# Miller Rabin in Comparison to Other Primality Tests

Agastya Prabhu

June 2025

## 1 Abstract

Over the course of this paper we primarily used group and number theory to examine error bounds while also using theoretical computer science to examine running time. We confirm why Miller-Rabin is the dominant primality test in the industry and we go through extensive proofs to prove its greater efficiency. We found that the Miller-Rabin error bound is 25% while the Solovay-Strassen test's error bound is 50%. Also we proved that the runtime for both the probabilistic tests were $O(\log^3 n)$ which is significantly faster than the mark established by the fastest deterministic test, AKS.

## 2 Introduction

The Rivest-Shamir-Adleman algorithm (RSA) is one of the primary methods to create secure communication and encrypt data, especially over the internet. Considering how internet use has exploded over the last few decades to billions of users, it is essential to have an extremely efficient cryptographic algorithm to save time and money. RSA relies on the difficulty of factoring extremely large semi-prime numbers which are part of the public key while the two prime factors remain private. These primes are extremely large, being 1024-bit or even 2048-bit numbers, to ensure safety. As a result, one of the best ways to improve the RSA's efficiency is to have a highly efficient primality test. The focus of this paper is analyzing different primality tests to show which one is the most efficient.

We will mainly focus on probabilistic tests over deterministic, where probabilistic tests have a certain degree of error while deterministic tests are always right when labeling a number prime or composite. First we will find the error bound of the major probabilistic tests, Miller-Rabin and Solovay-Strassen, then we will compare their runtimes along with bringing in runtime from deterministic test AKS to show why probabilistic tests are more efficient. Based on the error bound and runtime findings, I concluded that the Miller-Rabin test

is the most efficient and should be used in RSA key generation. In this paper I prove that the error bound is 25% for the Miller-Rabin test and 50% for the Solovay-Strassen test and that the runtime is $O(\log^3 n)$ for both of them.

# 3 What is the Miller-Rabin test?

According to Fermat's Little Theorem, for prime $n$ and integer $a$ not divisible by $n$, the following holds true:

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

This is the first primality test in history called the Fermat's Test where we can pick a random $a$ and see if $n$ passes the test. The problem with this is that there are actually Carmichael numbers such that no matter what $a$ is picked, as long as $(a, n) = 1$, $n$ always passes the test. The problem with this is that the error bound is 100% for certain numbers. The error bound for non-carmichael numbers in the Fermat test is 50% which we will prove as part of the Miller-Rabin error bound proof.

The Miller-Rabin test is actually derived from this Fermat test. We can express $n-1$ in the form $2^e d$ where $e$ is a positive integer and d is an odd integer. This lets us construct the following equation:

$$a^{2^e d} - 1 \equiv 0 \pmod{n}$$

which becomes

$$(a^{2^{e-1} d} + 1)(a^{2^{e-1} d} - 1) \equiv 0 \pmod{n}$$

which eventually becomes

$$(a^d - 1)(a^d + 1)(a^{2d} + 1)(a^{2^2 d} + 1)...(a^{2^{e-1} d} + 1) \equiv 0 \pmod{n}.$$

We can see in this altered equation how we get the Miller-Rabin test. We first check if $a^d \equiv 1 \pmod{n}$ and then we check if $a^d \equiv -1 \pmod{p}$ and repeatedly square the result until we are checking for $a^{2^{e-1} d} \equiv -1 \pmod{n}$. This is because we are basically checking each factor of the equation and if anyone of them are 0 the entire equation is 0. If any one of these holds true then the original equation from Fermat's Little Theorem must hold true and all primes must pass this test. Essentially the Miller-Rabin test is saying that if an integer $n$ is prime then

for $a \in \{1, 2, ..., n-1\}$ either $a^d \equiv 1 \pmod{n}$ or $a^{2^y d} \equiv -1 \pmod{n}$ for some $y \in \{1, 2, ..., e-1\}$. It is important to note that we only check for certain $a$ because of the restriction on Fermat's Little Theorem that $p$ must not divide $a$.

