrals using Carlson's relations	311
Louis-Sébastien Guimond and Jiří Patera , Proving the deterministic period breaking of linear congruential generators using two tile quasicrystals	319
Maria Isabel González Vasco and Igor E. Shparlinski , Security of the most significant bits of the Shamir message passing scheme	333

Timothy Kohl and Daniel R. Replogle , Computation of several cyclotomic Swan subgroups	343
W. R. Oudshoorn and M. van der Put , Lie symmetries and differential Galois groups of linear equations	349
Igor A. Semaev , Special prime numbers and discrete logs in finite prime fields	363
D. R. Stinson , Some baby-step giant-step algorithms for the low hamming weight discrete logarithm problem	379
S. D. Galbraith, S. M. Paulus, and N. P. Smart , Arithmetic on superelliptic curves	393
John Abbott , Sparse squares of polynomials	407
Anastasios Simalarides , Upper bounds for the prime divisors of Wendt's determinant	415
István Gaál and Michael Pohst , On the resolution of relative Thue equations	429
Chris K. Caldwell and Yves Gallot , On the primality of $n! \pm 1$ and $2 \times 3 \times 5 \times \cdots \times p \pm 1$	441
Tony Forbes , Fifteen consecutive integers with exactly four prime factors .	449
H. N. Mhaskar, F. J. Narcowich, and J. D. Ward , Corrigendum to "Spherical Marcinkiewicz-Zygmund inequalities and positive quadrature"	453

Vol. 71, No. 238

April 2002

Paul Castillo, Bernardo Cockburn, Dominik Schötzau, and Christoph Schwab , Optimal a priori error estimates for the hp -version of the local discontinuous Galerkin method for convection–diffusion problems	455
Walter Zulehner , Analysis of iterative methods for saddle point problems: a unified approach	479
Susanne C. Brenner , Convergence of the multigrid V -cycle algorithm for second-order boundary value problems without full elliptic regularity .	507
Gerard R. Richter , On the stability of a family of finite element methods for hyperbolic problems	527
Alfredo Bermúdez and Rodolfo Rodríguez , Analysis of a finite element method for pressure/potential formulation of elastoacoustic spectral problems	537
Laurent Gosse , Localization effects and measure source terms in numerical schemes for balance laws	553
Nicolas Fournier and Sylvie Méléard , A stochastic particle numerical method for 3D Boltzmann equations without cutoff	583
Roswitha März and Antonio R. Rodríguez-Santesteban , Analyzing the stability behaviour of solutions and their approximations in case of index-2 differential-algebraic systems	605
G. Everest, I. Gaál, K. Györy, and C. Röttger , On the spatial distribution of solutions of decomposable form equations	633

George Boros and Victor H. Moll , Landen transformations and the integration of rational functions	649
Robert Schaback and Holger Wendland , Inverse and saturation theorems for radial basis function interpolation	669
Leyla Daruis, Pablo González-Vera, and Olav Njåstad , Szegő quadrature formulas for certain Jacobi-type weight functions	683
Reiji Suda and Masayasu Takami , A fast spherical harmonics transform algorithm	703
David M. Hough , Asymptotic estimation of Gaussian quadrature error for a nonsingular integral in potential theory	717
Andreas Enge , Computing discrete logarithms in high-genus hyperelliptic Jacobians in provably subexponential time	729
Peter Dräxler and Klara Kögerler , An algorithm for finding all preprojective components of the Auslander-Reiten quiver	743
Manfred Göbel , Finite SAGBI bases for polynomial invariants of conjugates of alternating groups	761
Peter Borwein and Kevin G. Hare , Some computations on the spectra of Pisot and Salem numbers	767
Frank Emmerich , Average equidistribution and statistical independence properties of digital inversive pseudorandom numbers over parts of the period	781
Andreas Stein and Edlyn Teske , The parallelized Pollard kangaroo method in real quadratic function fields	793
Diane Meuser and Margaret Robinson , The Igusa local zeta functions of elliptic curves	815
Harvey Dubner and Yves Gallot , Distribution of generalized Fermat prime numbers	825
Harvey Dubner , Repunit R49081 is a probable prime	833
Andreas Stein and Edlyn Teske , Explicit bounds and heuristics on class numbers in hyperelliptic function fields	837
Joshua Holden , Comparison of algorithms to calculate quadratic irregularity of prime numbers	863
Myra B. Cohen, Charles J. Colbourn, Lee A. Ives, and Alan C. H. Ling , Kirkman triple systems of order 21 with nontrivial automorphism group	873
Andrew Granville and Carl Pomerance , Two contradictory conjectures concerning Carmichael numbers	883

