Editorial Information

As of September 30, 2001, the backlog for this journal was approximately 3 issues. This estimate is the result of dividing the number of manuscripts for this journal in the Providence office that have not yet gone to the printer on the above date by the average number of articles per issue over the previous twelve months, reduced by the number of issues published in six months (the time necessary for editing and composing a typical issue). In an effort to make articles available as quickly as possible, articles are posted to the AMS website individually after proof is returned from authors and before appearing in an issue.

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

Information for Authors

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

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

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

Electronically prepared manuscripts. For the final submission of accepted papers, the AMS encourages use of electronically prepared manuscripts, with a strong preference for AMS-IMTEX. To this end, the Society has prepared AMS-IMTEX 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 AMS-IMTEX 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 AMS-IMTEX 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. AMS-IMTEX papers also move more efficiently through the production stream, helping to minimize publishing costs.

AMS-IATEX 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 IATEX 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. IATEX users will find that AMS-IATEX is the same as IATEX with additional commands to simplify the typesetting of mathematics, and users of plain TEX should have the foundation for learning AMS-IATEX.

Authors may retrieve an author package from the AMS website starting from www.ams.org/tex/ or via FTP to ftp.ams.org (login as anonymous, enter username as password, and type cd pub/author-info). The AMS Author Handbook and the Instruction Manual are available in PDF format following the author packages link from www.ams.org/tex/. The author package can also be obtained free of charge by sending email to pub@ams.org (Internet) or from the Publication Division, American Mathematical Society, P.O. Box 6248, Providence, RI 02940-6248. When requesting an author package, please specify AMS-IFIEX 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, P.O. Box 6248, Providence, RI 02940-6248. When sending a manuscript electronically, please be sure to include a message indicating in which publication the paper has been accepted. No corrections will be accepted electronically. Authors must mark their changes on their proof copies and return them to the Providence office. Complete instructions on how to send files are included in the author package.

Electronic graphics. Comprehensive instructions on preparing graphics are available 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, 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, TeX files are available upon request for authors without Web access by sending email to file-request@ams.org or by contacting the Electronic Prepress Department, American Mathematical Society, P.O. Box 6248, Providence, RI 02940-6248. The request should include the title of the paper, the name(s) of the author(s), the name of the publication in which the paper has or will appear, and the volume and issue numbers if known. The TFX 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_FX production at the AMS sometimes requires extra fonts and macros that are not yet publicly available, TFX files cannot be guaranteed to run through the author's version of TEX without errors. The AMS regrets that it cannot provide support to eliminate such errors in the author's TEX environment.

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

Editorial Committee

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

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

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

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

Board of Associate Editors

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

HUGH C. WILLIAMS, Department of 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; E-mail: xu@math.psu.edu

AMERICAN MATHEMATICAL SOCIETY

Electronic Research Announcements

AMERICAN MATHEMATICAL SOCIETY

MANAGING EDITOR

Svetlana Katok

EDITORIAL BOARD

Stuart Antman David Benson Dmitri Burago Mark Freidlin Ronald Graham Yitzhak Katznelson David Kazhdan Alexander Kechris Alexandre Kirillov Frances Kirwan Krystyna Kuperberg Robert Lazarsfeld Gregory Margulis **Hugh Montgomery** Walter Neumann Klaus Schmidt Richard Schoen Masamichi Takesaki Michael Taylor **Guido Weiss** Zhihong (Jeff) Xia Don Zagier Efim Zelmanov

Volume 7, 2001 (Most Recent Articles)

Vadim Yu. Kaloshin and **Brian R. Hunt,** A stretched exponential bound on the rate of growth of the number of periodic points for prevalent diffeomorphisms I

Vadim Yu. Kaloshin and **Brian R. Hunt**, A stretched exponential bound on the rate of growth of the number of periodic points for prevalent diffeomorphisms II

V. Balaji, I. Biswas, and D. S. Nagaraj, Principal bundles with parabolic structure

Robert Lauter and **Victor Nistor**, *On spectra of geometric operators on open manifolds and differentiable groupoids*

Stephen Doty and **Anthony Giaquinto,** *Generators and relations for Schur algebras*

A. Yu. Ol'shanskii and M. V. Sapir, Non-amenable finitely presented torsion-by-cyclic groups

Pablo Pedregal, Fully explicit quasiconvexification of the meansquare deviation of the gradient of the state in optimal design

The American Mathematical Society's electronic-only journal, *Electronic Research Announcements of the AMS* (ERA-AMS), is available on the World Wide Web at www.ams.org/era.

ERA-AMS publishes high-quality research announcements of significant advances in all branches of mathematics. Authors may submit manuscripts to any editor. All papers are reviewed, and the entire Editorial Board must approve the acceptance of any paper. Papers are posted as soon as they are accepted and processed by the AMS.

ERA-AMS offers you ...

- · decreased turn-around time from submission to publication
- · fast access to your specific area of interest
- · up-to-the-minute research information

For more information about this journal for authors, and subscription information, go to www.ams.org/journals/era.

For more information, contact: cust-serv@ams.org 1-800-321-4267, 1-401-455-4000, fax 1-401-455-4046





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.



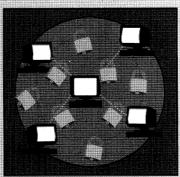
Securing Internet Communication

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.



@AMS

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

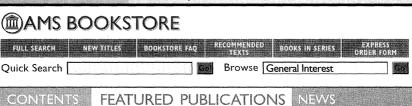
- Describing the Oceans
- Designing Aircraft
- Deciphering DNA
- Storing Fingerprints
- Investing in Markets
- · Creating Crystals
- Seeing the World through Fractals
- Experimenting with the Heart
- Securing Internet Communication
- Making Movies
 Come Alive
- Listening to Music
- Routing Traffic through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



www.ams.org/mathmoments



Visit the AMS Bookstore, our online catalog of books, videos, journals, software, and gift items at www.ams.org/bookstore.



