THEOREM OF THE DAY

Vaughan Pratt's Theorem *Primality testing is in **NP**.*

Registered Certificate of Primality

Issued by the Primality Certification Board

N	Prime factors of N − 1	c	c^{N-1} mod N = 1	$c^{(N-1)/p}$ mod N ≠ 1, for prime factors p of N − 1
2444789759	2, 1222394879	11	✓	$11^{1222394879} \equiv 2444789758$, $11^2 \equiv 121$
1222394879	2, 611197439	19	✓	$19^{611197439} \equiv 1222394878$, $19^2 \equiv 361$
611197439	2, 305598719	13	✓	$13^{305598719} \equiv 611197438$, $13^2 \equiv 169$
305598719	2, 152799359	37	✓	$37^{152799359} \equiv 305598718$, $37^2 \equiv 1369$
152799359	2, 76399679	11	✓	$11^{76399679} \equiv 152799358$, $11^2 \equiv 121$
76399679	2, 38199839	11	✓	$11^{38199839} \equiv 76399678$, $11^2 \equiv 121$
38199839	2, 19099919	13	✓	$13^{19099919} \equiv 38199838$, $13^2 \equiv 169$
19099919	2, 37, 258107	11	✓	$11^{9549959} \equiv 19099918$, $11^{516214} \equiv 7921368$, $11^{74} \equiv 6206319$
258107	2, 23, 31, 181	2	✓	$2^{129053} \equiv 258106$, $2^{11222} \equiv 67746$, 2^{8326} 71301, $2^{1426} \equiv 57204$

It is hereby confirmed that 2,444,789,759 has been certified prime.

Signed: Date: 1 September, 1975

The **Lucas test** (not to be confused with the Lucas-Lehmer test) says: *an integer $N \geq 2$ is prime if and only if an integer c can be found such that* c^{N-1} mod $N = 1$ *and, for all prime factors p of* $N - 1$, $c^{(N-1)/p}$ mod $N \neq 1$. Then c certifies the primality of N but the prime factors may need certifying in their turn. Here, 2444789759 terminates a so-called *Cunningham chain* of length 8: $N - 1 = 2 \times p$ for a prime p, and this repeats seven times. Nevertheless, eventually small primes factors are reached (say 3-digits or less) which may be certified directly from a dictionary.

NP is the class of those decision (Yes-No) problems for which a Yes-certificate may stated and checked in an amount of time which is a polynomial in the input size. For a candidate prime $N \geq 2$, a *No* is certified by any proper prime factor of N but a Yes seems to require an exhaustive proof that no such factor exists. Pratt showed that certification by repeated Lucas-Lehmer testing could be achieved using no more than about $4 \log N$ bits and checked in no more than about $\log^3 N$ steps.

Web link: maths-people.anu.edu.au/~brent/pd/AdvCom2t.pdf. The Cunningham chain I found at primerecords.dk/.

Further reading: *Algorithms and Complexity, 2nd edition* by Herbert S. Wilf, A K Peters, 2003.