Editorial Information

As of June 3, 1993, the backlog for this journal was approximately 2 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).

A Copyright Transfer Agreement is required before a paper will be published in this journal. By submitting a paper to this journal, authors certify that the manuscript has not been submitted to nor is it under consideration for publication by another journal, conference proceedings, or similar publication.

Information for Authors and Editors

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, there should be the 1991 *Mathematics Subject Classification* representing the primary and secondary subjects of the article. This may be followed by a list of *key words and phrases* describing the subject matter of the article and taken from it. A list of the numbers may be found in the annual index of *Mathematical Reviews*, published with the December issue starting in 1990, as well as from the electronic service e-MATH [**telnet e-MATH.ams.com** (or **telnet 130.44.1.100**). Login and password are **e-math**]. For journal abbreviations used in bibliographies, see the list of serials in the latest *Mathematical Reviews* annual index. 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. The AMS encourages submission of electronically prepared manuscripts in $\mathcal{A}\mathcal{M}\mathcal{S}$-TEX or $\mathcal{A}\mathcal{M}\mathcal{S}$-LATEX because properly prepared electronic manuscripts save the author proofreading time and move more quickly through the production process. To this end, the Society has prepared "preprint" style files, specifically the amsppt style of $\mathcal{A}\mathcal{M}\mathcal{S}$-TEX and the amsart style of $\mathcal{A}\mathcal{M}\mathcal{S}$-LATEX, which will simplify the work of authors and of the production staff. Those authors who make use of these style files from the beginning of the writing process will further reduce their own effort. Electronically submitted manuscripts prepared in plain TEX or LATEX do not mesh properly with the AMS production systems and cannot, therefore, realize the same kind of expedited processing. Users of plain TEX should have little difficulty learning $\mathcal{A}\mathcal{M}\mathcal{S}$-TEX, and LATEX users will find that $\mathcal{A}\mathcal{M}\mathcal{S}$-LATEX is the same as LATEX with additional commands to simplify the typesetting of mathematics.

Guidelines for Preparing Electronic Manuscripts provides additional assistance and is available for use with either $\mathcal{A}\mathcal{M}\mathcal{S}$-TEX or $\mathcal{A}\mathcal{M}\mathcal{S}$-LATEX. Authors with FTP access may obtain *Guidelines* from the Society's Internet node e-MATH@math.ams.org (130.44.1.100). For those without FTP access *Guidelines* can be obtained free of charge from the e-mail address guide-elec@math.ams.org (Internet) or from the Publications Department, American

Mathematical Society, P.O. Box 6248, Providence, RI 02940-6248. When requesting *Guidelines*, please specify which version you want.

At the time of submission, authors should indicate if the paper has been prepared using $\mathcal{A}\mathcal{M}\mathcal{S}$-TEX or $\mathcal{A}\mathcal{M}\mathcal{S}$-LATEX. The *Manual for Authors of Mathematical Papers* should be consulted for symbols and style conventions. The *Manual* may be obtained free of charge from the e-mail address cust-serv@math.ams.org or from the Customer Services Department, American Mathematical Society, P.O. Box 6248, Providence, RI 02940-6248. The Providence office should be supplied with a manuscript that corresponds to the electronic file being submitted.

Electronic manuscripts should be sent to the Providence office immediately after the paper has been accepted for publication. They can be sent via e-mail to pub-submit@math.ams.org (Internet) or on diskettes to the Publications Department address listed above. When submitting electronic manuscripts 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. Authors and editors are encouraged to make the necessary submissions of electronically prepared manuscripts and proof copies in a timely fashion.

An author should submit the original and two copies of the manuscript and retain one copy. The author may suggest an appropriate editor for his paper. All contributions intended for publication and all books for review should be addressed to Walter Gautschi, Chairman, Editorial Committee, Mathematics of Computation, Department of Computer Sciences, Purdue University, West Lafayette, Indiana 47907. The date received, which is published with the final version of an accepted paper, is the date received in the office of the Chairman of the Editorial Committee, and it is the responsibility of the author to submit manuscripts directly to this office.

Any inquiries concerning a paper that has been accepted for publication should be sent directly to the Editorial Department, American Mathematical Society, P. O. Box 6248, Providence, RI 02940-6248.

