DEF $a \pmod n$

multiplicative order k

= smallest k such that $a^k \equiv 1 \pmod n$

EG $2 \pmod 7$

$2^2 = 4,\ 2^3 \equiv 1 \pmod 7 \rightsquigarrow$ order $= 3$

$\phi(7) = 6$

possible orders: 1, 2, 3, 6

EG $3 \pmod 7$

$3^2 \equiv 2,\ 3^3 \equiv -1,\ 3^4 \equiv -3,\ 3^5 \equiv -2,\ 3^6 \equiv 1$

$\rightsquigarrow$ order $= 6$ (not needed)

FACTS: order of $a \pmod n$

- order $\leq \phi(n)$

  in fact: order $\mid \phi(n)$

  Euler: $a^{\phi(n)} \equiv 1 \pmod n$

- order $= \phi(n)$

  $\Rightarrow$ $a \pmod n$ primitive root (multiplicative generator)

  $\Rightarrow$ $1, a, a^2, a^3, \ldots, a^{\phi(n)-1}$ is a list of all invertible residues mod n