Strong Pseudoprimes and the Miller-Rabin Test

Definition: Let \( n \) be an odd composite number and write \( n - 1 = 2^\alpha s \), with \( s \) odd. If \( \gcd(b, n) = 1 \), then \( n \) called an \textit{strong pseudoprime to the base} \( b \) (\( spsp_b \)) if one of the following conditions holds:

1. \( b^s \equiv 1 \pmod{n} \)
2. \( b^{2^r s} \equiv -1 \pmod{n} \), for some \( r, 0 \leq r < \alpha \).

Miller-Rabin Test: Given an odd integer \( n \), test for a random \( b \) whether condition (1) or (2) holds.

Notation: Let \( S_n \) denote the set of all bases \( b \in (\mathbb{Z}/n\mathbb{Z})^\times \) such that \( b \) satisfies condition (1) or (2) with respect to \( n \), i.e., \( n \) is a \( spsp_b \). Thus:

\[
S_n = \{b \in (\mathbb{Z}/n\mathbb{Z})^\times : n \text{ is an spsp}_b\} \subset (\mathbb{Z}/n\mathbb{Z})^\times.
\]

Theorem 8: (a) If \( n \) is a \( spsp_b \), then \( n \) is an \( Esps_b \). Thus \( S_n \subset E_n \subset P_n \).
(b) If \( n \equiv 3 \pmod{4} \), then \( S_n = E_n \).
(c) If \( n \) is a prime, then \( S_n = (\mathbb{Z}/n\mathbb{Z})^\times \).
(d) If \( n \) is odd and composite, then \( |S_n| \leq \frac{1}{4}(n-1) \).

Remark: In general, \( S_n \) is not a subgroup of \( (\mathbb{Z}/n\mathbb{Z})^\times \).