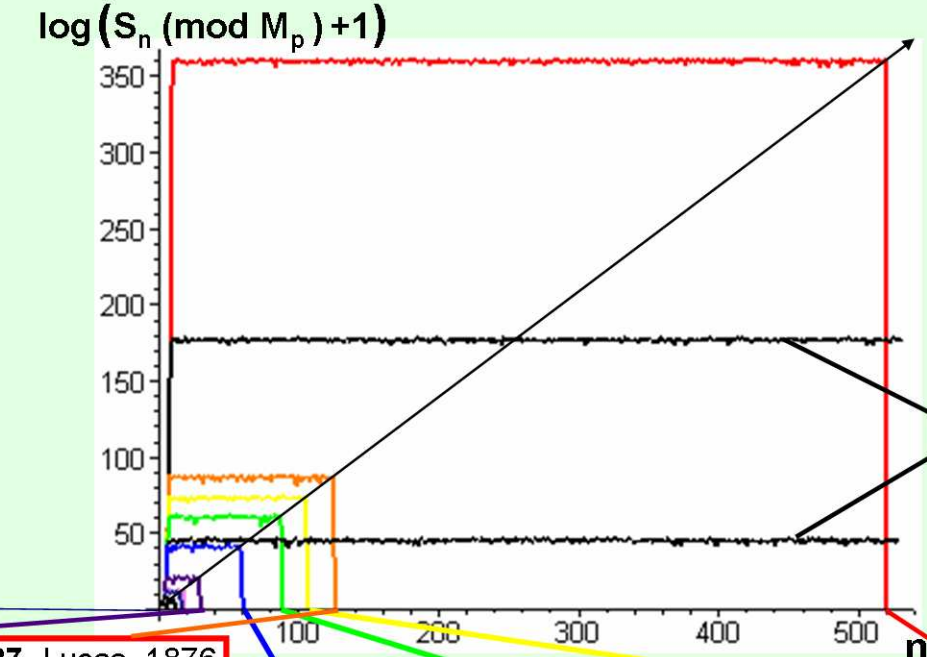
THEOREM OF THE DAY

The Lucas-Lehmer Test *The number* $M_p = 2^p - 1$, *for* p *an odd prime, is itself prime if and only if it divides* S_{p-1}, *the* $(p-1)$*-th term in the series:* $S_1 = 4,\ S_2 = 14,\ \ldots,$ *and, for* $i \geq 1,\ S_{i+1} = S_i^2 - 2$.



17, 19, Cataldi, 1588

31, Euler, 1772

127, Lucas, 1876

61, Pervushin , 1883

89, Powers, 1911

107, Powers, 1914

521, Robinson, 1952

67, 257 Mersenne, 1644

24.9-million digit Mersenne prime found!

Primes of the form $2^p - 1$ must have p also prime and are called *Mersenne primes*, after the French monk Marin Mersenne (1588–1648); they are, thanks to the Lucas-Lehmer test, the main focus of searches for large primes. The test is effective because the values of S_n, which quickly become gigantically large, can be remaindered modulo M_p as they are calculated. Primality testing of M_p, for various p values, is plotted in the graph above, on a log scale (to base e) to keep the different plots close together. For $p = 127$, for example, the plot climbs sharply with increasing S_n, beginning $\log(4 + 1),\ \log(14 + 1),\ \log(194 + 1),\ \log(37634 + 1), \ldots$. By S_8, the series values far exceed M_{127} and the remaindering takes effect, keeping the log values steady around 88 … until $n = 126$ when, suddenly, we get $S_{126} \mod M_{127} = 0$, the plot drops to $\log(0 + 1) = 0$, and we discover that M_{127} is prime. This drop never occurs for M_{67} and M_{257} — they were asserted by Mersenne to be prime, but erroneously.

Edouard Lucas (pictured, above left) used this test, although without fully establishing its mathematical credentials, to demonstrate the primality of the 39-digit M_{127}, a colossal achievement for his day. His test was first proved rigorously in 1930 by Derrick H. Lehmer (above right), who initiated the modern study of primality testing.

Web link: John Jaroma's article from www.maths.tcd.ie/pub/ims/bull54/. The image of Lehmer is from *I Have a Photographic Memory* by Paul Halmos, American Mathematical Society, 1987. The image of Lucas is from en.wikipedia.org/wiki/Image:Elucas_1.png.

Further reading: *Prime Numbers: A Computational Perspective, 2nd ed.,* by Richard Crandall and Carl Pomerance, Springer-Verlag, New York, 2005.