Comparing Primality Tests

Agastya Prabhu

July 2025

Motivation: Primality in Cryptography

- RSA relies on large prime generation for secure keys.
- Primes as big as 2048 bits are needed so efficient primality tests are important.
- Probabilistic vs. Deterministic Tests: probabalistic provide faster runtimes but have error.

Fermat's Little Theorem

If p is prime and $\gcd(a, p) = 1$, then

$$a^{p-1} \equiv 1 \pmod{p}.$$

The Fermat test checks $a^{n-1} \equiv 1 \pmod{n}$ to declare *probably prime*. Carmichael numbers can pass Fermat's test for all a coprime to n.

Deriving Miller–Rabin from Fermat's Theorem

- Fermat's Little Theorem: if n is prime and $\gcd(a, n) = 1$, then

$$a^{n-1} \equiv 1 \pmod{n}.$$

- Write $n - 1 = 2^e d$ with d odd.
- Then

$$a^{n-1} - 1 = a^{2^e d} - 1 = (a^d - 1)(a^d + 1)(a^{2d} + 1) \ldots (a^{2^{e-1} d} + 1).$$

- So if n is prime, then for any a coprime to n:

$$a^d \equiv 1 \pmod{n} \quad \text{or} \quad a^{2^r d} \equiv -1 \pmod{n} \text{ for some } 0 \leq r < e.$$

- Miller–Rabin tests whether one of these congruences holds. If not, n is composite.
- We keep picking a at random to retest the same number

Miller–Rabin: Witnesses and Nonwitnesses

Composite $n = 9$: $9 - 1 = 8 = 2^3 \cdot 1$.

- $a = 8$:

$$8^1 \bmod 9 = 8 \equiv -1 \pmod 9$$

  passes immediately *non-witness*.

- $a = 2$:

$$2^1 \bmod 9 = 2, \quad 2^2 \bmod 9 = 4, \quad 2^4 \bmod 9 = 7 \neq -1$$

  no ± 1 ever appears composite detected *witness*.

Prime $n = 7$: pick $a = 3$,

$$3^3 \bmod 7 = 27 \bmod 7 = 6 \equiv -1,$$

so always passes for any valid a.

Proof: Error Bound for Prime Powers

Theorem: Let $n = p^x$ for an odd prime p and $x \geq 2$. Then the error bound is at most $\frac{1}{4}$ because at most $\frac{1}{4}$ of the numbers are nonwitnesses. **Proof Outline:**

- By Theorem: nonwitnesses a must be coprime to n and satisfy $a^{n-1} \equiv 1 \pmod{n}$ and $a^{\varphi(n)} \equiv 1 \pmod{n}$.
- $(n-1, \varphi(n)) = (p^x - 1, p^{x-1}(p-1)) = p - 1$.
- So all nonwitnesses satisfy $a^{p-1} \equiv 1 \pmod{n}$.
- Inductively construct exactly $p - 1$ such a mod p^x by lifting from mod p^{x-1} and use binomial expansion:

  $$(\mathrm{a} + \mathrm{cp}^x)^{p-1} \equiv a^{p-1} + (p-1)a^{p-2}cp^x \pmod{p^{x+1}}.$$
- Solve for c uniquely $\Rightarrow$ only $p - 1$ nonwitnesses for all x.

Proof: MR Error Bound for Non-Carmichael Numbers

Theorem: If n is an odd composite and not a Carmichael number, then the error bound is at most $\frac{1}{4}$ because at most $\frac{1}{4}$ of the numbers are nonwitnesses.

Outline:

- $F_n = \{1 \leq a \leq n-1 : (a, n) = 1\}$
- $G_n = \{1 \leq a \leq n-1 : a^{n-1} \equiv 1 \pmod{n}\}$
- $H_n = \{1 \leq a \leq n-1 : a^{2^{r_0} d} \equiv \pm 1 \pmod{n}\}$. r_0 is the largest $r \in \{0, 1, ..., e-1\}$ such that for some a_0, $a_0^{2^{r_0}} \equiv -1 \pmod{}$
- Since n is not Carmichael, G_n is a proper .subgroup of F_n.
- Use Lagrange's theorem: $|G_n| \leq \frac{|F_n|}{2}$.
- Also, H_n is a proper subgroup of G_n because there exists a such that $a^{n-1} \equiv 1$ but $a^{2^r d} \not\equiv \pm 1$.
- Then $|H_n| \leq \frac{|G_n|}{2} \leq \frac{|F_n|}{4}$.

