VOLUME 61 NUMBER 203 JULY 1993

MATHEMATICS OF COMPUTATION

AMERICAN MATHEMATICAL SOCIETY

PROVIDENCE, RHODE ISLAND USA

ISSN 0025-5718

Mathematics of Computation

This journal publishes research articles in computational mathematics. Areas covered include numerical analysis, the application of computational methods, algorithms for advanced computer architectures, computational number theory and algebra, and related fields. Table errata and reviews of books in areas related to computational mathematics are also included.

Subscription information. *Mathematics of Computation* is published quarterly. Subscription prices for Volumes 60 and 61 (1993) are $249 list; $199 institutional member; $162 member of CBMS organizations; $149 individual AMS member. A late charge of 10% of the subscription price will be imposed upon orders received from nonmember institutions and organizations after January 1 of the subscription year. Subscribers outside the United States and India must pay a postage surcharge of $9; subscribers in India must pay a postage surcharge of $18. Expedited delivery to destinations in North America $13; elsewhere $40.

Back number information. For back issues see the *AMS Catalog of Publications.*

Subscriptions and orders should be addressed to the American Mathematical Society, P. O. Box 1571, Annex Station, Providence, RI 02901-1571. *All orders must be accompanied by payment.* Other correspondence should be addressed to P. O. Box 6248, Providence, RI 02940-6248.

Unpublished Mathematical Tables. The editorial office of the journal maintains a repository of Unpublished Mathematical Tables (UMT). When a table is deposited in the UMT repository a brief summary of its contents is published in the section *Reviews and Descriptions of Tables and Books.* Upon request, the chairman of the editorial committee will supply copies of any table for a nominal cost per page. All tables and correspondence concerning the UMT should be sent to Walter Gautschi, Chairman, Editorial Committee, Mathematics of Computation, Department of Computer Sciences, Purdue University, West Lafayette, IN 47907.

Mathematics of Computation is published quarterly by the American Mathematical Society at 201 Charles Street, Providence, RI 02904-2213. Second-class postage is paid at Providence, Rhode Island. Postmaster: Send address changes to Mathematics of Computation, American Mathematical Society, P. O. Box 6248, Providence, RI 02940-6248.

Printed in the United States of America.
The paper used in this journal is acid-free and falls within the guidelines established to ensure permanence and durability. ∞
This publication was typeset using $\mathcal{A}\mathcal{M}\mathcal{S}$-TEX, the American Mathematical Society's TEX macro system.
10 9 8 7 6 5 4 3 2 1 98 97 96 95 94 93

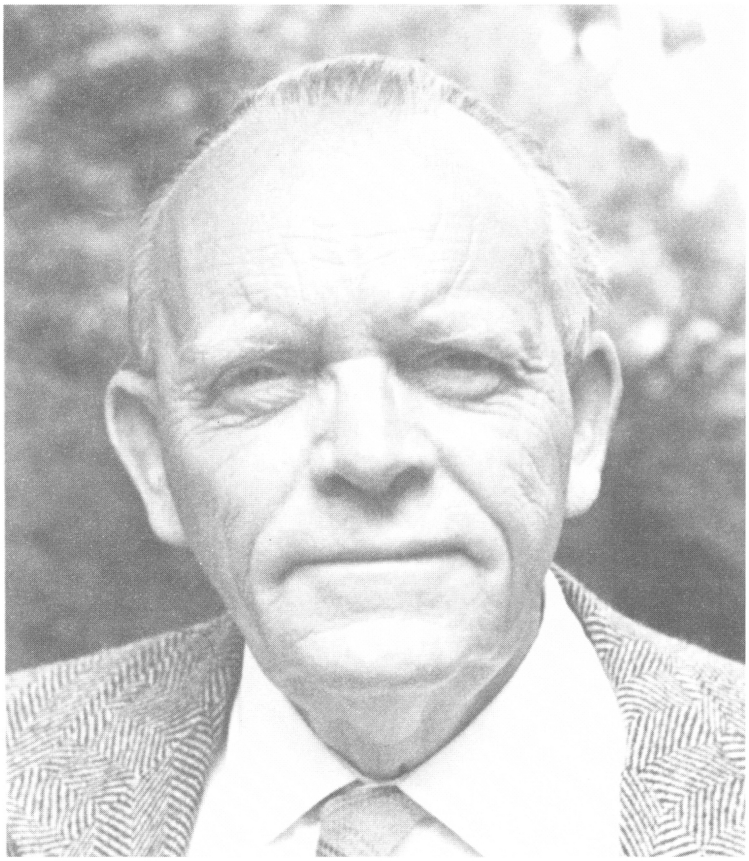
MATHEMATICS OF COMPUTATION

SPECIAL ISSUE

DEDICATED TO

DERRICK HENRY LEHMER

JULY 1993



Derrick Henry Lehmer
(1905–1991)