Let us define the $a$ that do not pass the test for odd composite $n$ as witnesses. We can then define the $a$ that pass the test for an odd, composite $n$ as nonwitnesses (since $a$ doesn't witness $n$'s compositeness). To prove our error bound of

25% we are trying to prove that the number of nonwitnesses in between 1 and $n-1$ is at most $\frac{n-1}{4}$.

**Example**:

Composite numbers can have nonwitnesses and witnesses. Let us have composite number 121. So $n-1 = 120 = 2^3 \cdot 15$. Take base $a = 81$, which is coprime to 121. Computing:

$$81^{15} \bmod 121 = 1,$$

we see that it satisfies the Miller-Rabin condition for a nonwitness. Therefore, $a = 81$ is a nonwitness for $n = 121$. All the nonwitnesses for 121 are $1, 3, 9, 27, 40, 81, 94, 112, 118, 120$. In practice we usually only pick $a \in (2, 3, ..., n-2)$ because 1 and $n-1$ are always non-witnesses.

**Theorem 3.1** *The set of all Miller-Rabin nonwitnesses for composite n is not always multiplicative.*

Proof: First notice how the set of Fermat nonwitnesses are multiplicative. Let us have set $A = \{1 \leq a \leq n-1 : a^{n-1} \equiv 1 \pmod{n}\}$. Let $b = a_0 a_1$ where $a_i \in A$. $b^{n-1} \equiv 1 \pmod{n}$ because $(a_0 a_1)^{n-1} = a_0^{n-1} a_1^{n-1} \equiv 1 \pmod{n}$.

Now take composite integer $1037 = 17 \cdot 61$. The set of all nonwitness for 1037 is $\{1, 72, 438, 599, 965, 1036\}$. Now notice $72 \cdot 438 \equiv 426 \pmod{1027}$ and 426 is not in the set. Therefore, the set of Miller-Rabin nonwitnesses is not always closed under multiplication.

This sets up implications for our proof later on because to use group theory to prove the error bound the group must be closed. So we must actually create a group that contains all the Miller-Rabin nonwitnesses but is as small as possible and is closed.

# 4 The Miller-Rabin Error Bound is 25%

**Theorem 4.1** *Let a be a nonwitness for odd composite n. a must be coprime to n.*

Proof: Let us define $a$ as a nonwitness for $n$. That means, as described in Section 3, that $a^{n-1} \equiv 1 \pmod{n}$ must also be true. This means that $a^{n-1} + bn = 1$ for some integer $b$. This is equivalent to $ca + bn = 1$ for some integer $c = a^{n-2}$. By Bézout's Identity, $ca + bn = 1$ must be a multiple of $(a, n)$; therefore, $(a, n) = 1$ must be true if $a$ is a nonwitness for $n$.

**Theorem 4.2** *For any integer a, if $a^x \equiv 1 \pmod{z}$ and $a^y \equiv 1 \pmod{z}$ then $a^{(x,y)} \equiv 1 \pmod{z}$.*

Proof: Let us say $b = (x, y)$. By Bézout's Identity, for some integer $c$ and $d$, $cx + dy = b$. From $a^{(x,y)} \equiv 1 \pmod{z}$ we then get $a^{cx+dy} \equiv 1 \pmod{z}$ which becomes $a^{cx}a^{dy} \equiv 1 \pmod{z}$ which is true.

**Theorem 4.3** *For $n = p^x$ where $x \geq 2$ and $p$ is an odd prime, the error bound is 25%.*

Proof: To prove this we will start by using 4.1 because the fact that all nonwitnesses $a$ are coprime with $n$ tells us that all nonwitnesses satisfy Euler's Theorem: $a^{\phi n} \equiv 1 \pmod{n}$.

Additionally all nonwitnesses $a$ must satisfy Fermat's Little Theorem: $a^{n-1} \equiv 1 \pmod{n}$. Using this information, we want to prove that any nonwitness $a$ for $n$ when $n$ is a prime power satisfies $a^{p-1} \equiv 1 \pmod{n}$.

We can start by finding $(n-1, \phi n) = (p^x - 1, p^{x-1}(p-1))$. Since $p^x - 1$ isn't divisible by $p$, we get $(p^x - 1, p^{x-1}(p-1)) = (p^x - 1, p - 1) = p - 1$. By what we found in 4.2 we now know that for any nonwitness $a$ where n is a prime power, $a^{p-1} \equiv 1 \pmod{n}$.

