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 IndexTM-Expanded, ISI Alerting ServicesSM, 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.

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 $\mathcal{A}_{\mathcal{M}}\mathcal{S}$ -IATEX. To this end, the Society has prepared $\mathcal{A}_{\mathcal{M}}\mathcal{S}$ -IATEX author packages for each AMS publication. Author packages include instructions for preparing electronic manuscripts, the $\mathcal{A}_{\mathcal{M}}\mathcal{S}$ -IATEX style file that generates the particular design specifications of that publication series. Articles properly prepared using the $\mathcal{A}_{\mathcal{M}}\mathcal{S}$ -IATEX 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 $\mathcal{A}_{\mathcal{M}}\mathcal{S}$ -IATEX 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}_{MS} -ETEX papers also move more efficiently through the production stream, helping to minimize publishing costs.

AMS-IFTEX is the highly preferred format of TEX, but author packages are also available in AMS-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 IFTEX 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. IFTEX users will find that AMS-IFTEX is the same as IFTEX with additional commands to simplify the typesetting of mathematics, and users of plain TEX should have the foundation for learning AMS-IFTEX.

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, 201 Charles Street, Providence, RI 02904-2294 USA. When requesting an author package, please specify AMS-IFTEX or AMS-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.

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, T_FX 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 TrX 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 TFX 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, 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@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 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

AMERICAN MATHEMATICAL SOCIETY

w.ams.o

AMERICAN MATHEMATICAL SOCIETY

Bookstores | CML | Journals | MathSciNet | MR Lookup | MS

News

Joint Mathematics Meetings in New Orleans

Research Conferences 20021

Summer 2001 Fellowships Opportunity for Graduate Students

What's New in Math Feature Column
Celestial Mechanics on a Graphing
Calculator
by Tony Phillips

Membership

Customer Services

Employment

Meetings &

Conferences

AMS Governance

MathSciNet

Journals Subscriptions, Search, Authors, Support...

Books AMS Bookstore, Books Online, Author Resources...

Mathematical Reviews Database

Math on the Web

Reference Tools

Government Relations

Relations

AMS in Washington,
News & Alerts,
Communicating with
Congress, Federal
Budget Information...

Public Awareness

Information for Journalists, Press Releases, AMS Fact Sheet...

Prizes & Awards

Giving to the AMS

Search the AMS website Site search, Site map...

Calendar 1/15 AMS-AAAS Summer Media Fellows Application Due 2/1 Deadline for Proposals for Summer Research Conferences 2002 Reserve hotel rooms early for the Williams College meeting, October 13 - 14, 2001.

¥ Race to settle Catalan conjecture

¥ The math melodrama

Recent Additions AMS Electronic Coversheet Service

The website of the AMS facilitates access to scientific information. resources, and tools for the mathematical community. Sample topics that you'll find include ...

Membership

www.ams.org/membership

Join the AMS, renew your membership, take advantage of member-only services, and more!

Employment Services

www.ams.org/employment

Check out job listings, visit the employment center, get help with your academic job search, and more!

Meetings & Conferences

www.ams.org/meetings

Register for meetings, find out about dates and places of meetings and conferences, learn how to submit an abstract or paper, and more!

Books

www.ams.org/bookstore

Visit the AMS Bookstore to browse and purchase publications, products, and services.

Journals

www.ams.org/journals

Read about cutting-edge research; view papers online prior to their publication in the printed issue, browse Notices of the AMS and Bulletin of the AMS—both are free online!

MathSciNet

www.ams.org/mathscinet

Mathematical Reviews on the Web—the premier source for searching the world's mathematical literature.

Math Reviews

www.ams.org/mr-database

Submit reviews, learn about MR-derived products, utilize MR resources, and more!

Careers and Education

www.ams.org/careers-edu

Find student help, learn about funding, surveys, and programs in the mathematical sciences!

