Miller-Rabin bases
Kichul Kim

Let $n \in \mathbb{N}$ be a composite. Define $\mathbf{S} = \{a \pmod n \mid a^t \equiv 1 \; or \; a^{2^j t} \equiv -1 \pmod n$, for $(0 \leq j \leq k-1)\}$, where $n = 2^k t$ and t is odd. Suppose $n = p_1^{e_1} p_2^{e_2} \dots p_r^{e_r}$. Furthermore, let $\nu(n)$ denote the largest integer such that $2^{\nu(n)} | p_i - 1$ for all $1 \leq i \leq r$. (This implies that $2^{\nu(n)} \| p_j - 1$ for some j.)

Claim 1. *If* $a^{2^j t} \equiv -1 \pmod n$, $j \leq \nu(n) - 1$.

Proof. $a^{2^{j+1} t} \equiv 1 \pmod n$ implies $a^{2^{j+1} t} \equiv 1 \pmod{p_i^{e_i}}$, for all i. For each $p_i^{e_i}$, the order of $a \pmod{p_i^{e_i}}$ is divisible by 2^{j+1}, because of the given condition above. That is, $2^{j+1} | \varphi(p_i^{e_i}) = p_i^{e_i - 1}(p_i - 1)$. Since $p_i^{e_i - 1}$ is odd, this implies that $2^{j+1} | p_i - 1$ for all i. Therefore, $j + 1 \leq m_i$ where $2^{m_i} \| p_i - 1$. This proves the claim. □

Claim 2. *The closure (under multiplication* $\bmod n$*) of the set* $\mathbf{A}_j = \{a \pmod n | a^{2^j t} \equiv -1 \pmod n\}$ *is the set* $\overline{\mathbf{A}}_j = \{a \pmod n | a^{2^j t} \equiv \pm 1 \pmod n\}$*, provided* $\mathbf{A}_j \neq \emptyset$.

Proof. It is clear that the closure of $\mathbf{A}_j$ is contained in $\overline{\mathbf{A}}_j$. Thus what remains to be proven is that $\{a \pmod n | a^{2^j t} \equiv 1 \pmod n\}$ is generated by $\mathbf{A}_j$. Let $c \in \{a \pmod n | a^{2^j t} \equiv 1 \pmod n\}$. Consider an element $a \in \mathbf{A}_j$. Since $a, c \in (\mathbb{Z}/n\mathbb{Z})^*$, there exists an element $b \in (\mathbb{Z}/nZ)^*$ such that $c \equiv ab \pmod n$. Then,

$$\begin{aligned} c^{2^j t} = (ab)^{2^j t} &= a^{2^j t} b^{2^j t} \\ &\equiv (-1) b^{2^j t} && \pmod n \\ &\equiv 1 && \pmod n \end{aligned}$$

Therefore, we know that $b^{2^j t} \equiv -1 \pmod n$, which implies that $b \in \mathbf{A}_j$. So c is in the span of the set $\mathbf{A}_j$. This completes the proof of the claim. □

It will follow from the computations below that $\mathbf{A}_j \neq \emptyset$ if $j \leq \nu(n) - 1$. Finally, observe that $\overline{\mathbf{A}}_j \subset \overline{\mathbf{A}}_{j+1}$. From the claim 1 above, it is clear that $\overline{\mathbf{S}} = \{a \pmod n | a^{2^{\nu(n)-1} t} \equiv \pm 1 \pmod n\}$ is the closure of $\mathbf{S}$. To prove that $\mathbf{S} = \overline{\mathbf{S}}$ *iff* n is divisible by a prime $3 \bmod 4$, we examine the condition for which the size of the sets $\mathbf{S}$ and $\overline{\mathbf{S}}$. That is, it suffices to show that the size of the two sets are equal if and only if n is divisible by a prime $3 \bmod 4$. First I count the size of the set $\{a | a^{2^{\nu(n)-1} t} \equiv 1 \pmod n\}$.

$$\begin{aligned} |\{a | a^{2^{\nu(n)-1} t} \equiv 1 \pmod n\}| &= \prod_{p | n} (2^{\nu(n)-1} \cdot \gcd(t, p_i - 1)) \\ &= 2^{(\nu(n)-1)\omega(n)} \prod \gcd(t, p - 1), \end{aligned}$$

where $\omega(n)$ is the number of distinct prime factors of n.
It can be easily computed that $\{a | a^{2^{\nu(n)-1} t} \equiv -1 \pmod n\}$ has the same size, using the fact that solutions to $a^{2^{\nu(n)} t} \equiv 1 \pmod{p_i^{j_i}}$ are solutions to $a^{2^{\nu(n)-1} t} \equiv \pm 1 \pmod{p_i^{j_i}}$, since $(\mathbb{Z}/p_i^{j_i}\mathbb{Z})^*$ is cyclic. To be more precise, the number of solutions to $a^{2^{\nu(n)-1} t} \equiv -1 \pmod{p_i^{j_i}}$ for each $p_i^{j_i} \| n$ is

$$2^{\nu(n)} \cdot \gcd(t, p_i - 1) - 2^{\nu(n)-1} \cdot \gcd(t, p_i - 1) = 2^{\nu(n)-1} \cdot \gcd(t, p_i - 1)$$

Multiplying the result for all primes dividing n, we conclude $a^{2^{\nu(n)-1}t} \equiv -1 \pmod{n}$ has the same number of solutions as $a^{2^{\nu(n)-1}t} \equiv 1 \pmod{n}$.

$$|\overline{\mathbf{S}}| = 2 \cdot 2^{(\nu(n)-1)\omega(n)} \prod \gcd(t, p-1) \tag{1}$$

Using the same method, I first calculate the size of solution set that satisfy each congruence condition of strong pseudo-primality and sum them up. First, sum the number of solutions to the condition $a^{2^j t} \equiv -1 \pmod{n}$, for all $j \leq \nu(n) - 1$.

$$\sum_{j=0}^{\nu(n)-1} 2^{j \cdot \omega(n)} \prod_{p|n} \gcd(t, p-1) = \left(\frac{2^{\omega(n)\nu(n)} - 1}{2^{\omega(n)} - 1} \right) \cdot \prod_{p|n} \gcd(t, p-1)$$

Similarly, the number of solutions to $a^t \equiv 1 \pmod{n}$ is $\prod_{p|n} \gcd(t, p-1)$. And thus

$$|\mathbf{S}| = \left(\frac{2^{\omega(n)\nu(n)} - 1}{2^{\omega(n)} - 1} + 1 \right) \cdot \prod_{p|n} \gcd(t, p-1) \tag{2}$$

And finally $|\mathbf{S}| = |\overline{\mathbf{S}}|$ *iff* (1) and (2) are the same. It can be concluded that $|\mathbf{S}| = |\overline{\mathbf{S}}|$ if and only if $2^{\omega(n)} = 2$ or $2^{\nu(n)-1} = 1$. That is, if n is a prime power or is divisible by a prime $3 \pmod{4}$.