PRIMALITY TESTING IN POLYNOMIAL TIME

(A THEOREM OF M. AGRAWAL, N. KAYAL, AND N. SAXENA)

The Algorithm:

```
Input:  integer n > 1

 1. if ( n is of the form a^b, b > 1 ) output COMPOSITE;
 2. r = 2;
 3. while ( r < n ) {
 4.    if ( gcd(n, r) ≠ 1 ) output COMPOSITE;
 5.    if ( r is prime )
 6.       let q be the largest prime factor of r − 1;
 7.       if ( q ≥ 4√r log n ) and ( n^((r−1)/q) ≢ 1 (mod r) )
 8.          break;
 9.    r → r + 1;
10. }
11. for a = 1 to 2√r log n
12.    if ( (x − a)^n ≢ x^n − a (mod x^r − 1, n) ) output COMPOSITE;
13. output PRIME;
```

Some Notation: $w(x) \pmod{f(x), n} = \texttt{Rem(w(x), f(x), x) mod n}$

$\pi_s(x) = \left|\{p : p \text{ prime} \le x, P(p-1) > p^{2/3}\}\right|$

$I_{g(x)} = \{m : g(x)^m \equiv g(x^m) \pmod{x^r - 1, p}\}$

Lemma 1. There is a constant $c > 0$ and an x_0 such that $\pi_s(x) \ge c\,\dfrac{x}{\log x}$ for all $x \ge x_0$.

Lemma 2. There are positive constants c_1 and c_2 such that the interval $I = (c_1(\log n)^6, c_2(\log n)^6]$ contains a prime r with $r - 1$ having a prime factor q satisfying $q \ge 4\sqrt{r}\log n$ and $q | \text{ord}_r(n)$.

Main Lemma. The set $G = \{(x-1)^{e_1}(x-2)^{e_2}\cdots(x-\ell)^{e_\ell} : e_j \ge 0\}$ forms a subgroup of the multiplicative group of non-zero elements of F (which necessarily is cyclic) of size $> 2^\ell = 2^{2\sqrt{r}\log n} = n^{2\sqrt{r}}$.