Problemas 3

① $3^{28} \bmod 10 = (3^2)^{14} \bmod 10 = 9^{14} \bmod 10 =$

$= (9^2)^7 \bmod 10 = 81^7 \bmod 10 =$

ou

$= (81 \bmod 10)^7 = 1^7 = \boxed{1}$

$3^{200} \bmod 15 = (3^2)^{100} \bmod 15 = 9^{100} \bmod 15 =$

$= (9^2)^{50} \bmod 15 = 81^{50} \bmod 15 =$

$= (81 \bmod 15)^{50} \bmod 15 = 6^{50} \bmod 15 =$

ou

$= (6^2)^{25} \bmod 15 = 36^{25} \bmod 15 =$

$= 6^{25} \bmod 15 = (6^2 \cdot 6^{23}) \bmod 15 =$

$= 36 \bmod 15 \cdot 6^{23} \bmod 15 = 6 \cdot 6^{23} \bmod 15 =$

$= \ldots = 6 \cdot 6 \bmod 15 = 36 \bmod 15 = \boxed{6}$

(2) Donats als pd. que calculi $a^{b^c} \bmod p$ $\begin{cases} a,b,c \in \mathbb{Z}^+ \\ p \in PRIMES \end{cases}$

```
input a,b,c,p {
    x = exp(b,c, p-1)  -> teorema petit de fermat
    return exp(a,x,p)
}

exp(base, exponent, mod){
    if exponent == 0  return 1
    if exponent % 2 == 0 {
        t = exp(base, exponent/2, mod)
        return (t*t) % mod  -> propietat de la exp. modular
    }
    else {
        t = exp(base, (exponent-1)/2, mod)
        return base * exp(base * t^2) % mod
    }
}
```

ou.

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

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

Recursiva?