Feb. 23rd

Derrick Henry (Dick) Lehmer

Born: Feb. 23, 1905;

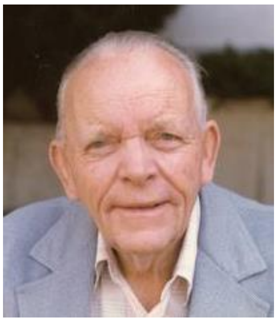
Berkeley, California
Died: May 22, 1991

In mathematics, Lehmer is perhaps best remembered for improving on Édouard Lucas' work during the 1930's to produce the Lucas-Lehmer test for Mersenne primes. Within computing, he served on the ENIAC [Feb 15] Computations Committee which decided how the machine would be used after it was moved to the Ballistics Research Lab at the Aberdeen Proving Grounds [July 29]. The other committee members were Haskell Curry [Sept 12], Leland Cunningham, and Franz Alt.

This job also meant that he wrote some of the first test programs for the ENIAC, mainly related to prime sieving and pseudorandom number generation. The prototypical prime sieve is the one ascribed to Eratosthenes (276 BC – 194 BC), which can be coded in a few lines of (inefficient) Haskell:

```
primes = sieve [2..]
where sieve (p:xs) =
  p : sieve (minus xs
              [p, p+p..])
```

On July 9, 1946: Lehmer delivered the talk "Computing Machines for Pure Mathematics" as part of the Moore School Lectures [July 8].



Derrick Henry Lehmer (1984). Photo by George Bergman. GFDL.

Lehmer later continued his work on Mersenne primes [Jan 30] using the Standards Western Automatic Computer (SWAC) [Aug 17].

For recent searches for Mersenne primes, see GIMPS [Jan 3], [Sept 18].

Enigma Patent Filed

Feb. 23, 1918

Arthur Scherbius, a German electrical engineer, filed a patent for a mechanical cipher machine about the size of a typewriter, which the Scherbius and Ritter company later sold under the name Enigma [July 15].

The Enigma's encryption was built around three rotors which could be adjusted to map letters to different ones. A typed input letter passed through all three rotors, bounced off a "reflector", and passed back through all the rotors in the other direction, to produce a nicely scrambled new letter. A plugboard added to the mix by sitting between the main rotors and the machine's input and output, to swap pairs of letters. In the earliest machines, up to six pairs could be flipped; later models increased the number to ten, and added a fourth rotor.

Despite this complexity, all an operator needed to set up the machine was the starting positions and order of the three rotors, plus the positions of the plugs in the board.

The Enigma was initially pitched at the commercial market, but sales took off when one was purchased by the German Navy in 1926. The German Army saw its value, and also started using Enigma machines a few years later (of course modified to be different from the Navy's).

Although the Enigma wasn't a computer, it stimulated computer design, including the development of machines like the Polish bomba [Aug 16], the bombe [March 18], the Heath Robinson [June 1], and the Colossus [Jan 18].

John Clifford Shaw

Born: Feb. 23, 1922;

Southern California
Died: Feb. 9, 1991

Shaw was co-author with Herbert A. Simon [June 15] and Allen Newell [March 19] of the first AI program, the "Logic Theorist" [Aug 9], and one of the developers of IPL (Information Processing Language) [Feb 26], used to implement it. IPL introduced numerous programming ideas that are common practice today, such as lists, recursion, and higher-order functions.

The same group also created the influential "General Problem Solver" (GPS [Dec 30]), and Shaw developed the JOSS (JOHNNIAC Open Shop System) [June 17], one of the first interactive, time-sharing services.

ISO

Feb. 23, 1947

Since it was founded in London, the ISO (International Standards Organization) has published over 22,000 standards covering most aspects of technology and business.

