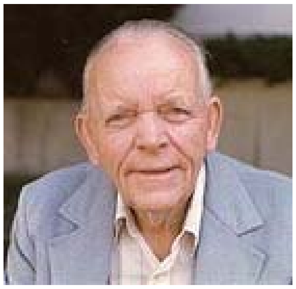
Derrick Henry Lehmer

Born February 23, 1905, Berkeley, Calif.; died May 22, 1991, Berkeley, Calif.; pre-WWII inventor of a mechanical method of solving congruence relations and finding prime numbers.



Education: AB, University of California, Berkeley, 1927; ScM, mathematics, Brown University, 1929; PhD, mathematics, Brown University, 1930.

Professional Experience: assistant, Brown University, 1928; National Research Council Fellow, California Institute of Technology, 1930-1932; researcher, Institute for Advanced Study, Princeton, N.J., 1933-1934; instructor, Lehigh University, 1934-1938; assistant professor, Lehigh University, 1938-1940; professor, University of California, Berkeley, 1940-1972, professor emeritus, 1972-1991; mathematician, Aberdeen Proving Ground, 1945-1946; director, Institute for Numerical Analysis (INA), National Bureau of Standards and University of California, Los Angeles, 1951-1953.

Honors and Awards: Guggenheim Fellow, Cambridge University, 1938-1939; Fullbright Lectureship in Australia, 1959; vice president, American Mathematical Society, 1953; vice president, Association for Computing Machinery, 1954-1957, research professor, Miller Institute for Basic Research in Science at Berkeley, 1962-1963.

Part 1. Sieve Computers[1]

Mechanical Sieve Computers

While an undergraduate at the University of California at Berkeley, Dick became interested in mechanizing the solution of linear congruence relations such as $x = y(m)$. The problem is to find those integer values of x (y or m) such that $x - y$ is a multiple of m. For example, if one can find an m different from 1 which satisfies $2^{257} = 1$ (m), then the Mersenne[2] conjecture that $2^{257}-1$ (a number of over 77 decimal digits) is prime is false. While still a graduate student (1928 to 1930) Dick and his wife, Emma, spent many hundreds of hours manually showing that $2^{257}- 1$ was not prime. They worked independently, comparing numbers at each step, so as to be confident in their results. Such congruence relations are useful in the problem of representing a number as the sum or difference of two squares. Obviously, if a number can be represented in the form $a^2 - b^2$ then a - b and a + b are factors. A machine (a special-purpose computer) which scans numbers in sequence searching for those that satisfy such congruence relations is called a sieve. Dick gives a more general definition in A *History of Computing in the Twentieth Century* (Metropolis et al. p. 445).

Dick's first sieve, constructed in the students' workshop at the University of California, Berkeley, in 1926, while he was an undergraduate, used 19 separately looped bicycle chains whose number of links were the primes up

[1] [Harry Huskey] I have divided this somewhat informal obituary of my friend, Dick, into two parts. First I describe his unique mechanical and electronic sieve computers, and then I tell the story of his life.

[2] Marin Mersenne (1588-1648) was a monk, a French mathematician, natural philosopher, and theologian. He studied numbers of the form 2*p*-1 where *p* is prime, and now such numbers are called Mersenne numbers.

to 67. Actually, very short chains were not practical, so the small primes were handled by “composite” chains of nonprime lengths 22, 25, 26, 27, 49, and 64 links representing the primes 11, 5, 13, 3, 7, and 2. These chains hung in loops from 10-tooth sprockets on a common shaft which was driven by a motor. A counter indicated how many teeth or links had passed the top position. Each chain (both of prime and composite length) had a zero position or link (painted red). Suppose each chain had a “pin” attached at the zero link. The composite chains had several pins, one at each multiple of each prime which divided the length of that chain. For example, the chain of length 22 had pins on all the even numbered links as well as on link 11. If for some (large) number of teeth *N*, a pin of one of the chains was at the top, then that corresponding prime divided *N*. Conversely, if for *N* no pin was at the top, then any prime divisors must be greater than 67.

