

# Math

## Exponentiation rapide

- Naïf 7 mul:  $2^8 = 2 \times 2$

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

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

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

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

# Math

## Génération probabiliste de nombre premiers (Miller-Rabin)

- Tire  $n$  aléatoirement tant que
  - Aucun de  $k$  nombres aléatoires  $a \in \mathbb{Z}_n^\times$  (i.e. tels que  $a \perp n$ ) ne témoigne contre  $n$
  - On dit qu'un nombre  $a$  **témoigne contre**  $n$  si
    - On calcule  $s, d$  tels que  $n - 1 = 2^s \times d$  pour un  $d$  impair et  $x = a^d \pmod{n}$
    - Aucun des  $s$  répétitions de  $x \leftarrow x^2 \pmod{n}$  ne sont égal à 1 ou  $n - 1$
  - Plus  $k$  est grand, plus on est confiant (pas sur) que  $n$  est premier