Math

Diviseurs et primalité

$a, b \in \mathbb{Z}$

- b **divise** a (noté $b \mid a$) si la division de a par b est un nombre entier
- Le **plus grand diviseur commun** de a et b (noté $\gcd(a, b)$) est le plus grand nombre qui divise à la fois a et b
- a est **premier** s'il n'a comme diviseurs que 1 et lui-même
- a et b sont **premiers entre eux** (noté $a \perp b$) si $\gcd(a, b) = 1$
- Il existe des entiers $x, y \in \mathbb{Z}$ (appelés **coefficients de Bézout**) tels que $ax + by = \gcd(a, b)$

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 $ax + by = d$

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