Primitive roots part 2

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

$x \pmod n$ primitive root $\Leftrightarrow$ $x \pmod n$ order $\phi(n)$

EG (a) Show that $7 \pmod{26}$ is a primitive root.
(b) List all primitive roots mod 26.

(a) $\phi(26) = \phi(2)\phi(13) = 1 \cdot 12 = 12$
$\Rightarrow$ order of 7 (mod 26) divides 12
possible orders: ~~1~~, ~~2~~, ~~3~~, ~~4~~, ~~6~~, 12
$7^2 \equiv -3$ $7^3 \equiv -3 \cdot 7 \equiv 5$
$7^4 \equiv 5 \cdot 7 \equiv 9$ $7^6 \equiv (7^3)^2 \equiv 25 \equiv -1$
$\Rightarrow$ order $= 12$ i.e. primitive root

(b) all invertible residues (mod 26) (12) are of the form 7^a for some a
order of $7^a \pmod{26} = \frac{12}{\gcd(12,a)}$
if $= 12$ primitive root!

7^a primitive root
$\Leftrightarrow \gcd(12,a) = 1$
$\Leftrightarrow a = 1, 5, 7, 11$

$\Rightarrow$ primitive roots are $7^1, 7^5, 7^7, 7^{11} \pmod{26}$

4 primitive roots
$= \phi(12) = \phi(\phi(26))$

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

true if n is of the form $1, 2, 4, p^k, 2p^k$ for odd prime p

EG mod 8: there are no primitive roots

THM # primitive roots (mod p) $= \phi(p-1)$