Dedication

Derrick Henry Lehmer (1905–1991)

It is not the policy of this journal to publish memorial issues; nevertheless, in the case of D. H. Lehmer it was felt that an exception should be made. This is simply because his case is unique in that he was the last remaining member of the committee that founded *MTAC* which later became *Mathematics of Computation.* As early as 1940, Lehmer was a member of the Executive Committee on Mathematical Tables and Aids to Computation, which had been established under the chairmanship of R. C. Archibald by the National Research Council. At that time, Lehmer was solely responsible for tables classified under Sections F (Theory of Numbers) and G (Higher Algebra). He also served on the subcommittee for Section Z (Calculating Machines and Mechanical Computation). In fact, the first report of the Committee, issued in 1941, was Lehmer's [8] on Section F, a volume which is still of considerable historic value and interest, but, unfortunately, is rather difficult to obtain today.

In January of 1943 this Committee published the first issue of the quarterly journal: *Mathematical Tables and other Aids to Computation* (*MTAC*). The two editors listed on the title page were Archibald and Lehmer. Lehmer continued to serve as a member of the Executive Committee and as one of the two editors for *MTAC* until 1949. In 1950 he became chairman of the Editorial Board for *MTAC*, a position he held until the end of 1954. In 1959 the Editorial Committee of *MTAC* unanimously approved a motion to change the name of the journal to *Mathematics of Computation.* This name change was meant to reflect a greater emphasis on research papers in the theory of computation and a slight de-emphasis on printed tables as such. Thus, Lehmer's association with *Mathematics of Computation* started even before the journal itself began.

Lehmer (Dick, as he was known to his friends) was born in Berkeley, California, on February 23, 1905. His father, Derrick Norman Lehmer, was a professor of Mathematics at Berkeley and was particularly interested in number theory, an interest that would have a profound effect upon his son. Lehmer graduated from Berkeley with an undergraduate degree in Physics in 1927, and in 1930 obtained his Ph.D. in Mathematics under Tamarkin at Brown University. Like many others during the Great Depression, he had difficulties in finding a permanent position. He spent some time at the California Institute of Technology, the Institute for Advanced Study, and Lehigh University until, in 1940, he accepted a position in the Mathematics Department at Berkeley, where he remained until he retired in 1972 as an Emeritus Professor. He (and his wife and co-worker, Emma) continued an active program of research during his retirement until he died on May 22, 1991.

During his long academic career, Lehmer published 181 scientific papers on a variety of subjects. In the three volumes [16] containing a selection of his papers up to 1981, when the volumes were published, he divided his work

among 17 different headings. These include such areas of research as: Lucas's functions, tests for primality, continued fractions, Bernoulli numbers and polynomials, Diophantine equations, numerical functions, etc. From the point of view of computational number theory, I consider his most important work to have been in the subjects of primality testing, factoring, sieves, and power residues. It should not, however, be forgotten that he made a number of major contributions to such areas as cyclotomy (a subject in which both he and his wife maintained an active interest throughout his intellectual life), partitions, modular forms, combinatorics, and, particularly, to the general area of computational techniques. In connection with this last topic, it is important to realize that he was also a very skilled numerical analyst. In fact, his first two papers in *MTAC* were on computing the Bessel function $I_n(x)$ [9] and the Graeffe process as applied to power series [10]; also, his machine method [13] for solving polynomial equations broke new ground. Further evidence of Lehmer's numerical analytic capabilities are certainly displayed in his very significant work [11, 12] on computing the zeros of the Riemann Zeta function and in his paper [7] on the computation of $p(n)$ using the Hardy-Ramanujan series.

Lehmer is perhaps most widely known for the Lucas-Lehmer primality test for Mersenne numbers. This came about as a result of the more general investigations, contained in his Ph.D. thesis [6], into what are now called Lehmer functions. He continued his interest in primality testing throughout his career. In particular, the paper [3] which he wrote with Brillhart and Selfridge exercised a very great influence upon the subject. Indeed, it is no exaggeration to state that its central ideas still form the basis of much modern thinking on the subject.

While an undergraduate, Lehmer began his life-long fascination with number sieves. Broadly speaking, these are electro-mechanical devices that are designed to find integers satisfying systems of linear congruences by, in effect, testing every integer between fixed bounds as a possible solution. Lehmer's first sieve, made from bicycle chains, was completed in 1927 and could test for solutions at the rate of 60 integers per second. Several such machines later, he was able to announce [14] that the DLS-127 could sieve numbers at the rate of 1,000,000 per second. Recently, C. D. Patterson [18] has constructed a VLSI sieve chip which can sieve at a rate of at least 200,000,000 numbers per second. It is not well known, but, as late as 1970, the most powerful integer factoring methods available involved the use of number sieves. It was the development of the continued fraction factoring technique by Morrison and Brillhart [17] in 1970 that ended the dominance of number sieves in factoring. Curiously, this paper of Morrison and Brillhart is an extension of previous work of Lehmer and Powers [15]. Three of Lehmer's original sieves, including the DLS-127(157), and a model of his bicycle chain sieve, are now in the Computer Museum in Boston.