Dick described (Lehmer 1928, p. 115) the pin arrangement as follows: “Whenever a link provided with a pin arrives at the top of the shaft a small spring with a tungsten point is lifted by the projecting pin. This breaks for the moment the electric contact between the spring and a brass bar running parallel to the shaft. By means of a relay in the circuit, the motor is shut off and the machine stops itself When several chains are provided with springs the machine will not stop unless all the springs are lifted, so that every time the machine stops it means that a number satisfying all the imposed conditions has appeared. This number can be read directly by means of a revolution counter connected to the shaft. The shaft revolves at 300 rpm so that the machine canvases 3,000 numbers per minute. When all chains are provided with springs a “solution” occurs once in several hours, during which time the machine runs without any attention.” The machine scanned about 4.3 million numbers per day, so the Mersenne number 2^{211} - 1 would require more than 1,070 years! This difficulty is overcome by applying number theory techniques too complicated for us to consider here.

To explain the use of the machine Dick gave (Lehmer 1928, p. 115) the following example: Consider the representation of the beautiful number

$$N =9999000099990001$$

(which happens to be (1020 + 1)/(104 + 1)) as a difference of two squares, a^2 - b^2. After nearly two pages of analysis (Lehmer 1928, p, 118) he concluded that *a* must be congruent to 2,3,9,16,23,30,37, and 44 modulo 49 (i.e., *a*= 2 (49), *a* = 3 (49), etc.).

These are called quadratic residues since 49 = 7^2. Now if pins are placed on links 2, 3, 9, 16, 23, 30, 37, and 44 on the 49-chain, then electrical contact will be broken for numbers satisfying the above relations. Similar relations are worked out for the other chains, pins are placed, and the machine started. After about two hours the machine stops, giving

$$a= 2983262201$$

and

$$N = (a - b) * (a + b) = 1676321*5964848081.$$

A model of this bicycle chain sieve has been constructed at the Computer Museum in Boston but in 1992 it was not on exhibit. In 1932 Dick constructed a much faster sieve using gears with different numbers of teeth (as above) driven from a common pinion.

He described it as follows (Lehmer 1934, p. 663): “There are 30 driven gears, all driven at the same linear speed of about 1700 meters per minute by a single driving gear. The 30 driven gears correspond to 30 moduli and have for numbers of teeth convenient multiples of every prime less than 127. The largest gear has 128 teeth and the smallest 67 teeth. At the base of each tooth on each driven gear, holes are drilled at a constant distance from the periphery of the gear, this distance being the same for all gears. These holes are about 2 millimeters in diameter and correspond to the numbers 0, 1, 2, - - - , p - 1 modulo p. If x is to be restricted to a set of s numbers modulo p the holes corresponding to these numbers are left open, while other holes are stopped with wooden pins. The gears are mounted parallel to one another and a common line of tangency so that if a beam of light from an incandescent lamp shines through a hole in any gear it is transmitted or blotted out by the next gear. If the driving gear is rotated (from some zero position) until x teeth have turned past and if x satisfies the conditions imposed by all the moduli, then there will be an alignment of open holes and the beam of light will traverse the system of gears.” A photocell detected whether a beam of light could pass through all the holes. At speed, the device processed 5,000 numbers per second and coasted many thousands past a “hit.” Dick exhibited this “photoelectric sieve” and ran the Mathematics Exhibit at the Chicago World's Fair during the summer of 1932.

Laura Gould, his daughter, describes a sieve “built sometime in the Thirties I suppose, which operated on loops of movie film-8 mm or 16 mm, I don't know which-of various lengths.[1] [2]

“The frames of these film loops were either punched (with a streetcar conductor's punch) or not, depending on the characteristics of the problem being run. These loops ran over a row of parallel pulley heads while an electric eye watched along these heads to detect either no punches or all punches, I'm not sure which. This machine was stored in my closet when I was a child. At home it was called the “baby ‘chine” because the celluloid would run smoothly over the wooden heads only if it was well dusted with baby powder. This fragrance lingered in my closet for many years.”

