THM $a \pmod n$ order k
$\Rightarrow a^m$ order $\frac{k}{\gcd(k,m)}$

in particular, if $a \pmod n$ prim. root $[k = \phi(n)]$
then: a^m prim. root mod n
$\iff \gcd(\phi(n), m) = 1$

THM If there is a prim. root mod n, then
prim. roots mod n $= \phi(\phi(n))$

true $\iff n = 1, 2, 4, p^k, 2p^k$

prim. roots mod p $= \phi(\phi(p)) = \phi(p-1)$

EG List all prim. roots mod 22

$\phi(22) = \phi(2)\phi(11)$
$= 10$

① find one prim. root
try ~~2~~, 3, ~~4~~, 5, ...
not invertible
$\rightsquigarrow$ 7 prim. root

② 7^m prim. root
$\iff \gcd(10, m) = 1$ $\quad m = 1, 3, 7, 9$
$\phi(22)$

$\Rightarrow$ prim. roots mod 22 $= \underbrace{7, 7^3, 7^7, 7^9}$
$4 = \phi(\phi(22))$