Math

Algorithme étendu d'Euclide

- Étant donné 2 entiers $a, b \in \mathbb{Z}$ on calcule
  - Le plus grand diviseur commun $d = \gcd(a, b)$
  - Les coefficients de Bézout $x, y \in \mathbb{Z}$ tels que $ax + by = d$

$$egcd(a,b) = \begin{cases} (1,0,a) & \text{si } b = 0 \\ (y, x - y\frac{a}{b}, d) & \text{si } (x,y,d) = egcd(b, a \mod b) \end{cases}$$

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 $\varphi(n)$