Math

Inverse modulaire

- Soit $a \in \mathbb{Z}_n^\times$ un entier premier avec n, on note son **inverse** $a^{-1} \in \mathbb{Z}_n^\times$ le nombre tel que

$$aa^{-1} \equiv 1 \pmod{n}$$

- On peut l'obtenir en calculant $(d, x, y) = egcd(a, n)$ puisque $d = \gcd(a, n) = 1$ et

$$\begin{aligned} ax + \cancel{ny} &\equiv d \pmod{n} \\ ax &\equiv 1 \\ \implies x &= a^{-1} \end{aligned}$$

Math

Exponentiation rapide

- Naïf 7 mul: $2^8 = 2 \times 2 \times 2 \times 2 \times 2 \times 2 \times 2 \times 2$

$$a^n = \begin{cases} 1 & \text{si n = 0} \\ a \times a^{n-1} & \text{sinon} \end{cases}$$

$$a^n = \begin{cases} 1 & \text{si } n = 0 \\ \left(a^{\frac{n}{2}}\right)^2 & \text{si } n \text{ est pair} \\ a \times a^{n-1} & \text{sinon} \end{cases}$$

- $2^8 = 2^{2^{2^2}}$ multiplie par lui-même 3 fois

- $\Longrightarrow$ exponentiation par ~1000 nécessite une dizaine de multiplications plutôt qu'un millier