General-Purpose Computers as Sieves

After describing the three kinds of sieves Dick said (1980): “Our next date is 1946 and this, of course, is the ENIAC. Can we use the high speed computer to do the sieve process? This was a highly parallel machine, before von Neumann spoiled it. We were able to build a sieve into it. I remember the occasion very clearly. We had a Fourth of July weekend situation when the Lehmer family was allowed to come in and pull everything off the machine and reset the ENIAC for our particular problem. The Lehmer family consisted of myself, my wife, and two teenage kids [Donald and Laura]. We marched in on the Friday about 5 p.m. and started setting it up with an entirely different kind of problem not concerned with interior or exterior ballistics. There was one other person there, *a meteorologist named John Mauchly* (emphasis added). He was the one who suggested that we ought to use some of the arithmetic units to make a kind of sieve, and I remember that we worked it out in a restaurant just before we went to work.” There were a long series of sieve programs written for various general-purpose computers such as the SWAC and the IBM-7094. Perhaps the best of these was a 7094 program written by John Brillhart that accomplished 100,000 counts per second. “The technique,” Dick said, “to get the high speed was to combine many moduli into five or six very long chains which filled most of memory.”

Electronic Sieves

[1] Laura Gould, private communication.

[2] According to Lehmer (1980) it was built in 1936 and was 16 mm.

In the early 1950s Dick, in cooperation with Paul Morton of the Electrical Engineering Department at Berkeley, had worked on a general-purpose magnetic drum computer (CALDIC-California Digital Computer). Thus, it was natural that they would cooperate in building electronic sieves. After a first abortive effort using electronic counters, which had reliability problems, they built a delay line version using Navy surplus electrical delay lines (Dick was "leery" of mercury delay lines). There were a number of recirculating delay lines of various lengths like the bicycle chains, movie film, or wheels of the earlier sieves. The system operated in two modes, serial (or idle) mode and parallel mode. In the idle mode all lines were connected in series, and bits were inserted one at a time using counting circuits; then the system was switched to parallel where each delay line recirculated independently. When a coincidence occurred the system automatically switched back to serial. I can remember stopping at the room in Cory Hall at UCB and if the sieve was in serial mode there was a flurry of activity as Emma or Dick copied down the "hit" number and did some auxiliary computation to see if this was a number of interest or a spurious result. In 1980 Dick said: "That's the way the delay line sieve has been operating for ten years now, 24 hours per day. We have no maintenance and since the whole system is just a long piece of wire, nothing ever went wrong to speak of except for occasional counter printer trouble." This system did 1 million counts per second. The above machine was followed by a shift register version that ran at 20 million counts per second. Dick mentioned (1980) that a Russian publication in 1970 said there was "one of Lehmer's sieves in the Institute for Mathematics in Leningrad," but claimed, "I don't know anything about it. All I can say is that none of my sieves is missing."

Part II. His Life

Early Life

Derrick H. Lehmer was born on February 23, 1905 in Berkeley, California. His father, Derrick N. Lehmer, was professor of mathematics and his mother, Eunice Mitchell, was a poet. He was one of five children; only an older sister survives. His father's interest in number theory and computation started Dick on a long and distinguished career in that field. He was educated in the Berkeley public schools and entered the University of California at Berkeley (UCB) in 1923. He graduated with an AB degree in mathematics in 1927 and spent 1927-1928 at the University of Chicago taking mathematics courses from Dickson, Bliss, Lane, and Graves. In 1928-1929 he was a graduate assistant at Brown University, where he received his MSc degree in mathematics in 1929 and his PhD in 1930, his thesis being titled, "An Extended Theory of Lucas' Functions." Lucas had published a well known book on number theory in Paris in 1891 entitled "Theorie des Nombres." Dick's thesis was essentially unsupervised since no one at Brown was interested in number theory, but he did have weekly discussions with Tamarkin. His thesis was sent to E.T. Bell at the California Institute of Technology for review. In 1928 he married Emma Trotskaya, who was also a mathematician and number theorist and was one of his father's students. He was appointed to the Henry D. Sharpe Fellowship in 1929 at Brown University.