To finish this proof we will prove that for any $x \geq 1$ the number of nonwitnesses is at most $p - 1$ for any $n = p^x$. We can use induction to do this. At $x = 1$, since $n$ is prime, there is clearly $p-1$ nonwitnesses. Let us have a witness $a$ such that $a^{p-1} \equiv 1 \pmod{p^x}$. We want to show that there is a unique $a'$ such that $a'^{p-1} \equiv 1 \pmod{p^{x+1}}$ and $a' \equiv a \pmod{p^x}$. We are doing this because we are trying to ensure that this is completely unique and there is essentially one $a'$ for every $a$. We can then notice that $a'$ can also be expressed as $a' \equiv a + cp^x \pmod{p^{x+1}}$ where $c$ is an integer. If we plug this in to our first equation we get $(a + cp^x)^{p-1} \equiv 1 \pmod{p^{x+1}}$ and now we have to prove that there is a unique $c$ that satisfies this for each $a$. Using Binomial Theorem we can get

$$(a + cp^x)^{p-1} \equiv a^{p-1} + (p-1)a^{p-2}cp^x \pmod{p^{x+1}}.$$

This is true because the higher order terms get reduced because $a^{xy} \equiv 0 \pmod{p^{x+1}}$ for $y \geq 2$. We can notice that $a = 1 + bp^x$ for some integer b and plug that into the equation:

$$\begin{aligned}
(1 + p^x b) + (p-1)a^{p-2}cp^x &\equiv 1 \pmod{p^{x+1}} \\
p^x b + (p-1)a^{p-2}cp^x &\equiv 0 \pmod{p^{x+1}} \\
p^x \left(b + (p-1)a^{p-2}c\right) &\equiv 0 \pmod{p^{x+1}} \\
b + (p-1)a^{p-2}c &\equiv 0 \pmod{p} \\
b - a^{p-2}c &\equiv 0 \pmod{p}
\end{aligned}$$

Therefore, there is a unique $c$ that satisfies this; therefore, there is always $p-1$ nonwitnesses for prime power $n$. If $n$ is a prime power $p^x$, that means the error bound is $\frac{p-1}{p^x-1}$ and since $x \geq 2$ and the smallest $p$ is 3, we get $\frac{3-1}{3^2-1} = \frac{1}{4}$. Therefore we have proved that the error bound for prime powers is 25%.

**Theorem 4.4** *The error bound for a composite, non-Carmichael number n with at least 2 distinct prime factors, is 25%.*

Proof: For this proof let $n$ be a composite, non-Carmichael number and is not a power of a prime power. The proof of this theorem hinges on Lagrange's Theorem that states if $H$ is a proper subgroup of $G$, $|H|$ divides $|G|$. We can make 3 groups to prove the error bound.

$$F_n = \{1 \leq a \leq n-1 : (a,n) = 1\}$$
$$G_n = \{1 \leq a \leq n-1 : a^{n-1} \equiv 1 \pmod{n}\}$$
$$H_n = \{1 \leq a \leq n-1 : a^{2^{y_0}d} \equiv \pm 1 \pmod{n}\}$$

In $H_n$, $y_0$ is the largest $y \in \{0, 1, ..., e-1\}$ such that some $a_0$ coprime to $n$ satisfies $a_0^{2^{y_0}} \equiv -1 \pmod{n}$ We constructed this group because we know that from 3.1, the set of Miller-Rabin nonwitnesses isn't always multiplicative. Constructing this group that is as close to the Miller-Rabin nonwitnesses as possible but is also closed by multiplication allows us to use Lagrange's Theorem.

