Let's look more at the group structure of $(\mathbb{Z}/n\mathbb{Z})^\times$:

Rmk ~~The 2-tor~~ ~~If n~~ For odd $n = p_1^{e_1} \cdots p_u^{e_u}$, the 2-torsion subgroup is

$$\begin{array}{ccc} (\mathbb{Z}/n\mathbb{Z})^\times[2] & \cong & \{\pm 1\} \times \dots \times \{\pm 1\} \,. \\ \cap & & \cap \qquad\qquad \cap \\ (\mathbb{Z}/n\mathbb{Z})^\times & & C_{\varphi(p_1^{e_1})} \times \dots \times C_{\varphi(p_u^{e_u})} \end{array}$$

cyclic groups of even order

Rmk Assume that n is an odd Carmichael number,

$n - 1 = 2^r \cdot s$ with $r \geq 1$ and odd s.

~~Then, the set~~

~~$T := \{ a \in (\mathbb{Z}/n\mathbb{Z})^\times \mid a^s \equiv 1 \bmod n$ or $a^{2^{i-1}s} \equiv -1 \bmod n$, $a^{2^i s} \equiv 1 \bmod n$ for some $i \in \{1, \dots, r\}\}$~~

~~is a subgroup of $(\mathbb{Z}/n\mathbb{Z})^\times$.~~

For $0 \leq j \leq r$, consider the subgroup

$$T_j := \{ a \in (\mathbb{Z}/n\mathbb{Z})^\times \mid a^{2^j s} \equiv 1 \bmod n \}.$$

Clearly, $T_r = (\mathbb{Z}/n\mathbb{Z})^\times$, but $-1 \notin T_0$. Let l be the largest index with $T_l \neq (\mathbb{Z}/n\mathbb{Z})^\times$. Consider the subgroup

(The l is the smallest nr. s.t. $\varphi(p_i^{e_i}) \mid 2^{l+1}s$ for all i.)

$$U := \{ a \in (\mathbb{Z}/n\mathbb{Z})^\times \mid a^{2^l s} \equiv \pm 1 \bmod n \}.$$

Lemma 15.6 Let n be an odd Carmichael number. We have

$U = (\mathbb{Z}/n\mathbb{Z})^\times$ if and only if n is prime.

Pf "$\Leftarrow$" $a^{2^{l+1}s} \equiv (a^{2^l s})^2 \equiv 1 \implies a^{2^l s} \equiv \pm 1$

"$\Rightarrow$" ~~For some (prime) factor~~ For some i, every $2^{l+1}s$-th power in

$(\mathbb{Z}/p_i^{e_i})^\times$ is 1 but [illegible] $\implies$ Some $2^l s$-th power is -1.

$\Rightarrow$ By the Chin. rem. thm., there is some $a \in (\mathbb{Z}/n\mathbb{Z})^\times$ s.t.

$a \equiv 1 \bmod p_{i'}^{e_{i'}} \quad \forall i' \neq i$

and $a^{2^\ell s} \equiv -1 \bmod p_i^{e_i}$.

$\Rightarrow a^{2^\ell s} \not\equiv \pm 1 \bmod n$. $\square$

Cor 15.7 There is a Monte Carlo alg. to determine whether n is prime with false pos. prob. $\leq \frac{1}{2}$, no false neg., avg. running time $\tilde{O}((\log n)^2)$

Alg Pick $a \in (\mathbb{Z}/n\mathbb{Z})^\times$ uniformly at random.

Compute $b = a^s$,

then b^{2^i} for $i = 1, \dots, r$.

If $b^{2^r} \not\equiv 1$, return $\boxed{\text{not prime}}$ (not even Carmichael).

If $b^{2^{i+1}} \equiv 1$ but $b^{2^i} \not\equiv \pm 1$ for some i, return $\boxed{\text{not prime}}$.

Otherwise, return $\boxed{\text{(maybe) prime}}$.