Much of the impetus for Lehmer's development of factoring techniques derived from the 1925 book of Cunningham and Woodall [5] on factorizations of $b^n \pm 1$ for $b = 2, 3, 5, 6, 7, 10, 11, 12$. The tables in [5] listed the known prime factors of $2^n \pm 1$ for $n \leq 500$, and of $b^n \pm 1$, $b > 2$, for $n \leq 109$, n odd, and for $n \leq 100$, n even. There were many numbers in these tables that the methods and equipment of the day were unable to factor. Over a

period of many years, Lehmer and Emma, later joined by Selfridge, Brillhart, and Wagstaff, collected factors of these difficult numbers, eventually publishing them in [4]. Still, some numbers from [5] had yet to be completely factored. In 1992 a factoring milestone was reached when the last remaining composite number in [5] was factored. For further details on Lehmer's life and work, and a complete list of his publications, see the notices of Brillhart [1, 2].

Lehmer's impact, particularly on computational number theory, has been enormous. It is difficult to investigate any aspect of this subject and not find a contribution from him. He was a most meticulous and careful researcher, whose investigative techniques have set the standard for his discipline. Whether they are aware of it or not, today's computational number theorists owe him an immense debt. He supervised 19 Ph.D. students, several of whom have also produced some very significant work. Furthermore, from his position as editor at the very beginning of *MTAC*, he was able to ensure the existence of a place in which computational number theorists could communicate their results. Indeed, so successful have he and his editorial successors been in this, that to this day *Mathematics of Computation* is the journal of choice for almost all authors of papers on computational number theory. It is to the memory of this singular individual that this memorial issue is affectionately dedicated.

H. C. Williams
for the editors

1. John Brillhart, *Derrick Henry Lehmer*, Acta Arith. **62** (1992), 207–220.
2. ——, *Derrick Henry Lehmer*, Notices Amer. Math. Soc. **40** (1993), 31–32.
3. J. Brillhart, D. H. Lehmer, and J. L. Selfridge, *New primality criteria and factorizations of* $2^m \pm 1$, Math. Comp. **29** (1975), 620–647.
4. J. Brillhart, D. H. Lehmer, J. L. Selfridge, B. Tuckerman, and S. S. Wagstaff, Jr., *Factorizations of* $b^n \pm 1$, $b = 2, 3, 5, 6, 7, 10, 11, 12$ *up to high powers*, Contemp. Math., vol. 22, Amer. Math. Soc., Providence, RI, 1983; 2nd edition, 1988.
5. A. J. C. Cunningham and H. J. Woodall, *Factorisations of* $y^n - 1$, $y = 2, 3, 5, 6, 7, 10, 11, 12$ *up to high powers* (n), Hodgson, London, 1925.
6. D. H. Lehmer, *An extended theory of Lucas' functions*, Ann. of Math. **52** (1930), 419–448.
7. ——, *On a conjecture of Ramanujan*, J. London Math. Soc. **11** (1936), 114–118.
8. ——, *Guide to the tables in the theory of numbers*, Bulletin of the National Research Council, no. 105, Washington, D.C., 1941, 177 pp.
9. ——, *Note on the computation of the Bessel function* $I_n(x)$, MTAC **1** (1944), 133–135.
10. ——, *The Graeffe process as applied to power series*, MTAC **1** (1945), 377–383.
11. ——, *On the roots of the Riemann zeta-function*, Acta Math. **95** (1956), 291–298.
12. ——, *Extended computation of the Riemann zeta-function*, Mathematika **3** (1956), 102–108.
13. ——, *A machine method for solving polynomial equations*, J. Assoc. Comput. Mach. **8** (1961), 151–162.
14. ——, *An announcement concerning the delay line SIEVE DLS-127*, Math. Comp. **20** (1966), 645–646.
15. D. H. Lehmer and R. E. Powers, *On factoring large numbers*, Bull. Amer. Math. Soc. **37** (1931), 770–776.

16. D. McCarthy, ed., *Selected papers of D. H. Lehmer,* 3 vols., Charles Babbage Research Centre, Winnipeg, Manitoba, Canada, 1981.

17. M. A. Morrison and J. Brillhart, *A method of factoring and the factorization of* F_7, Math. Comp. **29** (1975), 183–205.

18. C. D. Patterson, *The derivation of a high speed sieve device,* Ph.D. Thesis, Dept. of Computer Science, University of Calgary, Calgary, Alberta, Canada, 1991.

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*)

No microfiche supplement in this issue

MATHEMATICS OF COMPUTATION

CONTENTS

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

(*Continued on inside back cover*)

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