First, we will prove that $G_n$ is a proper subgroup of $F_n$. Since all $a$ in $G_n$ must be coprime to $n$ as shown in 4.1, $F_n \supset G_n$. We also know that $F_n \neq G_n$ because $n$ is not a Carmichael number so there is at least one $a$ in $F_n$ that is not in $G_n$. $G$ is closed under multiplication: if $a^{n-1} \equiv 1 \pmod{n}$ and $b^{n-1} \equiv 1 \pmod{n}$, $(ab)^{n-1} \equiv 1 \pmod{n}$. $G$ also contains the inverse of every element: $(a^{-1})^{n-1} \equiv (a^{n-1})^{-1} \equiv 1^{-1} \equiv 1 \pmod{n} \Rightarrow a^{-1} \in G$. Therefore by Lagrange's Theorem $|G_n|$ is at most $\frac{1}{2}$ of $|F_n|$. This is exactly what I described in section 3 and proves that the error bound for non-Carmichael numbers in the Fermat test is 50% because the amount of Fermat witnesses is less than $\frac{1}{2}$ of the possible $a$.

Before proving that $H_n$ is a subgroup of $G_n$, we will prove that $H_n$ contains all Miller-Rabin nonwitnesses for $n$. Miller-Rabin nonwitnesses, $a$, all fit these two categories: $a^d \equiv 1 \pmod{n}$ and $a^{2^y d} \equiv -1 \pmod{n}$ for some $y \in e-1$. If $a^d \equiv 1 \pmod{n}$ is true, then $a^{2^{y_0}d} \equiv \pm 1 \pmod{n}$ must be true. If $a^{2^y d} \equiv -1 \pmod{n}$ for some $y \in \{0, 1, ..., e-1\}$, then $a^{2^{y_0}d} \equiv \pm 1 \pmod{n}$ must also be true because $y_0 \geq y$. To ensure this we can make $a^d = b$, then $b^{2^y} \equiv -1 \pmod{n}$, but since $y_0$ is the largest possible $y$ that makes this possible, $y \leq y_0$ must be true.

Now we also have to prove that this set is contained in $G_n$. Crucially, we must recognize that $y_0 \leq e-1$ and all elements in $G_n$ follow the form $a^{n-1} = a^{2^e d} \equiv 1 \pmod{n}$, which means that if an element is in $H_n$ it must also be in $G_n$.

It is clear $H_n$ is closed by multiplication and contains its inverses. If $a^{2^{y_0}d} \equiv \pm 1 \pmod{n}$ and $b^{2^{y_0}d} \equiv \pm 1 \pmod{n}$ then $(ab)^{2^{y_0}d} \equiv \pm 1 \pmod{n}$ and $(a^{-1})^{2^{y_0}d} \equiv \pm 1 \pmod{n}$.

Lastly, we have to prove that $G_n \neq H_n$. Let us have an integer $b \in H_n$.

Since $n$ is not a prime power it can be expressed in the form $p^x m$ where $p$ is a prime factor of $n$ and $m$ is not divisible by $p$ and both are odd. We know $a_0^{2^{y_0}d} \equiv -1 \pmod{n}$. By the Chinese Remainder Theorem there exists some integer $c \in \{1, 2, ..., n-1\}$ such that $c \equiv a_0 \pmod{p^x}$ and $c \equiv 1 \pmod{m}$. We also know that $(c, n) = 1$ because $(a_0, n) = 1$. We get

$$c^{2^{y_0}d} \equiv a_0^{2^{y_0}d} \equiv (-1)^d \equiv -1 \pmod{p^x} \Rightarrow c^{2^{y_0}d} \not\equiv 1 \pmod{n}$$

since $p^x$ divides $n$. We also get

$$c^{2^{y_0}d} \equiv 1 \pmod{m} \Rightarrow c^{2^{y_0}d} \not\equiv -1 \pmod{n}.$$

Since $c^{2^{y_0}d} \neq \pm 1 \pmod{n}$, $c$ is not in $H_n$. But considering $c^{2^{y_0}d} \equiv -1 \pmod{p^x}$ and $c^{2^{y_0}d} \equiv 1 \pmod{m}$, we get $c^{2^{y_0+1}d} \equiv 1 \pmod{n}$ so $c^{n-1} \equiv 1 \pmod{n}$. Therefore, $c$ is in $G_n$ but not in $H_n$, so by Lagrange's Theorem, $|H_n|$ is at most $\frac{1}{2}$ of $|G_n|$. Therefore we get

$$\frac{|G_n|}{|F_n|}\frac{|H_n|}{|G_n|} \leq \frac{1}{4}$$

and since $F_n$ is a subset of all positive integers less than $n$, the error bound of all non-Carmichael numbers must be at most 25%.

