VOLUME 76 NUMBER 257 JANUARY 2007

MATHEMATICS OF COMPUTATION

AMERICAN MATHEMATICAL SOCIETY

EDITED BY

Randolph E. Bank
Peter B. Borwein
David W. Boyd
Susanne C. Brenner
Richard P. Brent
Carsten Carstensen
Bernardo Cockburn
Arjeh M. Cohen
Ronald F. A. Cools
Howard Elman
Ivan P. Gavrilyuk
Vivette Girault
Ernst Hairer
Daniel W. Lozier
Jean-François Mestre
Marian Neamtu
Harald Niederreiter
Ricardo H. Nochetto
Stanley Osher
Joseph E. Pasciak
Lothar Reichel
Jie Shen
Igor E. Shparlinski
Chi-Wang Shu, *Managing Editor*
Michael E. Stillman
Denis Talay
Tao Tang
Paul Y. Tseng
Hugh C. Williams
Jinchao Xu

PROVIDENCE, RHODE ISLAND USA

ISSN 0025-5718

Available electronically at
www.ams.org/mcom/

Mathematics of Computation

This journal is devoted to research articles of the highest quality in computational mathematics. Areas covered include numerical analysis, computational discrete mathematics, including number theory, algebra and combinatorics, and related fields such as stochastic numerical methods. Articles must be of significant computational interest and contain original and substantial mathematical analysis or development of computational methodology. 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/journals/`. Subscription prices for Volume 76 (2007) are as follows: for paper delivery, $486 list, $389 institutional member, $437 corporate member, $316 member of CBMS organizations; $292 individual member; for electronic delivery, $437 list, $350 institutional member, $393 corporate member, $284 member of CBMS organizations, $262 individual member. Upon request, subscribers to paper delivery of this journal are also entitled to receive electronic delivery. If ordering the paper version, add $18 for surface delivery outside the United States and India; $19 to India. Expedited delivery to destinations in North America is $27; 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.

© 2007 by the American Mathematical Society. All rights reserved.

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

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

10 9 8 7 6 5 4 3 2 1 12 11 10 09 08 07

MATHEMATICS OF COMPUTATION

CONTENTS

Vol. 76, No. 257 **January 2007**

Wang Ming and Jinchao Xu, Nonconforming tetrahedral finite elements for fourth order elliptic equations 1

Alan Demlow, Local a posteriori estimates for pointwise gradient errors in finite element methods for elliptic problems 19

Kwang Y. Kim, A posteriori error analysis for locally conservative mixed methods 43

Fatih Celiker and Bernardo Cockburn, Superconvergence of the numerical traces of discontinuous Galerkin and Hybridized methods for convection-diffusion problems in one space dimension 67

JaEun Ku, A least-squares method for second order noncoercive elliptic partial differential equations 97

Yinnian He and Weiwei Sun, Stabilized finite element method based on the Crank–Nicolson extrapolation scheme for the time-dependent Navier–Stokes equations 115

Huo-Yuan Duan, Shao-Qin Gao, Roger C. E. Tan, and Shangyou Zhang, A generalized BPX multigrid framework covering nonnested V-cycle methods 137

Pingbing Ming and Pingwen Zhang, Analysis of the heterogeneous multiscale method for parabolic homogenization problems 153

Long Chen, Pengtao Sun, and Jinchao Xu, Optimal anisotropic meshes for minimizing interpolation errors in L^p-norm 179

C. González and M. Thalhammer, A second-order Magnus-type integrator for quasi-linear parabolic problems 205

Bishnu P. Lamichhane and Barbara I. Wohlmuth, Biorthogonal bases with local support and approximation properties 233

Volker Elling, A Lax–Wendroff type theorem for unstructured quasi-uniform grids 251

Mihály Kovács, On the convergence of rational approximations of semigroups on intermediate spaces 273

Zhong-Zhi Bai, Gene H. Golub, and Chi-Kwong Li, Convergence properties of preconditioned Hermitian and skew-Hermitian splitting methods for non-Hermitian positive semidefinite matrices 287

R. Caira and F. Dell'Accio, Shepard–Bernoulli operators 299

Ramūnas Garunkštis and Jörn Steuding, On the distribution of zeros of the Hurwitz zeta-function 323

Nathanial P. Brown, Quasi-diagonality and the finite section method ... 339

Helen Avelin, Deformation of $\Gamma_0(5)$-cusp forms 361

Daniel J. Bernstein, Hendrik W. Lenstra, Jr., and Jonathan Pila, Detecting perfect powers by factoring into coprimes 385