Therefore, the fraction of nonwitnesses is at most $\frac{1}{4}$.

Solovay–Strassen Test and Jacobi Symbol

Solovay–Strassen Test: Let n be odd and a such that $\gcd(a, n) = 1$. Then n passes the test if:

$$a^{(n-1)/2} \equiv \left(\frac{a}{n}\right) \pmod{n}.$$

Otherwise, a is a **witness** and n is composite.
Jacobi Symbol: For odd $n = p_1^{e_1} \cdots p_k^{e_k}$, define:

$$\left(\frac{a}{n}\right) = \prod_{i=1}^{k} \left(\frac{a}{p_i}\right)^{e_i},$$

where each $\left(\frac{a}{p_i}\right)$ is the Legendre symbol. If $x^2 = a$ for some integer x, $(\frac{a}{p_i}) = 1$. Otherwise $(\frac{a}{p_i}) = -1$

Solovay–Strassen: Witnesses and Nonwitnesses

Composite $n = 14$:

- $a = 9$:

$$\left(\frac{9}{14}\right) = 1, \quad 9^6 \bmod 14 = 1$$

  test passes *non-witness*.

- $a = 11$:

$$\left(\frac{11}{14}\right) = -1, \quad 11^6 \bmod 14 = 13 \neq -1$$

  test fails composite detected *witness*.

Prime $n = 7$: pick $a = 3$,

$$\left(\frac{3}{7}\right) = -1, \quad 3^3 \bmod 7 = 6 \equiv -1$$

test passes for all valid bases.

Error Bound of Solovay–Strassen Test

Theorem: For odd composite n, at most half of the integers coprime to n pass the test. Error $\leq \frac{1}{2}$.

Sets:

$$F = \{a : \gcd(a, n) = 1,\ a^{(n-1)/2} \equiv \left(\frac{a}{n}\right) \bmod n\}$$

$$G = \{a : \gcd(a, n) = 1,\ a^{(n-1)/2} \not\equiv \left(\frac{a}{n}\right) \bmod n\}$$

$$H = \{a : \gcd(a, n) > 1\}$$

Construction: Pick any $a_0 \in G$. Define:

$$G_0 = \{ba_0 \bmod n : b \in F\}$$

Then $G_0 \subseteq G$ since multiplication by a_0 preserves failure of the test.

$\Rightarrow |G| \geq |G_0| = |F| \Rightarrow$ fraction of nonwitnesses:

$$\frac{|F|}{|F| + |G| + |H|} \leq \frac{|F|}{2|F| + 1} < \frac{1}{2}$$

Runtime: Miller–Rabin

Main cost: Modular exponentiation.

- First, write $n - 1 = 2^e d$ — takes at most $O(\log n)$ divisions.
- Compute $a^d \bmod n$ using **binary exponentiation**:
  - d has $O(\log n)$ bits.
  - Each modular multiplication takes $O(\log^2 n)$ time.
  - Total time: $O(\log^3 n)$.
- continuously square to compute $a^{2^e d} \bmod n$.
- Total cost $O(\log^3 n)$

Runtime: Solovay–Strassen

Two main computations per test round:

- Compute $a^{(n-1)/2} \bmod n$ using **binary exponentiation**:
  - Like Miller–Rabin, this costs $O(\log^3 n)$.
- Compute the **Jacobi symbol** $\left(\frac{a}{n}\right)$:
  - Based on quadratic reciprocity and reductions.
  - Runs in $O(\log^2 n)$ time.

Conclusion: Total cost per iteration is still $O(\log^3 n)$.

Comparison and Conclusion

- Both tests $O(\log^3 n)$, MR has smaller error per round (4^{-k} vs 2^{-k}).
- MR more accurate than SS and faster than AKS for large primes (AKS's runtime is $\log^6 n$).
- MR is standard in cryptographic libraries for prime generation.