SUSANNE C. BRENNER, Department of Mathematics and Computer Science, Clarkson University, Potsdam, NY 13699-5815; *E-mail*: brenner@sun.mcs.clarkson.edu
E. W. CHENEY, Department of Mathematics, University of Texas at Austin, Austin, TX 78712-1082; *E-mail*: cheney@cs.utexas.edu
JAMES W. DEMMEL, Department of Mathematics, University of California, Berkeley, CA 94720; *E-mail*: demmel@robalo.berkeley.edu
EUGENE ISAACSON, Courant Institute of Mathematical Sciences, New York University, 251 Mercer Street, New York, NY 10012; *E-mail*: isaacson@acf7.nyu.edu
JAMES N. LYNESS, Argonne National Laboratory, 9700 South Cass Avenue, Argonne, IL 60439; *E-mail*: lyness@mcs.anl.gov
HARALD NIEDERREITER, Institute for Information Processing, Austrian Academy of Sciences, Sonnenfelsgasse 19, A-1010 Vienna, Austria; *E-mail*: nied@qiinfo.oeaw.ac.at
JORGE J. NOCEDAL, Department of Electrical Engineering and Computer Science, Northwestern University, Evanston, IL 60208-3118; *E-mail*: nocedal@eecs.nwu.edu
SYVERT P. NØRSETT, Division of Numerical Mathematics, The University of Trondheim and The Norwegian Institute of Technology, Alfred Getz vei 1, N-7034 Trondheim-NTH, Norway; *E-mail*: norsett@imf.unit.no
JOHN E. OSBORN, Department of Mathematics, University of Maryland, College Park, MD 20742; *E-mail*: jeo@julia.umd.edu
STANLEY OSHER, Department of Mathematics, University of California, Los Angeles, CA 90024; *E-mail*: sjo@math.ucla.edu
CARL POMERANCE, Department of Mathematics, The University of Georgia, Athens, GA 30602; *E-mail*: carl@joe.math.uga.edu
RENÉ SCHOOF, Dipartimento di Matematica, Università degli Studi di Trento, I-38050 Povo (Trento), Italy; *E-mail*: schoof@itnvax.cineca.it (schoof@math.ruu.nl)
L. RIDGWAY SCOTT, Department of Mathematics, University of Houston, Houston, TX 77204-3476; *E-mail*: scott@casc.math.uh.edu
DANIEL SHANKS, Department of Mathematics, University of Maryland, College Park, MD 20742; *E-mail*: dns@gaby.umd.edu
CHI-WANG SHU, Applied Mathematics Division, Brown University, Providence, RI 02912-0001; *E-mail*: shu@cfm.brown.edu
FRANK STENGER, Department of Computer Science, University of Utah, Salt Lake City, UT 84112; *E-mail*: stenger@sinc.utah.edu
HANS J. STETTER, Institut für Numerische Mathematik, Technische Universität Wien, Wiedner Hauptstrasse 6-10, A-1040, Wien, Austria; *E-mail*: stetter@uranus.tuwien.ac.at
G. W. STEWART, Department of Computer Science, University of Maryland, College Park, MD 20742; *E-mail*: stewart@thales.cs.umd.edu
NICO M. TEMME, Stichting Mathematisch Centrum, Centrum voor Wiskunde en Informatica, Kruislaan 413, 1098 SJ Amsterdam, The Netherlands; *E-mail*: nicot@cwi.nl
VIDAR THOMÉE, Mathematics Department, Chalmers University of Technology, S-412 96 Göteborg, Sweden; *E-mail*: thomee@math.chalmers.se
HUGH C. WILLIAMS, Department of Computer Science, University of Manitoba, Winnipeg, Manitoba, Canada R3T 2N2; *E-mail*: Hugh_Williams@csmail.cs.umanitoba.ca
JOHN W. WRENCH, JR., 102 Mt. Olivet Boulevard, Frederick, MD 21701

(*Continued from back cover*)

