Let $n > 0$ be an odd integer. We determine the size of the set B of elements in $(\mathbf{Z}/n\mathbf{Z})^*$ that pass a Miller-Rabin primality test. Writing $n-1 = 2^k m$ with m odd, we have

$$B \;=\; \{x \in (\mathbf{Z}/n\mathbf{Z})^* : x^m \equiv 1 \text{ or } x^{m2^i} \equiv -1 \text{ for some } 0 \le i < k\}.$$

Theorem. *The number of elements in B is given by*

$$\#B \;=\; \left(1 + \frac{2^{\mu d}-1}{2^d-1}\right) \prod_{p|n} \gcd(m, p-1).$$

Here d is the number of different primes dividing n and μ is the largest integer for which 2^μ divides $p-1$ for every prime divisor p of n.

Proof. The set B is the disjoint union of the following subsets

$$\{x \in (\mathbf{Z}/n\mathbf{Z})^* : x^m \equiv 1\} \quad \text{and} \quad \{x \in (\mathbf{Z}/n\mathbf{Z})^* : x^{m2^i} \equiv -1\} \quad \text{for } 0 \le i \le k-1.$$

First we consider the set $\{x \in (\mathbf{Z}/n\mathbf{Z})^* : x^m \equiv 1\}$. We have $x^m \equiv 1$ in $(\mathbf{Z}/n\mathbf{Z})^*$ if and only if $x^m \equiv 1 \pmod q$ for any prime power q dividing n. Since no prime divisor p of n divides m, we have $\#\{x \in (\mathbf{Z}/q\mathbf{Z})^* : x^m \equiv 1\} = \#\{x \in (\mathbf{Z}/p\mathbf{Z})^* : x^m \equiv 1\}$ when $q = p^a$ for some $a \ge 1$. By the Chinese remainder Theorem we have therefore

$$\#\{x \in (\mathbf{Z}/n\mathbf{Z})^* : x^m \equiv 1\} \;=\; \prod_{p|n} \gcd(m, p-1).$$

Next we consider the subsets of the form $\{x \in (\mathbf{Z}/n\mathbf{Z})^* : x^{m2^i} \equiv -1\}$ for $i = 0, 1, \ldots, k-1$. An element $x \in (\mathbf{Z}/n\mathbf{Z})^*$ satisfies $x^{m2^i} \equiv -1$ in $(\mathbf{Z}/n\mathbf{Z})^*$ if and only if $x^{m2^i} \equiv -1 \pmod q$ for all prime powers q dividing n. Since q is odd, we have $x^{m2^i} \equiv -1 \pmod q$ if and only if $x^{m2^{i+1}} \equiv 1 \pmod q$ while $x^{m2^i} \not\equiv 1 \pmod q$. Since the prime divisors of n do not divide m, there are for a given $i \ge 0$, *zero* elements in $(\mathbf{Z}/n\mathbf{Z})^*$ for which $x^{m2^i} \equiv -1$ unless for every prime divisor p of n, the number $p-1$ is divisible by 2^{i+1}. There are in the latter case precisely $\gcd(m2^{i+1}, p-1) - \gcd(m2^i, p-1) = 2^i \gcd(m, p-1)$ such elements. By the Chinese Remainder Theorem there are therefore $\prod_{p|n} 2^i \gcd(m, p-1) \;=\; 2^{id} \prod_{p|n} \gcd(m, p-1)$ elements in $x \in (\mathbf{Z}/n\mathbf{Z})^*$ for which $x^{m2^i} \equiv -1$ in $(\mathbf{Z}/n\mathbf{Z})^*$.

Taking the sum of the cardinalities of the k subsets, we obtain

$$\begin{aligned} \#B \;&=\; \prod_{p|n} \gcd(m, p-1) + \prod_{p|n} \gcd(m, p-1) \sum_{i=0}^{\mu-1} 2^{id}, \\ &=\; \left(1 + \frac{2^{\mu d}-1}{2^d-1}\right) \prod_{p|n} \gcd(m, p-1), \end{aligned}$$

as required.

Note that when n is prime, we have $d = 1$ and we find $\#B = \gcd(m, n-1)2^\mu = m2^k = n-1$ which confirms the fact that $B = (\mathbf{Z}/n\mathbf{Z})^*$ in this case.

Corollary. *For odd composite $n \neq 9$ we have*

$$\#B \ \leq \ \frac{1}{4}\varphi(n).$$

Proof. Let $n \neq 9$ be an odd positive integer. By the theorem we must show that

$$\left(1 + \frac{2^{\mu d} - 1}{2^d - 1}\right) \prod_{p|n} \gcd(m, p-1) \ \leq \ \frac{1}{4}\varphi(n).$$

When $d = 1$ we have $n = p^a$ for some prime p and $a \geq 2$. We must show that $\gcd(m, p-1)2^\mu \leq \frac{1}{4}\varphi(p^a)$. Since $\mu = k$ in this case, the left hand side is precisely equal to $p - 1$. Therefore we must show that $p^{a-1} \geq 4$, which is true since $n \neq 9$. For $d \geq 3$ we observe that

$$\prod_{p|n} \gcd(m, p-1) \leq \frac{1}{2^{\mu d}} \prod_{p|n} (p-1) \leq \frac{1}{2^{\mu d}}\varphi(n).$$

Therefore it suffices to show that $1 + \frac{2^{\mu d}-1}{2^d-1} \leq \frac{1}{4}2^{\mu d}$, which follows from the fact that $\mu \geq 1$ and $d \geq 3$.

The remaining case is $d = 2$. If the 2-adic valuations of $p-1$ for the two prime divisors p of n are distinct, then

$$\prod_{p|n} \gcd(m, p-1) \leq \frac{1}{2^{2\mu+1}} \prod_{p|n} (p-1) \leq \frac{1}{2^{2\mu+1}}\varphi(n).$$

Therefore it suffices to show that $1 + \frac{2^{2\mu}-1}{3} \leq \frac{1}{4}2^{2\mu+1}$. This follows from the fact that $\mu \geq 1$. Finally, if $d = 2$ and the 2-adic valuations of $p - 1$ for the two prime divisors p of n are equal, then the odd parts of $\prod_{p|n} \gcd(m, p-1)$ and $\prod_{p|n}(p-1)$ cannot be the same. Indeed, it would follow that the odd part of $p - 1$ divides $n - 1$ for each prime divisor p of n. This easily implies that the two prime divisors of n must be equal, contradicting the assumption $d = 2$. It follows that the odd part of $\prod_{p|n} \gcd(m, p-1)$ is at most $\frac{1}{3}$ of the odd part of $\prod_{p|n}(p-1)$. Therefore we have

$$\prod_{p|n} \gcd(m, p-1) \leq \frac{1}{3 \cdot 2^{2\mu}} \prod_{p|n} (p-1) \leq \frac{1}{3 \cdot 2^{2\mu}}\varphi(n).$$

Therefore it suffices to show that $1 + \frac{2^{2\mu}}{3} \leq \frac{3}{4}2^{2\mu}$, which follows from the fact that $\mu \geq 1$.

This proves the corollary.

It follows from the proof that the inequality can only be sharp when $\mu = 1$ and $d = 2$ or 3. In the first case $n = pq$ with p and q primes of the form $p = 1+2m$ and $q = 1+4m$ for some odd m. This is probably an infinite set of examples. E.g. $n = 15$, 91, 703, ... In the second case n is a Carmichael number of the form $n = pqr$ with p, q and r primes that are congruent to 3 (mod 4). This is probably also an infinite set of examples. E.g. 8911, ...