Composite Numbers having Primitive Roots

We saw that 2 is a primitive root of 9, so we can notice that composite numbers can also possess primitive roots.

Theorem:- For $k \geq 3$, the integer 2^k has no primitive roots.

Proof:- If a is an odd integer then $\gcd(a, 2^k) = 1$ for $k \geq 3$, we just show that a is not primitive root of 2^k.

i.e $\quad a^m \equiv 1 \bmod 2^k$ for $m < \phi(2^k)$

$\phi(2^k) = 2^k - 2^{k-1} = 2^k(1-\frac{1}{2})$
$= 2^{k-1}$

for $m < 2^{k-1}$
If $a^m \equiv 1 \bmod 2^k \Rightarrow a$ is not primitive root of 2^k.

claim, $m = 2^{k-2}$

Logic:- $k = 3$, $\quad a^{2^{k-2}} \equiv 1 \bmod 2^k$

$a^2 \equiv 1 \bmod 8 \qquad \gcd(a, 8) = 1$
$\phi(8) = 4$

$\because a^2 \equiv 1 \bmod 8, \; 2 < \phi(8)$

$\therefore$ 2 is not primitive root of 2^3.

for $k > 3$: by induction,
suppose $a^{2^{k-2}} \equiv 1 \bmod 2^k$ is true for k
$\Rightarrow a^{2^{k-2}} = 1 + b2^k$

we prove it for $k+1$,

$(a^{2^{k-2}})^2 = 1^2 + b^2 2^{2k} + 2b2^k$
$= 1 + 2^{k+1}(b + b^2 2^{k-1})$

$a^{2^{k-1}} \equiv 1 \bmod 2^{k+1}$

$\therefore$ true for $k+1$

$\therefore$ a is not primitive root for any odd integer

Theorem: If $\gcd(m,n)=1$, where $m>2$ and $n>2$ then the integer mn has no primitive roots.

Proof: Consider any integer a for which $\gcd(a, mn)=1$ then $\gcd(a,m)=1$ and $\gcd(a,n)=1$

put $h = \operatorname{lcm}(\phi(m), \phi(n))$
$d = \gcd(\phi(m), \phi(n))$

Because $\phi(m)$ and $\phi(n)$ are both even,
$\therefore d \geq 2$. we know $hd = \phi(m)\phi(n)$

$$h = \frac{\phi(m)\phi(n)}{d} \leq \frac{\phi(mn)}{2}$$

by Euler's theorem, $a^{\phi(m)} \equiv 1 \bmod m$

$$a^h = \left(a^{\phi(m)}\right)^{\frac{\phi(n)}{d}} \equiv 1 \bmod m \quad \text{—(1)}$$

smly $a^h \equiv 1 \bmod n$ —(2)

$a^h \equiv 1 + k_1 m$
$a^h \equiv 1 + k_2 n$
$a^h . a^h \equiv 1 + k_2 n + k_1 m + k_1 k_2 mn$

$\Rightarrow a^h \equiv 1 \bmod mn$

$\because h \leq \frac{\phi(mn)}{2} < \phi(mn)$

$\Rightarrow h < \phi(mn)$

$\therefore$ a is not primitive root of mn.

Corollary: The integer n fails to have a primitive root if either

(a) n is divisible by two odd primes or
(b) n is of the form $n = 2^m p^k$, where p is odd prime and $m \geq 2$.