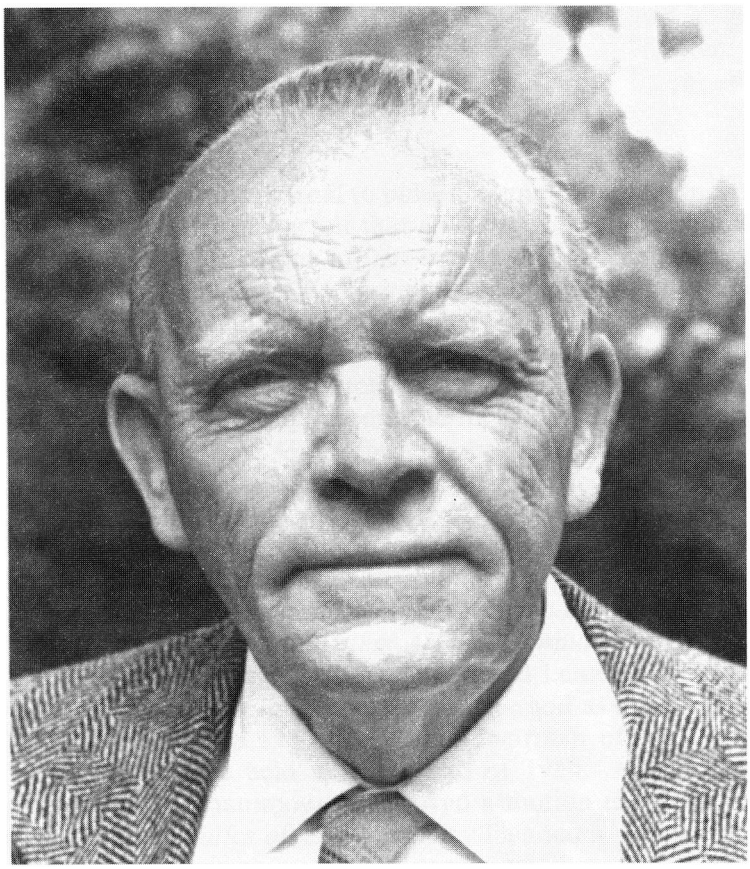

DERRICK HENRY LEHMER
(1905–1991)

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.