Daniel J. Bernstein, Proving primality in essentially quartic random time 389

Bernd C. Kellner, On irregular prime power divisors of the Bernoulli numbers 405

Daniel J. Bernstein and Jonathan P. Sorenson, Modular exponentiation via the explicit Chinese remainder theorem 443

Stéphane R. Louboutin, Efficient computation of root numbers and class numbers of parametrized families of real abelian number fields 455
P. Gaudry, E. Thomé, N. Thériault, and C. Diem, A double large prime variation for small genus hyperelliptic index calculus 475
F. Morain, Implementing the asymptotically fast version of the elliptic curve primality proving algorithm 493
Andrew D. Loveless, A compositeness test that never fails for Carmichael numbers 507

Editorial Information

Information on the backlog for this journal can be found on the AMS website starting from `http://www.ams.org/mcom`.

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. The AMS uses Centralized Manuscript Processing for initial submission. Authors should submit a PDF file using the Initial Manuscript Submission form found at `www.ams.org/cgi-bin/peertrack/submission.pl`, or send one copy of the manuscript to the following address: Centralized Manuscript Processing, MATHEMATICS OF COMPUTATION, 201 Charles Street, Providence, RI 02904-2294 USA. If a paper copy is being forwarded to the AMS, indicate that it is for *Mathematics of Computation* and include the name of the corresponding author and contact information, such as an email address or mailing address. The author may suggest an appropriate editor for his or her paper.

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, reasonably self-contained, and not exceed 300 words. 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/`.

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

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

system. LaTeX users will find that $\mathcal{AMS}$-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 $\mathcal{AMS}$-LaTeX.

Authors may retrieve an author package from the AMS website starting from `www.ams.org/tex/` or via FTP to `ftp.ams.org` (login as `anonymous`, enter username as password, and type `cd pub/author-info`). The *AMS Author Handbook* and the *Instruction Manual* are available in PDF format following the author packages link from `www.ams.org/tex/`. The author package can also be obtained free of charge by sending email to `tech-support@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 $\mathcal{AMS}$-LaTeX or $\mathcal{AMS}$-TeX and the publication in which your paper will appear. Please be sure to include your complete email address.

After acceptance. 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 to the Managing Editor, who will forward a copy to the Providence office. Accepted electronically prepared manuscripts can be submitted via the web at `www.ams.org/submit-book-journal/`, sent via email to `pub-submit@ams.org` (Internet), or sent on diskette to the Electronic Prepress Department, American Mathematical Society, 201 Charles Street, Providence, RI 02904-2294 USA. When sending a manuscript electronically via email or diskette, 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. 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 upon request. TEX files are available upon request for authors 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 TEX file will be sent to the author making the request after the article goes to the printer. If the requestor can receive Internet email, please include the email address to which the file should be sent. Otherwise please indicate a diskette format and postal address to which a disk should be mailed. **Note:** Because TEX production at the AMS sometimes requires extra fonts and macros that are not yet publicly available, TEX files cannot be guaranteed to run through the author's version of TEX without errors. The AMS regrets that it cannot provide support to eliminate such errors in the author's TEX environment.

Inquiries. Any inquiries concerning a paper that has been accepted for publication that cannot be answered via the manuscript tracking system mentioned above should be sent to `mcom-query@ams.org` or directly to the Electronic Prepress Department, American Mathematical Society, 201 Charles Street, Providence, RI 02904-2294 USA.

Editorial Committee

SUSANNE C. BRENNER, Center for Computation and Technology, Johnston Hall, Louisiana State University, Baton Rouge, LA 70803 USA; *E-mail*: `brenner@math.lsu.edu`

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`

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`

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

PETER B. BORWEIN, Department of Mathematics and Statistics, Simon Fraser University, Burnaby, BC, Canada V6T 1Z2; *E-mail*: `pborwein@cecm.sfu.ca`

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

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

CARSTEN CARSTENSEN, Humboldt-Universität zu Berlin, Department of Mathematics, Unter den Linden 6, D-10099 Berlin, Germany; *E-mail*: `mathcomp@math.hu-berlin.de`

BERNARDO COCKBURN, School of Mathematics, University of Minnesota, 206 Church Street SE, Minneapolis, MN 55455; *E-mail*: cockburn@math.umn.edu

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

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

IVAN P. GAVRILYUK, Berufsakademie Thüringen, Am Wartenberg 2, D-99817 Eisenach, Germany; *E-mail*: ipg@ba-eisenach.de

VIVETTE GIRAULT, Laboratoire Jacques-Louis Lions, Boite Courrier 187, Université de Pierre et Marie Curie, 4, place Jussieu, 75252 Paris Cedex 05, France; *E-mail*: girault@ann.jussieu.fr

ERNST HAIRER, Université de Genève, Section de Mathématiques, 2-4 Rue du Livre, CP 248, CH 1211 24 Genève, Switzerland; *E-mail*: ernst.hairer@math.unige.ch

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

JEAN-FRANÇOIS MESTRE, UFR de Mathématiques, 2 place Jussieu, Université de Paris VII, Paris 75005, France.