While I only proved the error bound for non-Carmichael numbers, it still holds true for Carmichael numbers as well according to Keith Conrad and Bobby Kleinburg [Con11, Sta10]. One of the reasons the Miller-Rabin primality test is so widely used is because it has the lowest proven error bound of any probabilistic test. We will now prove that the Solovay-Strassen error bound is at most 50%. The next section will still use group theory but is more elementary.

# 5 Solovay-Strassen Test and Error Bound

Euler's Criterion states that for odd prime $p$ and integer $a$ such that $\gcd(a, p) = 1$. Then:

$$a^{\frac{p-1}{2}} \equiv \begin{cases} 1 \pmod{p} & \text{if there exists an integer } x \text{ such that } x^2 \equiv a \pmod{p}, \\ -1 \pmod{p} & \text{if no such integer exists.} \end{cases}$$

The Legendre symbol is used to simplify notation and is written as $(\frac{a}{n})$ where $(\frac{a}{n}) = -1$ if $a$ cannot be expressed as a square of another number modulo $n$ or 1 if it can. In this $n$ must be prime. Additionally the Legendre Symbol is equal to 0 if $n$ divides $a$ in $(\frac{a}{n})$. The Jacobi Symbol, which is used in the actual Solovay-Strassen test, is a generalization of the Legendre Symbol, in which it can be applied to all odd numbers, even if it is composite. It functions by separating a composite $n$ into its prime factors and multiplying the Legendre symbols for each one. For example, $(\frac{a}{15})$ would become $(\frac{a}{3})(\frac{a}{5})$.

Essentially this is the Solovay-Strassen Test: let $n$ be an odd integer greater than 2, and let $a$ be an integer such that $1 < a < n$ and $\gcd(a, n) = 1$.

$$\text{Check whether} \quad a^{\frac{n-1}{2}} \equiv \left(\frac{a}{n}\right) \pmod{n}$$

Here, $\left(\frac{a}{n}\right)$ is the Jacobi symbol. If the congruence does not hold, then $n$ is composite. If it does hold, $n$ passes the Solovay–Strassen test for base $a$ and is a probable prime.

**Theorem 5.1** *If* $(a, n) > 1$ *then* $(\frac{a}{n}) = 0$.

Let us have integer $a$ and odd composite $n$ such that $(a, n) > 1$. This Jacobi symbol, $(\frac{a}{n})$, becomes represented by the multiplication of Legendre symbols. $(\frac{a}{p_1})(\frac{a}{p_2})...(\frac{a}{p_i})$ where $i \geq 2$. Since $(a, n) > 1$, $a$ must be divisible by at least one of $n$'s prime factors and as I noted earlier, $(\frac{a}{p}) = 0$ when $p$ divides $a$. Therefore $(\frac{a}{n}) = 0$.

**Theorem 5.2** *There exists a number* $a$ *such that* $1 \leq a \leq n-1 : \gcd(a, n) = 1$ *and* $a^{\frac{n-1}{2}} \not\equiv \left(\frac{a}{n}\right) \pmod{n}$.

This is essentially proving that witnesses for the Solovay-Strassen test exist. For this proof we will have two cases: $n$ is square-free, and $n$ has a repeated prime factor.

Let us say $n$ is square-free and can be expressed in the form $n = p_1 p_2 ... p_i$ where $p$ is prime and $i \geq 2$. Let us have an integer $b$ such that $(\frac{b}{n}) = -1$. By the Chinese Remainder Theorem there exists an integer $a$ where $1 \leq a \leq n-1$ such that $a \equiv b \pmod{p_1}$ and $a \equiv 1 \pmod{(p_2 ... p_i)}$. Since $a$ is coprime to $p_1$ and $p_2 ... p_i$, $(a, n) = 1$. We know that $(\frac{a}{p_j})$ for any $2 \leq j \leq i$ since 1 is always a quadratic residue and $a \equiv 1 \pmod{p_j}$. That tells us that $(\frac{a}{n}) = -1$. If $a$ is a nonwitness $a^{(n-1)/2} \equiv (\frac{a}{n}) \pmod{n}$, which tells us $a^{(n-1)/2} \equiv -1 \pmod{n}$. For this to be true, $a \equiv -1 \pmod{p_2}$, which is not true because of $a$'s definition. Therefore $a$ is a witness and there exists at least one witness for a square-free $n$.