1930-1945

Dick had a National Research Fellowship from 1930 to 1932 working with E. T. Bell at the California Institute of Technology (1930-1931) and with Uspenski at Stanford (1931-1932). He then received a Princeton Institute Fellowship [the Institute for Advanced Study was just being formed] for 1933-1934. He taught at the Stanford Summer School in 1934, and then taught mathematics at Lehigh University from 1934 to 1940. He was on leave from Lehigh for 1938-1939 on a Guggenheim Fellowship at Cambridge and Manchester Universities in England. In 1940 he joined the Mathematics Department at UCB as an assistant professor.

World War II

In 1945 Dick took a temporary appointment at the Ballistic Research Laboratory of Aberdeen Proving Ground. They were financing the construction of the ENIAC (the first electronic general-purpose computer) at the University of Pennsylvania. He observed the completion of the ENIAC and participated in its testing. It was while working on the ENIAC that I first met Dick. At the end of the war (1946) he returned to the Mathematics Department at UCB as an associate professor.

The Institute for Numerical Analysis

In 1950, taking exception to the loyalty oath requirements of UCB (a result of the McCarthy era), he left, taking leave without pay, and joined the Institute for Numerical Analysis of the National Bureau of Standards at the University of California at Los Angeles. He was director of the Institute for two years, 1951 to 1953. The SWAC (National Bureau of Standards Western Automatic Computer, the first stored-program computer on the West Coast) was just becoming operational at the institute. About this time, Raphael Robinson at the UCB Department of Mathematics, using the SWAC instruction documentation, programmed the Lucas test for primality to search for Mersenne primes. This was mailed from Berkeley to Los Angeles, the program was punched, and it ran on the SWAC without error. It quickly verified the known results and that evening found two new primes, 2^{521} - 1 and 2^{607} -_ 1.

Back to Berkeley

Dick returned to Mathematics at UCB in 1954, when the signing of the loyalty oath was no longer required. He was chairman of the Mathematics Department from 1954 to 1957, where he was instrumental in my joining UCB in 1954. He was vice chairman of the Letters and Science Computer Science Department from 1969 to 1970. He retired in 1972, becoming professor emeritus.

Publications, Awards, and Honors

He published over 181 research papers and received a number of awards, invitations, honors, and elective offices in professional societies. Among these were: Guggenheim Fellowship (Cambridge University, 1938), Fulbright Lectureship (Australia, 1959), Research Professorship (Miller Institute for Basic Research in Science, Berkeley, 1962-1963), invited address at the 1958 International Congress of Mathematicians, Gibbs Lecturer (American Mathematical Society, 1964), vice president of the American Mathematical Society (1953-1954) and of the American Association for the Advancement of Science (1955-1956), and Council Member at Large of the Association for Computing Machinery (1953-1954) and a Governor of the Mathematical Association of America (1953-1954).

Reprise

Dick excelled in using computers to solve problems in number theory. Typically, he used computers to prove conjectures wrong, to reduce the number of cases to be investigated, or to show that additional assumptions were required. Dick was a popular lecturer, spoke in a relaxed manner, and always provided opportunities for dialogue with students. His informal methods and droll humor were very effective. For example, he might start some pronouncement with the words “the other day . . .” and later you would discover that the event being described happened 20 years ago! Dick was a very considerate person. Many Saturday mornings he and Emma invited graduate students and young faculty to accompany them on walks in the Berkeley Hills[1].

BIBLIOGRAPHY

Biographical

Brillhart, John, “Derrick H. Lehmer,” *Mathematics of Computation*, to be published.

Kelley, J.L., Raphael M. Robinson, Abraham H. Taub, and P. Emery Thomas, “In Memoriam,” University of California, Berkeley, 1991, pp. 112-115.

Lehmer, D.H., “A History of the Sieve Process,” in Metropolis, N., J. Howlett, and Gian-Carlo Rota, *A History of Computing in the Twentieth Century,* Academic Press, New York, 1980, pp. 445-456.

Significant Publications

Lehmer, D.H., “The Mechanical Combination of Linear Forms,” *American Mathematical Monthly,* Vol. 35, 1928, pp. 114-121.

Lehmer, D.H., “A Machine for Combining Sets of Linear Congruences,” *Mathematische Annalen*, 1934, pp. 661-667.

UPDATES

Portrait added (MRW, 2013)

[1] Harry D. Huskey.