1040-11-229 **Vilmar Trevisan*** (trevisan@mat.ufrgs.br), Instituto de Matemática, UFRGS, Porto Alegre, RS 91509900. *Randomized Primality Testing with Chebyshev Polynomials.*

We present a simple randomized primality test that runs in $O(log^3(n))$ time. Let $U_n(x)$ denote the degree-n Chebyshev polynomial of the second kind. Our algorithm is based on the fact that if p is an odd prime, then exactly $\frac{p-1}{2}$ of the numbers $a \in Z_p - \{1, -1\}$, satisfy $U_{\frac{p-1}{2}}(a) \equiv 0 \bmod p$, and the remaining $\frac{p-3}{2}$ numbers satisfy $U_{\frac{p-3}{2}}(a) \equiv 0 \bmod p$. We show that when n is an odd composite, at least half of the members $a \in Z_n$ are witnesses, unless $n = pq$ where p and q are twin primes, in which case there must be at least $\frac{3}{8}n$ witnesses. These ratios are not typical, and in practice the number of witnesses is much higher. In one experiment involving a million consecutive composite numbers, all but two composites were recognized with the first randomly chosen a, the other two requiring only an additional guess. (Received February 25, 2008)