The Miller-Rabin Primality Test

**Given:** a positive odd integer \( n \).

**The Miller-Rabin Test:**

Step 0: Write \( n - 1 = 2^\alpha s \), where \( s \) is odd.

Step 1: Choose a random \( b \) with \( 1 < b < n - 1 \) and check that \((b, n) = 1\). [If not, stop: \( n \) is composite.]

Step 2: Compute \( b_0 \equiv b^s \pmod{n} \) and check whether

\[
b_0 \equiv \pm 1 \pmod{n}.
\]

If so, then \( n \) passes the test for this \( b \). (Choose the next \( b \).) Otherwise, go to step 3.

Step 3: Compute successively \( b_1, b_2, \ldots, b_{\alpha-1} \) via

\[
b_k \equiv b_{k-1}^2 \pmod{n}, \quad \text{for } 1 \leq k \leq \alpha - 1.
\]

If

\[
b_k \equiv -1 \pmod{n} \quad \text{for some } k \text{ with } 1 \leq k < \alpha,
\]

then \( n \) passes the test for this \( b \). (Choose next \( b \).)

Otherwise, \( n \) fails the test and hence \( n \) is composite.

**Notes:** 1) If \( n \) passes \( k \) Miller-Rabin tests, then

\[
\text{Prob}(n \text{ is composite}) \leq \frac{1}{4^k}.
\]
2) By using **GRH** (= Generalized Riemann Hypothesis), Adleman, Pomerance, Rumely (1983) and Bach (1985) have shown:

\[ n \text{ composite } \Rightarrow \exists b < 2 \log^2(n) \text{ such that } b \notin \mathcal{S}_n. \]

This leads to a **different primality test**: in place of taking random \( b \)'s, we take successively small numbers \( b = 2, 3, 5, \ldots \) and apply the Miller-Rabin test to those. (We can restrict to prime bases because \( \langle \mathcal{S}_n \rangle \leq \mathcal{E}_n \neq (\mathbb{Z}/n\mathbb{Z})^\times \).

In fact: there are only **13** composite \( n \leq 25 \times 10^9 \) with \( 2, 3, 5 \in \mathcal{S}_n \), and **0** with \( 2, 3, 5, 7, 11, 13 \in \mathcal{S}_n \).

3) Maple’s **isprime(n)** command uses **1** Miller-Rabin test and **1** Lucas Test. According to Maple’s documentation, **no examples** of composite numbers are known which pass Maple’s **isprime** test.