Douglas N. Arnold, Daniele Boffi, and Richard S. Falk , Approximation by quadrilateral finite elements	909
Ville Havu and Juhani Pitkäranta , Analysis of a bilinear finite element for shallow shells I: Approximation of inextensional deformations	923

Carsten Carstensen and Sören Bartels , Each averaging technique yields reliable a posteriori error control in FEM on unstructured grids. Part I: Low order conforming, nonconforming, and mixed FEM	945
Sören Bartels and Carsten Carstensen , Each averaging technique yields reliable a posteriori error control in FEM on unstructured grids. Part II: Higher order FEM	971
Vladimir Druskin and Shari Moskow , Three-point finite-difference schemes, Padé and the spectral Galerkin method. I. One-sided impedance approximation	995
Heinrich Freistühler and Christian Rohde , Numerical computation of viscous profiles for hyperbolic conservation laws	1021
V. Girault and L. R. Scott , Hermite interpolation of nonsmooth functions preserving boundary conditions	1043
Donald J. Estep and Andrew M. Stuart , The dynamical behavior of the discontinuous Galerkin method and related difference schemes	1075
Xue-Cheng Tai and Paul Tseng , Convergence rate analysis of an asynchronous space decomposition method for convex minimization ..	1105
Pierre Dusart , Estimates of $\theta(x; k, l)$ for large values of x	1137
M. C. De Bonis, B. Della Vecchia, and G. Mastroianni , Approximation of the Hilbert transform on the real line using Hermite zeros	1169
Beatrice Meini , Efficient computation of the extreme solutions of $X + A^*X^{-1}A = Q$ and $X - A^*X^{-1}A = Q$	1189
David W. Boyd , On a problem of Byrnes concerning polynomials with restricted coefficients, II	1205
Andreas Enge and Andreas Stein , Smooth ideals in hyperelliptic function fields	1219
Karl Entacher, Thomas Schell, and Andreas Uhl , Efficient lattice assessment for LCG and GLP parameter searches	1231
Hyun Kwang Kim and Jung Soo Kim , Evaluation of zeta function of the simplest cubic field at negative odd integers	1243
D. W. Farmer and K. James , The irreducibility of some level 1 Hecke polynomials	1263
Jesse Ira Deutsch , A computational approach to Hilbert modular group fixed points	1271
Keith Matthews , Thue's theorem and the diophantine equation $x^2 - Dy^2 = \pm N$	1281
Denis Simon , Solving norm equations in relative number fields using S -units	1287
A. Paszkiewicz and A. Schinzel , On the least prime primitive root modulo a prime	1307
H. Dubner, T. Forbes, N. Lygeros, M. Mizony, H. Nelson, and P. Zimmermann , Ten consecutive primes in arithmetic progression	1323

Reviews and Descriptions of Tables and Books	1329
Heinz-Otto Kreiss and Hedwig Ulmer Busenhart 1 , Ronald A. Devore, Arieh Iserles, and Endre Süli, Editors 2 , Zhaojun Bai, James Demmel, Jack Dongarra, Axel Ruhe, and Henk van der Vorst, Editors 3 , Guillermo Sapiro 4 , Chee Keng Yap 5 , Kwok-Yan Lam, Igor Shparlinski, Huaxiong Wang, and Chaoping Xing, Editors 6	
Table Errata	1335
I. S. Gradshteyn and I. M. Ryzhik 636 , I. S. Gradshteyn and I. M. Ryzhik 637	
Toshihiro Kumada, Hannes Leeb, Yoshiharu Kurita, and Makoto Matsumoto , Corrigenda to “New primitive t -nomials ($t = 3, 5$) over $GF(2)$ whose degree is a Mersenne exponent,” and some new primitive pentanomials	1337

