Euler Pseudoprimes and the Euler Test

Recall: Euler’s Theorem:

\[ n \text{ prime} \Rightarrow b^{\frac{n-1}{2}} \equiv \left( \frac{b}{n} \right) \pmod{n}, \forall b, \gcd(b, n) = 1. \]

Here \( \left( \frac{b}{n} \right) \) denotes the Legendre/Jacobi symbol.

Definition: If \( n \) is an odd composite number (i.e., \( n \) is odd, not prime) and if \( \gcd(b, n) = 1 \), then \( n \) called an Euler pseudoprime to the base \( b \) (\( \text{Epsp}_b \)) if

\[ (1) \quad b^{\frac{n-1}{2}} \equiv \left( \frac{b}{n} \right) \pmod{n}. \]

Euler Test: Given an odd integer \( n \), test for a random \( b \) whether (1) holds, i.e., whether \( n \) is an \( \text{Epsp}_b \).

Note: The name “Euler pseudoprime” is due to D. Shanks (1978).

Notation: Let \( \mathcal{E}_n \) denote the set of all bases \( b \in (\mathbb{Z}/n\mathbb{Z})^\times \) such that \( n \) is an Euler pseudoprime to the base \( b \). Thus:

\[ \mathcal{E}_n = \{ b \in (\mathbb{Z}/n\mathbb{Z})^\times : n \text{ is an } \text{Epsp}_b \} \subset (\mathbb{Z}/n\mathbb{Z})^\times. \]
Theorem 6: (a) If \( n \) is an \( E_{p_{sp_b}} \), then \( n \) is a \( p_{sp_b} \). Thus \( \mathcal{E}_n \subset \mathcal{P}_n \).
(b) \( \mathcal{E}_n \) is a subgroup of \( (\mathbb{Z}/n\mathbb{Z})^\times \).
(c) If \( n \) is odd and composite, then \( \mathcal{E}_n \leq \frac{1}{2} \phi(n) \).

Remark: The proof of part (c) uses:

Theorem 7: Every Carmichael number is square-free.

Test 2 (Solovay-Strassen Primality Test, 1977):
Given: an odd positive integer \( n \)
Method: Repeat the following steps \( k \) times, as long as \( n \) passes each of the steps:
1) Choose an integer \( b \) with \( 1 < b < n \) at random.
2) Check whether \( \gcd(b, n) = 1 \). If false, stop: \( n \) has failed the test. Otherwise, continue with step 3.
3) Compute both sides of (1). If they are equal in \( \mathbb{Z}/n\mathbb{Z} \), then \( n \) has passed the test, otherwise \( n \) has failed the test.

Result: If \( n \) passes \( k \) tests, then
\[
\text{Prob}(n \text{ is composite}) \leq \frac{1}{2^k}.
\]

Note: Each pass of the Euler test takes \( O(\log^3(n)) \) bit operations.