

**DANIEL SHANKS, DEDICATION
Special Issue
Mathematics of Computation**

This special issue of *Mathematics of Computation* (Volume 48, Number 177, January 1987) is dedicated to Daniel Shanks on the occasion of his 70th birthday. Since 1959, when Shanks joined the Editorial Committee for this journal, he has been a guiding force in shaping the computational number theory component of the journal, and has had an immense influence in the field. This volume contains papers by some of the top researchers in the field and covers such topics as elliptic curves, primality testing, congruences, class groups, and cyclotomic fields. Although a numbered issue of the *Mathematics of Computation* journal, it will serve as a stand alone reference work for computational number theory.

Contents

William W. Adams, *Characterizing Pseudoprimes for third-order linear recurrences*

Leonard M. Adelman, Dennis R. Estes, and Kevin S. McCurley, *Solving bivariate quadratic congruences in random polynomial time*

Richard Blecksmith, John Brillhart, and Irving Gerst, *Parity results for certain partition functions and identities similar to theta function identities*

Johannes Buchmann, *The computation of the fundamental unit of totally complex quartic orders*
Johannes Buchmann and H. C. Williams, *On principal ideal testing in totally complex quartic fields and the determination of certain cyclotomic constants*

Nicholas Buck, Lones Smith, Blair K. Spearman, and Kenneth S. Williams, *The cyclotomic numbers of order fifteen*

Duncan A. Buell, *Class groups of quadratic fields. II*

David G. Cantor, *Computing in the Jacobian of a hyperelliptic curve*

H. Cohen and A. K. Lenstra, *Implementation of a new primality test*

H. Cohen and J. Martinet, *Class groups of number fields: numerical heuristics*

Harvey Cohn and Jesse Deutsch, *Application of symbolic manipulation to Hecke transformations of modular forms in two variables*

T. W. Cusick and Lowell Schoenfeld, *A table of fundamental pairs of units in totally real cubic fields*

Daniel Gordon, Douglas Grenier, and Audrey Terras, *Hecke operators and the fundamental domain for $(\text{SL}(3, \mathbb{Z}))$*

Marie-Nicole Gras, *Special units in real cyclic sextic fields*

R. K. Guy, C. B. Lacampagne, and J. L. Selfridge, *Primes at a glance*

Neal Koblitz, *Elliptic curve cryptosystems*

D. H. Lehmer and Emma Lehmer, *Cyclotomic resultants*

H. W. Lenstra, Jr. and R. J. Schoof, *Primitive normal bases for finite fields*

R. A. Mollin, *Class numbers of quadratic fields determined by solvability of diophantine equations*

Peter L. Montgomery, *Speeding the Pollard and elliptic curve methods of factorization*

Morris Newman and Robert C. Thompson, *Numerical values of Goldberg's coefficients in the series for $\log(e^x e^y)$*

A. M. Odlyzko, *On the distribution of spacings between zeros of the zeta function*

M. Pohst, *On computing isomorphisms of equation orders*

Carl Pomerance, *Very short primality proofs*

Herman J. J. te Riele, *On the sign of the difference $\pi(x) - \text{li}(x)$*

Robert D. Silverman, *The multiple polynomial quadratic sieve*

Jonathan W. Tanner and Samuel S. Wagstaff, Jr., *New congruences for the Bernoulli numbers*

Heinz M. Tschöpe and Horst G. Zimmer, *Computation of the Néron-Tate height on elliptic curves*

Lawrence C. Washington, *Class numbers of the simplest cubic fields*

H. C. Williams, *Effective primality tests for some integers of the forms $A5^n - 1$ and $A7^n - 1$*

H. C. Williams and M. C. Wunderlich, *On the parallel generation of the residues for the continued fraction factoring algorithm*

Don Zagier, *Large integral points on elliptic curves*

1980 *Mathematics Subject Classification* 11
ISSN 0025-5718

448 pages (softcover), January 1987
Individual member \$29, List price \$48,
Institutional member \$38
To order, please specify SHANKS/MC

Shipping/Handling. 1st book \$2, each add'l \$1,
\$25 max. By air, 1st book \$5, each add'l \$3,
\$100 max.

Prepayment required Order from AMS, P.O. Box
1571, Annex Station, Providence, RI 02901-9930,
or call 800-556-7774 to use VISA or MasterCard



(Continued from back cover)

Reviews and Descriptions of Tables and Books	639
Oden and Carey 13 , Chavent and Jaffre 14 , Reinhardt 15 , Elschner 16 , Čížek 17 , Abramowitz and Stegun, Editors 18 , Bauer and Eidel 19a, b, c , Fibonacci (Sigler) 20 , van der Burgh and Mattheij, Editors 21 , Collatz, Meinardus and Nürnberger, Editors 22 , Keast and Fairweather, Editors 23 , Jamieson, Gannon and Douglass, Editors 24 , Deuffhard and Engquist, Editors 25	
Table Errata	653
Bateman Manuscript Project 610 , Oberhettinger and Badii 611 , Fibonacci 612	
Corrigenda	655
Rabinowitz, Dueck and Williams	
Author Index	659

No microfiche supplement in this issue

MATHEMATICS OF COMPUTATION

TABLE OF CONTENTS

April 1988

Kenneth Eriksson and Claes Johnson , An Adaptive Finite Element Method for Linear Elliptic Problems	361
Sunil Kumar , Superconvergence of a Collocation-Type Method for Simple Turning Points of Hammerstein Equations	385
Andrew R. Conn, Nicholas I. M. Gould, and Philippe L. Toint , Testing a Class of Methods for Solving Minimization Problems with Simple Bounds on the Variables	399
D. Bini and V. Pan , Efficient Algorithms for the Evaluation of the Eigenvalues of (Block) Banded Toeplitz Matrices	431
James W. Demmel , The Probability That A Numerical Analysis Problem Is Difficult	449
F. W. J. Olver , Error Bounds for Linear Recurrence Relations	481
Jean-Francois Loiseau, Jean-Pierre Codaccioni, and Regis Cáböz , Hyperelliptic Integrals and Multiple Hypergeometric Series	501
Henry L. Gray and Nien fan Zhang , On a New Definition of the Fractional Difference	513
Shu Tezuka , On Optimal GFSR Pseudorandom Number Generators	531
Emma Lehmer , Connection Between Gaussian Periods and Cyclic Units ...	535
René Schoof and Lawrence C. Washington , Quintic Polynomials and Real Cyclotomic Fields with Large Class Numbers	543
Harvey Cohn and Jesse Deutsch , An Explicit Modular Equation in Two Variables for $\mathbf{Q}(\sqrt{3})$	557
Johannes Buchmann and H. C. Williams , On the Infrastructure of the Principal Ideal Class of an Algebraic Number Field of Unit Rank One	569
Pascual Llorente and Jordi Quer , On Totally Real Cubic Fields with Discriminant $D < 10^7$	581
Francis Buekenhout and Sarah Rees , The Subgroup Structure of the Mathieu Group M_{12}	595
E. Seah and D. R. Stinson , On the Enumeration of One-Factorizations of Complete Graphs Containing Prescribed Automorphism Groups	607
A. J. Stephens and H. C. Williams , Some Computational Results on a Problem Concerning Powerful Numbers	619
S. Battiato and W. Borho , Are There Odd Amicable Numbers Not Divisible by Three?	633

(Continued on inside back cover)