1023-11-483 **Jonathan W Bayless*** (jonathan.bayless@dartmouth.edu), 6188 Kemeny Hall, Hanover, NH 03755. *The Lucas-Pratt primality tree.* Preliminary report.

In 1876, E. Lucas showed that a quick proof of primality for a prime p could be attained through the prime factorization of $p-1$ and a primitive root for p. V. Pratt's proof that PRIMES is in NP, done via Lucas's theorem, showed that a certificate of primality for a prime p could be obtained in $O(\log^2 p)$ modular multiplications with integers at most p. We show that for all constants $C \in \mathbb{R}$, the number of modular multiplications necessary to obtain this certificate is greater than $C \log p$ for a set of primes p with relative asymptotic density 1. (Received September 14, 2006)