# Multiplicative order

**DEF** multiplicative order of $x \pmod n$
= smallest $k>0$ so that
$x^k \equiv 1 \pmod n$

needs to be invertible [$\gcd(x,n)=1$]

**EG** order of $2 \pmod 7 = 3$
$2^1=2,\ 2^2=4,\ 2^3=8\equiv 1 \pmod 7$

order of $3 \pmod 7 = 6$

list of all invertible residues mod 7

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

**Euler's theorem:** $x^{\phi(n)}\equiv 1 \pmod n$
if $\gcd(x,n)=1$

$n=7$: $x^6\equiv 1 \pmod n$

**DEF** $x \pmod n$ is a **primitive root**
or: multiplicative generator
if order of $x \pmod n$ is $\phi(n)$.

in that case
$\underbrace{x^0}_{\equiv 1}, x^1, x^2, \dots, x^{\phi(n)-1}$ $\Big\}$ $\underbrace{x^{\phi(n)}}_{\equiv 1}$
is a list of all invertible residues mod $n$

**EG** $3 \pmod 7$ is a primitive root
[order = 6]

$2 \pmod 7$ is not a primitive root
[order = 3]