Vol. 71, No. 240

October 2002

Ivo Babuška and Jan Chleboun , Effects of uncertainties in the domain on the solution of Neumann boundary value problems in two spatial dimensions	1339
Christine Bernardi and Frédéric Hecht , Error indicators for the mortar finite element discretization of the Laplace equation	1371
Ricardo H. Nochetto and Lars B. Wahlbin , Positivity preserving finite element approximation	1405
Zhimin Zhang , Derivative superconvergent points in finite element solutions of harmonic functions—A theoretical justification	1421
Ulisse Stefanelli , Analysis of a variable time-step discretization of the three-dimensional Frémond model for shape memory alloys	1431
Gabriel N. Gatica and Norbert Heuer , Conjugate gradient method for dual-dual mixed formulations	1455
Tai-Lin Wang and William B. Gragg , Convergence of the shifted QR algorithm for unitary Hessenberg matrices	1473
Johnson C. M. Fok, Benyu Guo, and Tao Tang , Combined Hermite spectral-finite difference method for the Fokker-Planck equation	1497
M. P. Calvo and C. Palencia , Avoiding the order reduction of Runge-Kutta methods for linear initial boundary value problems	1529
Nikolai Bakaev and Alexander Ostermann , Long-term stability of variable stepsize approximations of semigroups	1545
Avram Sidi , New convergence results on the generalized Richardson extrapolation process $GREP^{(1)}$ for logarithmic sequences	1569
Winfried Kohnen and Michael Kuß , Some numerical computations concerning spinor zeta functions in genus 2 at the central point	1597
I. H. Sloan, F. Y. Kuo, and S. Joe , On the step-by-step construction of quasi-Monte Carlo integration rules that achieve strong tractability error bounds in weighted Sobolev spaces	1609
Fred J. Hickernell and Xiaoqun Wang , The error bounds and tractability of quasi-Monte Carlo algorithms in infinite dimension	1641

Shuhong Gao and Alan G. B. Lauder , Hensel lifting and bivariate polynomial factorisation over finite fields	1663
Joachim von zur Gathen and Jürgen Gerhard , Polynomial factorization over \mathbb{F}_2	1677
Zhenxiang Zhang , A one-parameter quadratic-base version of the Baillie-PSW probable prime test	1699
Stéphane Louboutin , Computation of class numbers of quadratic number fields	1735
Ana-Cecilia de la Maza , Bounds for the smallest norm in an ideal class .	1745
A. Campillo and J. I. Farrán , Symbolic Hamburger-Noether expressions of plane curves and applications to AG codes	1759
A. Paszkiewicz and A. Schinzel , Numerical calculation of the density of prime numbers with a given least primitive root	1781
Reviews and Descriptions of Tables and Books	1799
R. B. Pari and D. Kaminski 7	
Table Errata	1801
M. Abramowitz and I. Stegun 638	
John B. Friedlander, Carl Pomerance, and Igor E. Shparlinski , Corrigendum to “Period of the power generator and small values of Carmichael’s function”	1803

Editorial Information

As of May 31, 2002, 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. 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 USA. 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 $\mathcal{A}\mathcal{M}\mathcal{S}\text{-}\mathcal{L}\mathcal{A}\mathcal{T}\mathcal{E}\mathcal{X}$. To this end, the Society has prepared $\mathcal{A}\mathcal{M}\mathcal{S}\text{-}\mathcal{L}\mathcal{A}\mathcal{T}\mathcal{E}\mathcal{X}$ 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 $\mathcal{A}\mathcal{M}\mathcal{S}\text{-}\mathcal{L}\mathcal{A}\mathcal{T}\mathcal{E}\mathcal{X}$ 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 $\mathcal{T}\mathcal{E}\mathcal{X}$, using $\mathcal{A}\mathcal{M}\mathcal{S}\text{-}\mathcal{L}\mathcal{A}\mathcal{T}\mathcal{E}\mathcal{X}$ 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](ftp://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, 201 Charles Street, Providence, RI 02904-2294 USA. 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, 201 Charles Street, Providence, RI 02904-2294 USA. 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 starting from www.ams.org/jourhtml/authors.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.

T_EX 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*, T_EX 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, T_EX 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, 201 Charles Street, Providence, RI 02904-2294 USA. 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 T_EX 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 T_EX production at the AMS sometimes requires extra fonts and macros that are not yet publicly available, T_EX files cannot be guaranteed to run through the author’s version of T_EX without errors. The AMS regrets that it cannot provide support to eliminate such errors in the author’s T_EX 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, 201 Charles Street, Providence, RI 02904-2294 USA.