There's more! Other AMS Website features include:

- AMS User Account Services NEW!
- "Your Subscriptions" Information
- Mathematical News and Information
- · What's New in Math



American Mathematical Society

Bookstore



www.amsbookstore.org

MAMS BOOKSTORE				
FULL SEARCH NE	BOOKSTORE FAQ RECOMMENDED BOOKSTORE FAQ GOI Browse	OKS IN SERIES EXPRESS ORDER FORM		
CONTENTS	FEATURED PUBLICATIONS	NEWS		
Over 3000 Books And More! • AMS Chelsea Publishing Titles • Journals • MathSciNet • Videos • Gift Items • Where to find AMS Titles • Sales Items	Classical and Quantum Computation A. Yu. Kitaev A. H. Shen M. N. Vyalyi Available in Hardcover and Softcover This book presents a concise introduction to an emerging and increasingly important topic, the theory of quantum computing. In less than 300 pages, the authors set forth a solid foundation to the theory, including results that have not appeared elsewhere and improvements on existing works. It would make an excellent textbook for course adoption, complete with problems and solutions.	New titles from the AMS: See New Titles. New Title Email Notification: Sign up to receive email notification about new publications as they are posted to the AMS Bookstore. AMS Publications Update Click here to receive our quarterly mailing announcing new AMS titles.		

Your Key Source for AMS Information and Purchases

Visit the AMS Bookstore for the most up-to-date information on our books, journals, and electronic products and services.

If you need information or want to make a purchase, the AMS Bookstore is your destination: www.amsbookstore.org

Go to the Bookstore for the complete listing of over 3,000 mathematical books, journals, videos, gift items, and more.

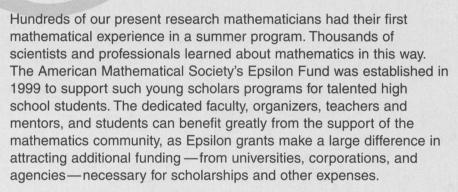
Web Exclusive Sales!



AMERICAN MATHEMATICAL SOCIETY

The Epsilon Fund

A lifelong passion for mathematics most often grows from youthful enthusiasm



The AMS invites members and others in the mathematical community to build the Epsilon Fund for the future.

"The summer math program was the single most important event of my high school years. It gave me the opportunity to broaden my horizons and challenge myself in ways my high school did not."

For more information or to make a donation to this endowment, see www.ams.org/giving-to-ams.



Contact: Raquel Storti, Development Office, American Mathematical Society, 201 Charles Street, Providence, RI 02904-2294, USA; tel. 800-321-4267, ext. 4111 (U.S. and Canada) or 401-455-4111 (worldwide); email: res@ams.org



AMERICAN MATHEMATICAL SOCIETY

AMERICAN MATHEMATICAL SOCIETY

ATHEMATICS

AMERICAN MATHEMATICAL SOCIETY



ATHEMATICS

AMERICAN MATHEMATICAL SOCIETY

ISSN 1088-6842 (e) ISSN 0025-5718 (p)

Recently posted articles | Most recent issue | All issues

About this journal

- Editorial board
- Copying and reprin Back issues from JST

Subscription information

- Subscribe from the AMS B
 Electronic Journals Online
- ion Agreement

Information can

be found on the iournal's Initial

Submission page.

- Journals Home Search Journals

For authors

- Author packages
 Consent to publish and copyright agreements

- Permissions
 Where to send files for accepted papers
 AMS policy on making changes to articles after posting
- sacking information
 Information for authors on submitting citations
- Manuscript tracking system

lournal overview: This journal is devoted to 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 and occasional microfiche supplements are also included.

Journals Home
 Search Journals
 For Authors
 Subscribe
 Tech Support



ATHEMATICS

AMERICAN MATHEMATICAL SOCIETY

ISSN 1088-6842 (c) ISSN 0025-5718 (p)

Recently posted articles | Most recent issue | All issues

mal overview: This journal is devoided to research articles in computational mathematics. Areas covered include numerical sits, with emphasis can be mathematical analysis and development of methods, computational number theory and algebra, amed of lidels. Table restant and reviews or books in areas related to computational mathematics and coessissam aimsrifels supplement.