Over 3000 Books And More!

- * AMS Chelsea Publishing Titles
- Journals
- MathSciNet
- Videos
- Gift Items
- Where to find AMS
- Sales Items



Triangle of Thoughts

Alain Connes, André Lichnerowicz, and Marcel Paul Schützenberger

The "conversations" in this book by three outstanding scientists are sprinkled with stories and quotes that enliven the discourse. The book will make you think again about things that you once thought were familiar.

Chaotic Elections! A Mathematician Looks At Voting

Donald G. Saari

Required reading for anyone who wants to understand not only what happened in the presidential election of 2000, but also how we can avoid similar problems from appearing anytime any group is making a choice using a voting procedure.

CHAOTIC ELECTIONS!

- New Title Email Notification: Sign up to receive email notification about new publications as they are posted to the AMS Bookstore.
- New titles from the AMS: See New Titles published June through August 2001.
- . New AMS Briefcases! Sturdy and functional, AMS briefcases are now available. Visit AMS Gift Items. AMS Briefcases, t-shirts, and other gift items are available.
- · AMS Publications Update Click here to receive our quarterly mailing announcing new AMS
- News Archive

www.ams.org/bookstore

AMERICAN MATHEMATICAL SOCIETY

www.ams.org the AMS website

AMERICAN MATHEMATICAL SOCIETY

- ABOUT THE AMS
- . JOIN THE AMS
- CONTACT US
- CONTACT US
- YOUR SUBSCRIPTIONS

Membership

Join, Renew, Benefits, Ear Members Only...

Customer Services

Contact Us, Customer FAO, License Agreements...

Employment Services

Job Ads, Employment Center, AMS Coversheet Service...

Meetings & Conferences

Sectionals, National, International, AMS Conferences, Other Meetings and Activities...

AMS Governance

Secretary, Leadership, Elections, Committees...

Careers & Education

Survey Data, Funding, Programs at all levels...

MathSciNet

About, Subscriptions, Consortia, Free Trial, Demo, Support, Guidebook...

<u>Journals</u>

Subscriptions, Search, Authors, Support...

Books

AMS Bookstore, Books Online, Author Resources...

Mathematical Reviews Database

Editorial Statement, Publication Formats, MSC, Featured Reviews, Review Submission...

Math on the Web

Guides, Servers, People...

Reference Tools

Tex Resources, Books Online, Preprints, Journal Price Survey, Tools, Staff, Other Societies...

Government Relations

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

Public Awareness

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

Prizes & Awards

Recipients, Press Releases...

Giving to the AMS

Giying, Epsilon Fund...

Search the AMS website

Site search, Site map...

News

Bookstores | CML | Journals | MathSciNet | MR Lookup | MSC

Summer 2001 Fellowships Opportunity for Graduate Students

Joint Mathematics Meetings in New Orleans

Call for Proposals for Summer

Research Conferences 2002!

more...

What's New in Math

Feature Column

Celestial Mechanics on a Graphing Calculator by Tony Phillips

Math in the Media

¥ Race to settle Catalan conjecture

Y President mentions math

Y The math melodrama

more.

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.

Recent Additions

AMS Electronic Coversheet Service



AMERICAN MATHEMATICAL SOCIETY

30-day free

athSciNet Mathematical Reviews on the Web

Facts and Figures: 14,792 items added in 2001; 1,799 journals covered; links to 150,623 original articles; 10,843 active reviewers; 358,128 authors indexed

Quick Search		
Providence	•	
Select a field	(e) [
G ₀		
Searches Full Search Author database Journals database MSC by Keyword	Browse Current books Current journals Math. Subject Classification	n

Reviewers, Authors, Publishers

MR Lookup

Verify references and add links

MathSciNet Getitem

Create direct links

Electronic submission

Submit reviews

Guide for Reviewers

Reviewing schedules, style elements, etc.

What's New

- New version of MathSciNet released
- · New Clipboard Feature
- More publishers link to MathSciNet
- Changes to Author and Classification
- Clearer navigation of results
- More...

About MathSciNet

- Serials
- Original article links
- Featured Reviews
- Subscriptions
- Consortia
- 30-Day Free Trial
- Guidebook
- Demo
- Support

MathSciNet has an especially powerful system of internal links between reviews and provides direct links to the papers themselves if they are available on line. The reviews are classified by subject and are searchable in multiple ways. Thus, it provides an unparalleled method of browsing the literature for serious content (along with accurate bibliographic data).

—Journal of Electronic Publishing, University of Michigan Press

Go to

ww.ams.org/mathscinet

for updates and to view a demo.

Consortia pricing is available: Please contact Lori Sprague, Publications Administrator, by telephone at 1-401-455-4064 or by email at las@ams.org.

* A 30-day free trial is available to corporations and academic institutions. A downloadable Free Trial Form is available at: www.ams.org/customers/msntrial.pdf or www.ams.org/customers/ejournaltrial.pdf. For more information, 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.



(Continued from back cover)

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	0 10
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 quad-	
rature^n	453

No microfiche supplement in this issue

MATHEMATICS OF COMPUTATION CONTENTS

Vol. 71, No. 237 January 2	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-Thomée criterion for H^1 -stability of the L^2 -projection onto	141
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
matrix	217
Nataša Krejić and Zorana Lužanin, Newton-like method with	025
modification of the right-hand-side vector	237
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
(Continued on inside back co	
· ·	



0025-5718(200201)71:237;1-N