Editorial Committee

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

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

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

JOSEPH D. WARD, Department of Mathematics, Texas A&M University, College Station, TX 77843-3368 USA; *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 USA; *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 USA; *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 USA; *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 USA; *E-mail*: elman@cs.umd.edu

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

DANIEL W. LOZIER, National Institute of Standards and Technology, 100 Bureau Drive, Mail Stop 8910, Gaithersburg, MD 20899-8910 USA; *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@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 USA; *E-mail*: rhn@math.umd.edu

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

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

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

IGOR E. SHPARLINSKI, Department of Computing, Macquarie University, Sydney, New South Wales 2109, Australia; *E-mail*: igor@comp.mq.edu.au

FRANK STENGER, School of Computing, University of Utah, Salt Lake City, UT 84112-1102 USA; *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 Mathematics and Statistics, University of Calgary, Calgary AB, Canada T2N 1N4; *E-mail*: williams@math.ucalgary.ca

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

(Continued from back cover)

Ana-Cecilia de la Maza , Bounds for the smallest norm in an ideal class	1745
A. Campillo and J. I. Farrán , Symbolic Hamburger-Noether expressions of plane curves and applications to AG codes	1759
A. Paszkiewicz and A. Schinzel , Numerical calculation of the density of prime numbers with a given least primitive root	1781
Reviews and Descriptions of Tables and Books	1799
R. B. Pari and D. Kaminski	7
Table Errata	1801
M. Abramowitz and I. Stegun	638
John B. Friedlander, Carl Pomerance, and Igor E. Shparlinski , Corrigendum to “Period of the power generator and small values of Carmichael’s function”	1803

No microfiche supplement in this issue

MATHEMATICS OF COMPUTATION
CONTENTS

Vol. 71, No. 240

October 2002

Ivo Babuška and Jan Chleboun, Effects of uncertainties in the domain on the solution of Neumann boundary value problems in two spatial dimensions	1339
Christine Bernardi and Frédéric Hecht, Error indicators for the mortar finite element discretization of the Laplace equation	1371
Ricardo H. Nochetto and Lars B. Wahlbin, Positivity preserving finite element approximation	1405
Zhimin Zhang, Derivative superconvergent points in finite element solutions of harmonic functions—A theoretical justification	1421
Ulisse Stefanelli, Analysis of a variable time-step discretization of the three-dimensional Frémond model for shape memory alloys	1431
Gabriel N. Gatica and Norbert Heuer, Conjugate gradient method for dual-dual mixed formulations	1455
Tai-Lin Wang and William B. Gragg, Convergence of the shifted QR algorithm for unitary Hessenberg matrices	1473
Johnson C. M. Fok, Benyu Guo, and Tao Tang, Combined Hermite spectral-finite difference method for the Fokker-Planck equation	1497
M. P. Calvo and C. Palencia, Avoiding the order reduction of Runge-Kutta methods for linear initial boundary value problems	1529
Nikolai Bakaev and Alexander Ostermann, Long-term stability of variable stepsize approximations of semigroups	1545
Avram Sidi, New convergence results on the generalized Richardson extrapolation process GREP ⁽¹⁾ for logarithmic sequences	1569
Winfried Kohlen and Michael Kuß, Some numerical computations concerning spinor zeta functions in genus 2 at the central point	1597
I. H. Sloan, F. Y. Kuo, and S. Joe, On the step-by-step construction of quasi-Monte Carlo integration rules that achieve strong tractability error bounds in weighted Sobolev spaces	1609
Fred J. Hickernell and Xiaoqun Wang, The error bounds and tractability of quasi-Monte Carlo algorithms in infinite dimension	1641
Shuhong Gao and Alan G. B. Lauder, Hensel lifting and bivariate polynomial factorisation over finite fields	1663
Joachim von zur Gathen and Jürgen Gerhard, Polynomial factorization over \mathbb{F}_2	1677
Zhenxiang Zhang, A one-parameter quadratic-base version of the Baillie-PSW probable prime test	1699
Stéphane Louboutin, Computation of class numbers of quadratic number fields	1735

(Continued on inside back cover)



0025-5718(200210)71:240*;1-W