The other case is that $n$ is not square-free and can be expressed in some form $n = p^x m$ where $p$ is an odd prime and $m$ is an odd integer. By the Chinese Remainder Theorem there exists an integer $a$ where $1 \leq a \leq n-1$ such that

$$a \equiv p + 1 \pmod{p^2} \quad \text{and} \quad a \equiv 1 \pmod{m}.$$

First of all $(a, n) = 1$ because $(a, m) = 1$ and $(a, p) = 1$. Let us say that $a$ is a nonwitness and $a^{\frac{n-1}{2}} \equiv (\frac{a}{n}) \pmod{n}$. Therefore $a^{n-1} \equiv 1 \pmod{n}$ by squaring both sides. This means $a^{n-1} \equiv 1 \pmod{p^2}$ substituting with $a \equiv p+1 \pmod{p^x}$ we get $(p+1)^{n-1} \equiv 1 \pmod{p^2}$. By binomial theorem $(p+1)^{n-1} \equiv 1 + p(n-1) \pmod{p^2}$. Therefore $1 + p(n-1) \equiv 1 \pmod{p^2}$ or $n - 1 \equiv 0 \pmod{p^2}$ which

is false because $n$ is a multiple of $p^2$. Therefore we have a contradiction and $a^{\frac{n-1}{2}} \not\equiv (\frac{a}{n}) \pmod{n}$.

Ultimately there is at least one $a$ such that $1 \leq a \leq n-1 : \gcd(a,n) = 1$ and $a^{\frac{n-1}{2}} \not\equiv \left(\frac{a}{n}\right) \pmod{n}$ which means there is at least one witness. We will use the fact that there exists a witness for composite $n$ in the next proof to show that there are at least the same number of witnesses as nonwitnesses.

**Theorem 5.3** *The error bound of the Solovay-Strassen test for an odd composite $n$ is at most 50%.*

Now we can get into proving the error bound. Let us say we have an odd composite number $n$. Similar to the Miller-Rabin proof, we will have witnesses and nonwitnesses, where witnesses are the bases that let $n$ fail the test, while the nonwitnesses let $n$ pass the test. We will have three subsets of positive integers less than $n$: one that contains all the nonwitnesses, one that contains all the witnesses, and one that contains all numbers not coprime to $n$.

$$F = \left\{1 \leq a \leq n-1 : \gcd(a,n) = 1 \text{ and } a^{\frac{n-1}{2}} \equiv \left(\frac{a}{n}\right) \pmod{n}\right\},$$
$$G = \left\{1 \leq a \leq n-1 : \gcd(a,n) = 1 \text{ and } a^{\frac{n-1}{2}} \not\equiv \left(\frac{a}{n}\right) \pmod{n}\right\},$$
$$H = \{1 \leq a \leq n-1 : \gcd(a,n) > 1\}$$

Because of 5.2 we know that $G$ isn't empty. Also because of 5.1 we know that $H$ exists and is separate from $F$ and $G$. Let us construct a set $G_0$ such that for all $b \in F$ and specific $a_0 \in G$, $ba_0 \pmod{n} \in G_0$. We will now prove that every element in $G_0$ is in $G$. First of all $(ba_0, n) = 1$ because $a_0$ and any $b$ is coprime with $n$. We can do this by checking if $(ba_0)^{\frac{n-1}{2}} \not\equiv (\frac{ba_0}{n}) \pmod{n}$. We then get

$$(ba_0)^{\frac{n-1}{2}} \equiv b^{\frac{n-1}{2}} a_0^{\frac{n-1}{2}} \equiv \left(\frac{b}{n}\right) a_0^{\frac{n-1}{2}} \pmod{n}.$$

