Notions d'arithmétique modulaire

$a \ mod \ m$ est le reste de la division entière de a par m ($0 \leq a \ mod \ m \leq m - 1$).

$a \equiv b (mod \ m)$ si m divise $(b - a)$.

lem.: $a \equiv b (mod \ m)$ ssi $a \ mod \ m = b \ mod \ m$.

Exemple : $143 \ mod \ 5$? $-18 \ mod \ 7$?

$pgcd$ est le plus grand commun diviseur.

$\mathbb{Z}_m = \{0, \ldots, m - 1\}$
$x \ op_m \ y : x \ op \ y \ mod \ m$ avec $op \in \{+, -, *\}$

La fonction indicatrice d'Euler $\phi(m)$ est définie par le nombre d'entiers de $\mathbb{Z}_m$ qui sont premiers avec m.

Soit $a \in \mathbb{Z}_m$, $a^{-1} \in \mathbb{Z}_m$ est l'inverse de a si $a *_m a^{-1} \equiv a^{-1} *_m a \equiv 1 (mod\ m)$.

Th.: Un nombre a admet un inverse dans $\mathbb{Z}_m$ si et seulement si $pgcd(a, m) = 1$ (i.e. a et m sont premiers entre-eux).

Algo. d'Euclide : Le plus grand commun diviseur de deux nombres b et a ($b > a$) est donné par la définition récursive suivante :

$$pgcd(a, b) = \begin{cases} a \text{ si } b\ mod\ a = 0 \\ pgcd(b\ mod\ a, a) \text{ sinon} \end{cases}$$

Algo. d'Euclide étendu : L'inverse de x dans $\mathbb{Z}_m$ si il existe est $x_m^{-1} = inverse(x, m, 0, 1, m)$ avec :

$$inverse(u, v, t, t', m)$$
$$\begin{cases} t' \text{ si } v\ mod\ u = 0 \text{ et } u = 1 \\ \perp \text{ si } v\ mod\ u = 0 \text{ et } u \neq 1 \\ inverse(v\ mod\ u, u, t', (t - (v\ div\ u) * t')\ mod\ m, m) \end{cases}$$