

### problems 3

$$\begin{aligned} \textcircled{1} \quad 3^{28} \bmod 10 &= (3^2)^{14} \bmod 10 = 9^{14} \bmod 10 = \\ &= (9^2)^7 \bmod 10 = 81^7 \bmod 10 = \\ &= (81 \bmod 10)^7 = 1^7 = \boxed{1} \end{aligned}$$

$$\begin{aligned} 3^{200} \bmod 15 &= (3^2)^{100} \bmod 15 = 9^{100} \bmod 15 = \\ &= (9^2)^{50} \bmod 15 = 81^{50} \bmod 15 = \\ &= (81 \bmod 15)^{50} \bmod 15 = 6^{50} \bmod 15 = \\ &= (6^2)^{25} \bmod 15 = 36^{25} \bmod 15 = \\ &= 6^{25} \bmod 15 = (6^2 \cdot 6^{23}) \bmod 15 = \\ &= 36 \bmod 15 \cdot 6^{23} \bmod 15 = 6 \cdot 6^{23} \bmod 15 = \\ &= \dots = 6 \cdot 6 \bmod 15 = 36 \bmod 15 = \boxed{6} \end{aligned}$$

② Donner alg. pol. que calcule:  $a^b \bmod p$   $\begin{cases} a, b, c \in \mathbb{Z}^+ \\ p \in \text{PRIMES} \end{cases}$

input  $a, b, c, p$  {

$x = \text{exp}(b, c, p-1) \rightarrow$  *théorème petit de Fermat*  
return  $\text{exp}(a, x, p)$

}

$\text{exp}(\text{base}, \text{exponent}, \text{mod})$  {

if  $\text{exponent} == 0$  return 1

if  $\text{exponent} \% 2 == 0$  {

$t = \text{exp}(\text{base}, \text{exponent}/2, \text{mod})$

return  $(t * t) \% \text{mod}$

}

else {

$t = \text{exp}(\text{base}, (\text{exponent}-1)/2, \text{mod})$

return  ~~$\text{base} * \text{exp}(\text{base}, \text{exponent}/2, \text{mod})$~~   $(\text{base} * t^2) \% \text{mod}$

}

$$\text{cost: } \log_2(2^{|a|}) = O(|a|)$$

el cost de  $|b|, |c|$  i  $|a|$  és similar.

$\rightarrow$  *proprietat de la exp. modular*