Let us say $ba_0 \in F$, then $(ba_0)^{\frac{n-1}{2}} \equiv (\frac{ba_0}{n}) = (\frac{b}{n})(\frac{a_0}{n}) \pmod{n}$. Therefore $(\frac{b}{n})a_0^{\frac{n-1}{2}} \equiv (\frac{b}{n})(\frac{a_0}{n}) \pmod{n}$ so, $a_0^{\frac{n-1}{2}} \equiv (\frac{a_0}{n}) \pmod{n}$ which is not true by definition. Therefore $ba_0 \in G$ and $G_0 \in G$. Since $|G_0| = |F|$, $|G| \geq |F|$. Additionally, note that $|H| \geq 1$ since $n$ is composite. We now have

$$\frac{|F|}{n-1} = \frac{|F|}{|F|+|G|+|H|} \leq \frac{|F|}{|F|+|G|+1} \leq \frac{|F|}{2|F|+1} < \frac{1}{2}.$$

. $F$ is a set of all the nonwitnesses and is less than half of all numbers, the error bound for any odd, composite $n$ is at most 50%.

This illustrates why the Miller-Rabin test has largely been used instead of the Solovay-Strassen test since its lower error bound means the test has to have fewer iterations. Over the next section we will compare the run times of the tests to show why Miller-Rabin is the best test: it has the same runtime with a low error.

# 6 Runtime

Runtime might be the most important aspect concerning the efficiency of a primality test. While being less of a number theory concept, like what was covered earlier in the paper, and more of a computer science concept, it is nonetheless important to understand it because it is actually servers executing these tests. Runtime consists of generalizing the amount of computations required to do an action in relation to the input. For example, $O(\log^3 n)$, the runtime we will prove for the Miller-Rabin test requires roughly $\log^3 n$ for any odd $n$.

**Theorem 6.1** *The runtime of the Miller-Rabin test is $O(\log^3 n)$ where $n$ is odd and $n > 2$.*

Proof: Going back to Section 3, we can see the actual process of the Miller-Rabin test.

$$\text{Given odd } n > 2, \text{ write } n - 1 = 2^e d \text{ with } d \text{ odd}$$

$$\text{Choose } 1 < a < n - 1, \text{ and compute } a^d \mod n$$

$$\text{If } a^d \equiv 1 \pmod{n}, \text{ then } n \text{ passes}$$

$$\text{Otherwise, for } x = 0 \text{ to } e - 1, \text{ check if } a^{2^x d} \equiv -1 \pmod{n}$$

$$\text{If none hold, then } n \text{ is composite}$$

$$\text{If any hold, then } n \text{ passes the test for base } a.$$

Looking at the first part of the test we have to express $n - 1$ in some form $2^e d$, this takes at most $\log_2 n$ calculations because that's the most times $n$ could possibly be divided by 2. This becomes $O(\log n)$.

For the second step, we have to recognize how computers actually do modular exponentiation. We will start with $a^d$ to analyze this. To compute $a^d \mod n$ efficiently, we use binary exponentiation.

We write the exponent $d$ in binary:

$$d = (d_k d_{k-1} \dots d_1 d_0)_2$$

Where each $d_i$ is a digit.

We initialize:

$$\text{result} \leftarrow 1, \quad \text{current\_power} \leftarrow a$$

For each bit $d_i$, starting from the smallest bit:

- If $d_i = 1$, then:

$$\text{result} \leftarrow (\text{result} \cdot \text{current\_power}) \pmod{n}$$

- Regardless of the bit, square the current power:

$$\text{current\_power} \leftarrow (\text{current\_power} \cdot \text{current\_power}) \pmod{n}$$

After processing all bits, the final value of result is $a^d \mod n$.

First notice how there is $\log_2 n$ bits in $d$. This means that there is a maximum of $\log_2 n$ times it multiplies the result and the current power to get the new result and the same to square the current power. Multiplication takes $O(\log^2 n)$ runtime because if $n$ has $b$ bits, it takes $O(b^2)$ computations. If a bit in $d$ is 1, we will have to do 2 multiplications for that bit but we can erase that coefficient due to big O notation. Additionally, since addition and subtraction take $O(1)$ runtime, they are negligible. Since there are $\log_2 n$ bits, and $O(\log^2 n)$ runtime per bit, the runtime of this step is $O(\log^3 n)$. What the computer does after calculating $a^d \pmod n$ is it squares that repeatedly to get each $a^{2^x d} \pmod n$. Since there are at most $\log_2 n$ times needed to square, and squaring takes $O(\log^2 n)$ runtime, the runtime for this step is $O(\log^3 n)$. Examining these three steps we get $O(\log n) + O(\log^3 n) + O(\log^3 n) = O(\log^3 n)$. Therefore the runtime for each iteration of the Miller-Rabin test is $O(\log^3 n)$.