Pf False pos. (even just for $i = \ell$) can only occur when $a \in U \subsetneq (\mathbb{Z}/n\mathbb{Z})^\times$. $\square$

Rmk There is also an unconditional ~~a~~ deterministic alg. that determines whether n is prime in time $\tilde{O}((\log n)^6)$. (AKS algorithm)

Rmk Assuming the generalized Riemann Hypothesis, $(\mathbb{Z}/n\mathbb{Z})^\times$ is generated by $1, \dots, \lfloor 3(\log n)^2 \rfloor$, so it suffices to check $a = 1, \dots, \lfloor 3(\log n)^2 \rfloor$ for a deterministic primality test (Miller test).

Thm 15.8 There's an alg. that returns a random number $p \le N$ in expected time $\tilde{O}(k \cdot (\log N)^3)$ with $\mathbb{P}(p \text{ not prime}) \le 2^{-k} \log N$.
All primes $p \le N$ are equally likely to occur.

Alg Pick $p \le N$ uniformly at random. If Rabin-Miller "prob. prime" k times, return p. Otherwise, start over.

Pf The number of primes $p \le N$ is $\ge \Omega\left(\frac{N}{\log N}\right)$.

$\Rightarrow$ The alg. makes $\le O(\log N)$ attempts on average.
On each attempt, the prob. of returning a composite no. is $\le \frac{1}{2^k}$.

$\square$

Rmk Many alg. that require choosing a random prime p actually "work" with composite numbers as well:
Either they succeed, or they prove that p is composite (e.g. when trying to divide by a nonzero noninvertible element of $\mathbb{Z}/n\mathbb{Z}$).
For others, you may need to prove primality.

Lemma 15.9 Let $n \geq 3$ be an odd composite integer. Given a uniform random element $a \in (\mathbb{Z}/n\mathbb{Z})^\times$ and its (multiplicative) order $\mathrm{ord}(a)$ (or the size $\varphi(n) = \#(\mathbb{Z}/n\mathbb{Z})^\times$), we can with prob. $\geq \frac{1}{4}$ find a proper divisor $1 < d < n$ of n in time $\tilde{O}((\log n)^2)$.

Pf Write $\varphi(n) = 2^r s$ and $\mathrm{ord}(a) = 2^t v$.

($\mathrm{ord}(a) \mid \varphi(n) \Rightarrow t \leq r$ and $v \mid s$.)

~~Consider the map~~

$$\cancel{f: (\mathbb{Z}/n\mathbb{Z})^\times \longrightarrow (\mathbb{Z}/n\mathbb{Z})^\times, \quad x \longmapsto x^s}$$

~~Under the CRT, it corr. to~~

$$\cancel{\prod_i (\mathbb{Z}/p_i^{e_i}\mathbb{Z})^\times \longrightarrow \prod_i \{\pm 1\}, \quad (x_i)_i \longmapsto (x_i^s)_i}$$

Claim: With prob. $\geq \frac{1}{4}$, of the numbers $d_i = \gcd(a^{2^i v} - 1, n)$ for $i = 0, \ldots, t-1$, a proper divisor.

Pf As before, let ℓ be the smallest nr. s.t. $\varphi(p_i^{e_i}) \mid 2^{\ell+1} s \quad \forall i$.

Let $\varphi(p_i^{e_i}) \nmid 2^\ell s$ and let $j \neq i$.

$\Rightarrow$ We have hom.

$$f_i : (\mathbb{Z}/p_i^{e_i}\mathbb{Z})^\times \twoheadrightarrow \{\pm 1\}, \quad x \mapsto x^{2^\ell s}, \qquad f_j : (\mathbb{Z}/p_j^{e_j}\mathbb{Z})^\times \to \{\pm 1\}, \quad x \mapsto x^{2^\ell s}$$

with surjective f_i.

$$\left.\begin{array}{l} \text{With prob. } \frac{1}{2}, \; f_i(a) = -1 \; \Rightarrow a^{2^\ell v} \equiv -1 \bmod p_i^{e_i} \\ \text{With prob. } \geq \frac{1}{2}, \; f_j(a) = +1 \; \Rightarrow a^{2^\ell v} \equiv +1 \bmod p_j^{e_j} \end{array}\right\} \text{independent by CRT}$$

$\Rightarrow$ With prob. $\geq \frac{1}{4}$, $\gcd(a^{2^\ell v} - 1, n)$ is divisible by p_j, but not by p_i.