MARIAN NEAMTU, 1326 Stevenson Center, Department of Mathematics, Vanderbilt University, Nashville, TN 37240; *E-mail*: neamtu@math.vanderbilt.edu

RICARDO H. 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

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

JIE SHEN, Department of Mathematics, Purdue University, West Lafayette, IN 47907; *E-mail*: shen@math.purdue.edu

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

MICHAEL E. STILLMAN, Department of Mathematics, Cornell University, Mallott Hall, Ithaca, NY 14853-4201 USA; *E-mail*: mike@math.cornell.edu

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

TAO TANG, Department of Mathematics, Hong Kong Baptist University, Kowloon Tong, Hong Kong *E-mail*: ttang@math.hkbu.edu.hk

PAUL Y. TSENG, Department of Mathematics, University of Washington, Box 354350, Seattle, WA 98195-4350 USA; *E-mail*: tseng@math.washington.edu

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)

Daniel J. Bernstein, Proving primality in essentially quartic random time 389
Bernd C. Kellner, On irregular prime power divisors of the Bernoulli numbers 405
Daniel J. Bernstein and Jonathan P. Sorenson, Modular exponentiation via the explicit Chinese remainder theorem 443
Stéphane R. Louboutin, Efficient computation of root numbers and class numbers of parametrized families of real abelian number fields 455
P. Gaudry, E. Thomé, N. Thériault, and C. Diem, A double large prime variation for small genus hyperelliptic index calculus 475
F. Morain, Implementing the asymptotically fast version of the elliptic curve primality proving algorithm 493
Andrew D. Loveless, A compositeness test that never fails for Carmichael numbers 507

MATHEMATICS OF COMPUTATION

CONTENTS

Vol. 76, No. 257 **January 2007**

Wang Ming and Jinchao Xu, Nonconforming tetrahedral finite elements for fourth order elliptic equations 1
Alan Demlow, Local a posteriori estimates for pointwise gradient errors in finite element methods for elliptic problems 19
Kwang Y. Kim, A posteriori error analysis for locally conservative mixed methods 43
Fatih Celiker and Bernardo Cockburn, Superconvergence of the numerical traces of discontinuous Galerkin and Hybridized methods for convection-diffusion problems in one space dimension 67
JaEun Ku, A least-squares method for second order noncoercive elliptic partial differential equations 97
Yinnian He and Weiwei Sun, Stabilized finite element method based on the Crank–Nicolson extrapolation scheme for the time-dependent Navier–Stokes equations 115
Huo-Yuan Duan, Shao-Qin Gao, Roger C. E. Tan, and Shangyou Zhang, A generalized BPX multigrid framework covering nonnested V-cycle methods 137
Pingbing Ming and Pingwen Zhang, Analysis of the heterogeneous multiscale method for parabolic homogenization problems 153
Long Chen, Pengtao Sun, and Jinchao Xu, Optimal anisotropic meshes for minimizing interpolation errors in L^p-norm 179
C. González and M. Thalhammer, A second-order Magnus-type integrator for quasi-linear parabolic problems 205
Bishnu P. Lamichhane and Barbara I. Wohlmuth, Biorthogonal bases with local support and approximation properties 233
Volker Elling, A Lax–Wendroff type theorem for unstructured quasi-uniform grids 251
Mihály Kovács, On the convergence of rational approximations of semigroups on intermediate spaces 273
Zhong-Zhi Bai, Gene H. Golub, and Chi-Kwong Li, Convergence properties of preconditioned Hermitian and skew-Hermitian splitting methods for non-Hermitian positive semidefinite matrices 287
R. Caira and F. Dell'Accio, Shepard–Bernoulli operators 299
Ramūnas Garunkštis and Jörn Steuding, On the distribution of zeros of the Hurwitz zeta-function 323
Nathanial P. Brown, Quasi-diagonality and the finite section method ... 339
Helen Avelin, Deformation of $\Gamma_0(5)$-cusp forms 361
Daniel J. Bernstein, Hendrik W. Lenstra, Jr., and Jonathan Pila, Detecting perfect powers by factoring into coprimes 385

(*Continued on inside back cover*)

0025-5718(200701)76:257;1-Y

Mathematics of Computation VOLUME 76 NUMBER 257 PAGES 1–508 JANUARY 2007