**Theorem 6.2** *The runtime of the Solovay-Strassen test is $O(\log^3 n)$ where $n$ is odd and $n > 2$.*

Proof: First, let's write out how the computer executes the Solovay-Strassen test. It just calculates if $a^{\frac{n-1}{2}} \equiv (\frac{a}{n})$. First, we will focus on the left side of the equation. From our findings in 6.1, the runtime for modular exponentiation is $O(\log^3 n)$ for the Solovay-Strassen test since $\frac{n-1}{2} < n$. Therefore the runtime of the Solovay-Strassen test is at least $O(\log^3 n)$.

Now we can move on to the right side of the equation which is calculating the Jacobi symbol. The way computers are able to calculate the Jacobi and Legendre symbols is by mainly 3 rules. It can use quadratic reciprocity to flip the numerator and denominator, and it can reduce the numerator modulo the denominator.

Multiplicativity: $(\frac{ab}{n}) = (\frac{a}{n})(\frac{b}{n})$

Quadratic Reciprocity: $\left(\frac{a}{n}\right)\left(\frac{n}{a}\right) = (-1)^{\frac{a-1}{2}\frac{n-1}{2}}$ which becomes $\left(\frac{n}{a}\right) = \left(\frac{a}{n}\right)(-1)^{\frac{a-1}{2}\frac{n-1}{2}}$ since $(\frac{a}{n}) = \pm 1$.

Reducing by the modulus of the denominator: $(\frac{a}{n}) = (\frac{a \pmod n}{n})$

Multiplicativity is used for separating 2 out of the numerator since only then can quadratic reciprocity be used so the runtime for that action is $O(1)$. Also notice that quadratic reciprocity can be calculated in this fashion:

$$(-1)^{\frac{(a-1)(n-1)}{4}} = \begin{cases} -1 & \text{if } a \equiv n \equiv 3 \pmod 4 \\ +1 & \text{otherwise} \end{cases}$$

This means that this is also not a very costly action because 4 is a power of 2 so the runtime is $O(1)$. Reducing by modular arithmetic takes more time

at $O(\log n \log a)$, but in essence that step dominates the time and, in addition, the cost of that step decreases rapidly because the numbers themselves also decrease rapidly. Since the numbers are decreasing rapidly when calculating the Jacobi Symbol the runtime just ends up being $O(\log a \log n)$ but since $a < n$ it is $O(\log^2 n)$. Since this is less than the cost of modular exponentiation, the cost of the Solovay-Strassen algorithm as a whole is $O(\log^3 n)$.

A great proof of AKS's runtime from Roeland Singer-Heinze suggests that its runtime is $O(\log^{15/2} n)$ or $O(\log^6 n)$ if the Sophie-Germain Prime Density conjecture is true [Sin13]. When working with 2048-bit numbers a runtime that slow would be extremely detrimental. C

# References


[Con11] Keith Conrad. The miller–rabin primality test. *https://kconrad.math.uconn.edu/blurbs/ugradnumthy/millerrabin.pdf*, 2011.

[Con12] Keith Conrad. The solovay-strassen test. *https://kconrad.math.uconn.edu/blurbs/ugradnumthy/solovaystrassen.pdf*, 2012.

[Sin13] Roeland Singer. Run time efficiency and the aks primality test. *https://ccs.math.ucsb.edu/senior-thesis/Roeland-Singer.pdf*, 2013.

[Sta10] Cornell University CS4820 Course Staff. Handout: Miller–rabin primality test. *https://www.cs.cornell.edu/courses/cs4820/2010sp/handouts/MillerRabin.pdf*, 2010.