It played an important role in standardizing programming languages (e.g. for FORTRAN [Feb 26], SQL [May 1], C++ [Oct 14], and C [Dec 8]). But perhaps its most significant standard is the OSI (Open Systems Interconnection) architecture for networks [Feb 28]. Another popular one is the ISO 9660 standard for file systems used by CD-ROMs [Sept 1].

ISO acts as an umbrella organization for over 160 national standards bodies. For example, ANSI (the American National Standards Institute) is a member.

Officially the letters "ISO" are not an acronym because

"International Standards Organization" would have different acronyms in different languages (e.g. OIN in French). ISO is instead a real word derived from the Greek "isos", meaning equal.

TED Founded

Feb. 23, 1984

The TED (Technology, Entertainment, Design) conference was conceived by architect and graphic designer Richard Saul Wurman as a place where speakers (aka Tedsters) had a maximum of 18 minutes to present their ideas.

The first TED included a demo of the compact disc [Aug 17], the e-book, 3D graphics from Lucasfilm [Sept 12], and Benoit Mandelbrot [Nov 20] talking about fractal geometry. Nevertheless, the event was financially unsuccessful, and it was six years before a second meeting was held.

Chris Anderson, the Curator of TED (2007). Photo by Pierre Omidyar. CC BY 2.0.

In 2001, Wurman sold TED to Chris Anderson, and under his leadership TED expanded to cover a broader range of topics, including business and global issues; it also adopted the catchy slogan, "ideas worth spreading".

Videos of the talks were posted on the TED website, and to dedicated YouTube and iTunes channels, which proved a savvy move. On Nov. 13, 2012, the TED site reported that it had reached its billionth video view. As of Dec. 2020, over 3,500 TED Talks were available at the site.

There have been a few naysayers: in 2010, statistician Nassim Taleb called TED a "monstrosity that turns scientists and thinkers into low-level entertainers, like circus performers." Also, attendance at the 2018 conference cost $10,000 per person.

Stac Wins

Feb. 23, 1994

Stac (short for "State of the Art Consulting") Electronics filed a lawsuit against Microsoft in Jan. 1993 over the inclusion of file compression software called DoubleSpace in MS-DOS 6.0 [Aug 12], which it claimed infringed Stac's patents.

Microsoft had previously been in discussions with Stac to license its technology, which had involved detailed technical discussions with Stac engineers, and examinations of Stac's code. Microsoft argued that it had licensed its DoubleSpace technology from another file compression company, Vertisoft.

On this day, a California jury awarded Stac $120 million in damages, worth about $5.50 for each copy of MS-DOS 6.0 sold. The jury also agreed with a Microsoft counterclaim, and awarded Microsoft $13.6 million.

Microsoft had obviously realized which way the wind was blowing and had already started shipping an "upgrade" of MS-DOS (v.6.21) which removed DoubleSpace.

At the end of 1994, Microsoft and Stac came to an agreement involving Microsoft investing $39.9 million in Stac, and paying $43 million in royalties.

First Java Demo

Feb. 23-25, 1995

Prev: [Jan 00] Next: [May 23]

John Gage and James Gosling [May 19] gave the first public Java demo at the TED6 conference [two entries back], three months before the official announcement of Java at SunWorld '95 [May 23].

Gage, then director of Sun's Science Office, was planning to demonstrate the WebRunner browser (later to be called HotJava). Gosling, concerned that the still-rough browser might crash in a major public demonstration, joined Gage as his "demo dolly."

Gosling recalled later that at the beginning of the talk many people were only casually paying attention. After all, what was so exciting about a new language driving a page of text and pictures in a clone of Mosaic? [Sept 28] Then Gosling moved the mouse over an illustration of a 3D molecule in the middle of the text, which promptly rotated with the mouse movement: back and forth, up and around. "The entire audience went `Aaaaaaah!'" remembered Gosling. "Their view of reality had completely changed because it MOVED." Now everyone was paying close attention.

Next, Gosling and Gage amazed the crowd with an animated line-sorting algorithm that Gosling had written.

