Math

Arithmétique modulaire

$n \in \mathbb{N}$

- On note $\mathbb{Z}_n$ l'ensemble des entiers modulo n, représentés par les restes de la division par n
- On note $\mathbb{Z}_n^\times = \{a \in \mathbb{Z}_n \mid a \perp n\}$ l'ensemble des **inversibles** modulo n
- On note $\varphi(n)$ (appelée indicatrice d'Euler) la cardinalité de cet ensemble
- Théorème d'Euler:

$$\forall a \in \mathbb{Z}_n^\times : a^{\varphi(n)} \equiv 1 \pmod{n}$$

- i.e. L'exposant d'un entier modulo n est modulo $\varphi(n)$

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

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