D. R. Heath-Brown, W. M. Lioen, and H. J. J. te Riele, On solving the Diophantine equation $x^3 + y^3 + z^3 = k$ on a vector computer 235
D. A. Hejhal and S. Arno, On Fourier coefficients of Maass waveforms for PSL(2, **Z**) 245
Marvin I. Knopp, On the cuspidal spectrum of the arithmetic Hecke groups 269
Donald E. Knuth, Johann Faulhaber and sums of powers 277
Andrew J. Lazarus, Cyclotomy and delta units 295
D. H. Lehmer, The mathematical work of Morgan Ward 307
D. H. Lehmer and Emma Lehmer, The Lehmer project 313
A. K. Lenstra, H. W. Lenstra, Jr., M. S. Manasse, and J. M. Pollard, The factorization of the ninth Fermat number 319
H. W. Lenstra, Jr. and J. O. Shallit, Continued fractions and linear recurrences 351
R. A. Mollin, Ambiguous classes in quadratic fields 355
Peter L. Montgomery, New solutions of $a^{p-1} \equiv 1 \pmod{p^2}$ 361
Joseph B. Muskat, Generalized Fibonacci and Lucas sequences and rootfinding methods 365
Andrew M. Odlyzko, Iterated absolute values of differences of consecutive primes 373
R. G. E. Pinch, The Carmichael numbers up to 10^{15} 381
Raphael M. Robinson, Numbers having m small mth roots mod p 393
Robert Rumely, Numerical computations concerning the ERH 415
A. Schinzel, An extension of the theorem on primitive divisors in algebraic number fields 441
Robert D. Silverman and Samuel S. Wagstaff, Jr., A practical analysis of the elliptic curve factoring algorithm 445
H. C. Williams, How was F_6 factored? 463
Kenneth S. Williams and Kenneth Hardy, A refinement of H. C. Williams' qth root algorithm 475
D. Zagier, Algebraic numbers close to both 0 and 1 485
Supplement to "A conjecture in addition chains related to Scholz's conjecture" by **Walter Aiello and M. V. Subbarao** S1
Supplement to "Explicit primality criteria for $h \cdot 2^k \pm 1$" by **Wieb Bosma** S7
Supplement to "On Fourier coefficients of Maass waveforms for PSL(2, **Z**)" by **D. A. Hejhal and S. Arno** S11
Supplement to "Numerical computations concerning the ERH" by **Robert Rumely** S17

No microfiche supplement in this issue

MATHEMATICS OF COMPUTATION
CONTENTS

Vol. 61, No. 203 **July 1993**

Leonard M. Adleman and Jonathan DeMarrais, A subexponential algorithm for discrete logarithms over all finite fields 1

Walter Aiello and M. V. Subbarao, A conjecture in addition chains related to Scholz's conjecture 17

Tom M. Apostol, An extension of the Lehmers' picturesque exponential sums 25

A. O. L. Atkin and F. Morain, Elliptic curves and primality proving..... 29

Eric Bach and Lorenz Huelsbergen, Statistical evidence for small generating sets 69

Richard Blecksmith, John Brillhart, and Irving Gerst, A fundamental modular identity and some applications 83

Wieb Bosma, Explicit primality criteria for $h \cdot 2^k \pm 1$ 97

Andrew Bremner and Duncan A. Buell, Three points of great height on elliptic curves 111

Andrew Bremner, Richard K. Guy, and Richard J. Nowakowski, Which integers are representable as the product of the sum of three integers with the sum of their reciprocals? 117

Richard P. Brent, On computing factors of cyclotomic polynomials 131

J. Buhler, R. Crandall, R. Ernvall, and T. Metsänkylä, Irregular primes and cyclotomic invariants to four million 151

Harvey Cohn, How branching properties determine modular equations .. 155

T. W. Cusick, Zaremba's conjecture and sums of the divisor function ... 171

Ivan Damgård, Peter Landrock, and Carl Pomerance, Average case error estimates for the strong probable prime test 177

J.-M. Deshouillers and F. Dress, Numerical results for sums of five and seven biquadrates and consequences for sums of 19 biquadrates ... 195

Jean-Marc Deshouillers, Andrew Granville, Władysław Narkiewicz, and Carl Pomerance, An upper bound in Goldbach's problem 209

P. Erdős, C. B. Lacampagne, and J. L. Selfridge, Estimates of the least prime factor of a binomial coefficient 215

Tom Hansen, Gary L. Mullen, and Harald Niederreiter, Good parameters for a class of node sets in quasi-Monte Carlo integration 225

(Continued on inside back cover)

0025-5718(199307)61:203;1-K