

Wilson's Theorem (and  $p$  is prime)

$$(p-1)! \bmod p = -1 \text{ or } (p-1)$$

now when you want to take out mod of a factorial.

Note that for  $(n!) \% p$   
if  $n > p$

$$(1 \times 2 \times 3 \dots \times p \times \dots \times n) \% p = 0$$

but for  $n < p$

$$(1 \times 2 \times 3 \dots \times n) \% p$$

now extend this to  $(p-1)$

$$(1 \times 2 \times 3 \times \dots \times n \times (n+1) \times \dots \times (p-1)) \% p$$

$$n! \bmod p \times (n+1) \bmod p \times \dots \times (p-1) \bmod p = -1$$

Wilson's applied.

$$n! \bmod p = (n+1)^{-1} \bmod p \times \dots \times (p-1)^{-1} \bmod p$$

Fermat's says  $a^{-1} \bmod p = a^{p-2} \bmod p$

mod exp application

$$n! \bmod p = (n+1)^{p-2} \bmod p \times (n+2)^{p-2} \bmod p \times \dots \times (p-1)^{p-2} \bmod p \times -1$$