But... Richard Wurman, who ran the conference that year, recalled that there wasn't much of a reaction to the presentation. "Later, of course," he added, "everyone who was there said, 'Oh my God, I saw it there first.'"

Distributed DES Challenge

Feb. 23, 1998

The DES [Jan 15] Challenges were a series of contests created by RSA Data Security to highlight the lack of security provided by the Data Encryption Standard (DES).

In 1997, 40-bit, 48-bit, and 56-bit DES keys had been cracked by various teams [Jan 28]. But the first *distributed* DES challenge took a different approach – tens of thousands of computers were linked across the Internet to decrypt a 56-bit key. That size was chosen since it was the strongest exportable encryption allowed by US law at the time.

The participants collectively examined 6.3 x 10^{16} (63 quadrillion) keys, or about 87% of the entire keyspace, before the correct one was found on the fortieth day. The decrypted message read, "The secret message is: Many hands make light work."

Perhaps forty days wasn't too bad, but DES Challenge III, in Jan. 1999, involved another distributed effort, this time with the help of special purpose hardware called "Deep Crack". The 56-bit key was found in a mere 22 hours and 15 minutes.

Industry and federal authorities had to finally admit that 56-bit DES keys were ineffectual, and the government started to allow the export of 128-bit keys. Some technical people claimed this was equivalent to rearranging the deck chairs on the Titanic, and eventually DES was withdrawn, replaced by the Advanced Encryption Standard (AES [Jan 15]).

Christie's "The Origins of Cyberspace"

Feb. 23, 2005

Christie's held its first auction of computer technology, under the title "The Origins of Cyberspace: A Library on the History of Computing, Networking & Telecommunications". The items came from Jeremy Norman, which he'd been collecting since 1971. They included:

- Ada Lovelace's "Sketch of the Analytical Engine Invented by Charles Babbage . . . with Notes by the Translator" [July 10].
- A first edition of Karel Capek's play "Rossum's Universal Robots" [Jan 25].
- The first published paper on the stored-program computer, "Preliminary Discussion of the Logical Design of an Electronic Computing Instrument" by John Von Neumann, Arthur W. Burks and Herman H. Goldstine [June 28].
- "Outline of Plans for Development of Electronic Computers" by J. Presper Eckert and John Mauchly (dated March 13, 1946). This was essentially the business plan the pair wrote just before they left the Moore School [March 31].

There was also materials from Edmund Berkeley [Feb 22], John Atanasoff [Oct 4], Howard Aiken [March 8], Grace Hopper [Dec 9], Vannevar Bush [March 11], Jay Forrester [July 14], John McCarthy [Sept 4], and many others.

The auction brought in more than $700,000, which was somewhat disappointing, as Christie's had estimated that the sale would rake in nearer $2 million.

Lovelace's sketch was the top seller, going for $78,000, followed by Eckert and Mauchley's business plan for $72,000. Third was a letter from Babbage to Humphry Davy giving some details of his difference engine [July 3], which sold for $38,400.

iTunes 1 Billion

Feb. 23, 2006

The iTunes Store [April 28] announced the sale of its one billionth song. The recipient was Alex Ostrovsky, age 16, of West Bloomfield, Michigan, and the song was "Speed of Sound" from the Coldplay album X&Y; it cost 99 cents

To commemorate the milestone, Ostrovsky received a phone call from an Apple employee (or perhaps Steve Jobs [Feb 24] according to some articles) with the news that he was getting ten iPods (one for each finger), an iMac, a $10,000 music gift certificate, and a Juilliard School scholarship.

Not a bad result for Ostrovsky, who wasn't an iTunes regular. "I've downloaded maybe 50 songs." he told *The New York Times*. "I'm certainly going to download more songs now."

Four years and one day later (on Feb. 24, 2010): the 10 billion songs record was reached. By May 28, 2014, the store had sold 35 billion.