Chapitre 3 : Arithmétique modulaire

Nombres premiers : simplement réécrire la liste des nombres premiers et ensuite diviser.

Division euclidienne : multiplier le quotient afin d'éliminer le plus haut degré du polynômes.

MOD :

le mod est simplement le reste entre la division entre 2 termes.

Inverse modulaire :

L'inverse modulaire de a modulo n signifie que lorsqu'on multiplie a par n, on retrouve 1.

$$a\,x \equiv 1 \pmod{n}$$

⚠ a peut être inversé dans n uniquement si leur PGCD = 1. (Bachet-Bézout)

Le PGCD peut s'écrire ainsi

$$a\,x + n\,y = PGCD(a, n)$$

$$\Leftrightarrow \quad a\,x + n\,y = 1$$

Le coefficient x sera l'inverse de a dans n.

Résolution dans un tableau :

r	s	t	Q
a	1	0	X
n	0	1	q_i

r_i : $r_{i-2} - (r_{i-1} \cdot Q_{i-1})$

s_i : $t_{i-2} - (t_{i-1} \cdot q_{i-1})$

t_i : $s_{i-2} - (s_{i-1} \cdot Q_{i-1})$

Q : la colonne des quotient

Pour chaque nouvelle ligne, je dois soustraire l'élément 2 lignes au-dessus par la ligne au-dessus × Q.

Exemple : inverse de 7 dans 26

D'abord, j'initialise tout

r	s	t	Q
26	1	0	
7	0	1	3

→ quotient de 26/7

Je passe à la ligne suivante en faisant les opérations nécessaires :

$r = 26 - (7 \times 3) = 5$
$s = 1 - (0 \times 3) = 1$
$t = 0 - (1 \times 3) = -3$

r	s	t	Q
5	1	-3	1

→ quotient de 7/5

⚠ pour calculer le quotient on va prendre le reste de notre ligne actuelle et le faire diviser par celui de la ligne précédente

Ligne suivante :

$r = 7 - (5.1) = 2$
$s = 0 - (1.1) = -1$
$t = 1 - (-3.1) = 4$

r	s	t	Q
2	-1	4	2

Et ainsi de suite jusqu'à ce que le reste vaille 1

r	s	t	Q
1	3	-11	2

Ça veut dire que l'écriture finale sera

$$PGCD(26,7) = 3.26 + (-11).7 = 1$$

Donc l'inverse de 7 dans 26 sera -11

⚠ grosse erreur : lorsque le coefficient est négatif, il faut le soustraire au modulaire donc $26 - 11 = 15$