Primitive roots

review: order of $x \pmod n$ = smallest $k>0$ so that $x^k \equiv 1 \pmod n$

DEF $x \pmod n$ is a **primitive root** if its order is $\phi(n)$.
— maximal possible order

THM order $x \pmod n$ divides $\phi(n)$

follows from the following:

if $x^r \equiv 1$ and $x^s \equiv 1 \pmod n$ then $x^{\gcd(r,s)} \equiv 1 \pmod n$

Why? Bezout's identity:

$\gcd(r,s) = a\cdot r + b\cdot s$ for some a,b

$x^{\gcd(r,s)} = x^{a\cdot r + b\cdot s} = (x^r)^a \cdot (x^s)^b \equiv 1 \pmod n$
($x^r \equiv 1$, $x^s \equiv 1$)

$r = k$ (order of x)
$s = \phi(n)$

$\Rightarrow x^{\gcd(k,\phi(n))} \equiv 1 \pmod n$
$\Rightarrow k = \gcd(k,\phi(n))$
$\Rightarrow k \mid \phi(n)$

EG order of $2 \pmod 9$

$\phi(9) = \phi(3^2) = 3^2 - 3^1 = 6$
$\Rightarrow$ possible orders ~~1~~, ~~2~~, ~~3~~, 6

$2^2 = 4 \qquad 2^3 \equiv -1 \qquad \Rightarrow$ order $= 6$

in particular: $2 \pmod 9$ is a primitive root

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

$(x^a)^m = x^{am} \equiv 1$ — smallest $m = \frac{k}{\gcd(k,a)}$

know: $x^k \equiv 1$

EG order of $4 \pmod 9$ $= \frac{6}{\gcd(6,2)} = 3$
(order of 2 $\pmod 9$)

$4 = 2^2$

note: $4^3 = (2^2)^3 = 2^6$

every invertible residue $\pmod 9$ can be written as 2^a for some a

order of $2^5 \pmod 9 = \frac{6}{\gcd(6,5)} = 6$

$2^5 = 32 \equiv 5$ is another primitive root