

# Euler's theorem

THM (Little Fermat)

$$a^{p-1} \equiv 1 \pmod{p}$$

provided that  $p \nmid a$  ← "a invertible"

THM (Euler)

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

provided that  $\gcd(a, n) = 1$

$$\phi(p) = p-1$$

in fact:  
 $a^{-1} \equiv a^{\phi(n)-1} \pmod{n}$

EG

$$37^{101} \pmod{35}$$

$$\equiv 2^{101}$$

$$\equiv 2^5 = 32 \equiv -3 \pmod{35}$$

$$101 \equiv 5 \pmod{24}$$

Euler:  $\phi(35) = \phi(5)\phi(7) = 4 \cdot 6 = 24$

$$a^{24} \equiv a^0 \equiv 1 \pmod{35}$$

EG

What are the last two (decimal) digits of  $3^{4242}$ ?

need:  $3^{4242} \pmod{100}$

$$4242 \equiv 2 \pmod{40}$$

$$\equiv 3^2 = 9 \pmod{100}$$

⇒ last two digits: 09

$$\phi(100) = \phi(2^2)\phi(5^2) = (2^2-2)(5^2-5^1) = 40$$