Submission information: Information can be found on the journal's Initial Submission page

The AMS has released enhanced versions of its electronic journals. These upgrades improve usefulness and relevance for both journal subscribers and journal authors.

A 30-day free trial is available to corporations and institutions. A downloadable Free Trial Form is available at: www.ams.org/ customers/ejournaltrial.pdf.

Contact AMS Membership and Customer Services, P. O. Box 6248, Providence, RI 02940-6248, USA; phone 1-800-321-4267 or 1-401-455-4000 worldwide; fax 1-401-455-4046; email: cust-serv@ams.org. Note: A signed license agreement is required for AMS electronic journal subscriptions. A newly updated and expanded agreement can be found online at http://www.ams.org/customers/jour-license.html.







MATHEMATICAL MOMENTS

The **Mathematical Moments** program is a series of illustrated "snapshots" designed to promote appreciation and understanding of the role mathematics plays in science, nature, technology, and human culture.

Download these and other *Mathematical Moments* pdf files at www.ams.org/mathmoments.



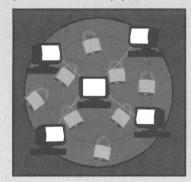
Securing Internet Communication

No one could shop, pay bills, or conduct business securely on the Internet without the mathematics of encryption. Although based on algebraic facts proved centuries ago, today's sophisticated encryption techniques were formulated within the past twenty-five years.

Public key encryption allows a user to publish the encryption key for all to use, while keeping the decryption key secret. One such algorithm, called RSA, is behind the encryption in modern browsers. The National Institute of Standards and Technology recently adopted an Advanced Encryption Standard that will be used for electronic communication in the years to come. This new standard uses permutations, modular arithmetic, polynomials, matrices, and finite fields to transmit information freely but securely.

For More Information:

"Communications Security for the Twenty-first Century," Susan Landau, Notices of the American Mathematical Society, April 2000.



AMERICAN MATHEMATICAL SOCIETY

The Mathematical Moments program promotes appreciation and understanding of the role mathematics plays in science, nature, technology, and human culture.

- · Describing the Oceans
- Designing Aircraft
- Deciphering DNA
- Storing Fingerprints
- Investing in Markets
- Creating Crystals
- Seeing the World through Fractals
- Experimenting with the Heart
- Securing Internet Communication
- Making Movies Come Alive
- Listening to Music
- Routing Traffic through the Internet
- Tracking Products
- Forecasting Weather
- Manufacturing Better Lenses



www.ams.org/mathmoments

American Mathematical Society **lathema** www.ams.org/new-in-math Feature Column Monthly essays on mathematical topics. Recent columns include "Voting and Elections" and "Mathematics and the Genome," by Joe Malkevitch (York College, CUNY). The archive includes essays by Malkevitch, Tony Phillips, and Steven Weintraub. Math in the Media Highlights of math news in the media. Tony Phillips (Stony Brook University) provides analysis and personal commentaries on math-related stories from major metropolitan newspapers and science magazines on a wide range of topics: John Nash, Ben Franklin's Magic Squares, the Abel Prize, the hat problem, education, Fourier transform of the fossil record, differential equations of pathogen virulence, and many more. Math Digest Summaries of articles on mathematics. AMS staff writers and AMS-AAAS Media Fellows post summaries of math-related articles that appear in Science, Nature, Scientific American, American Scientist, Science News, Discover, Nature Science Update, New Scientist, newspapers, and other print and Web sources.

(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	1000
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	1911
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-	1500
Kutta methods for linear initial boundary value problems	1529
Nikolai Bakaev and Alexander Ostermann, Long-term stability of variable stepsize approximations of semigroups	15.45
Avram Sidi, New convergence results on the generalized Richardson	1545
extrapolation process GREP ⁽¹⁾ for logarithmic sequences	1569
Winfried Kohnen and Michael Kuß, Some numerical computations	1008
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	100.
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	1 70 0
fields	1735
(Continued on inside back of	cover

