TD – Décodage des codes de Reed-Solomon

Exercice 1. *Division de polynômes*

La division euclidienne de polynômes peut s'effectuer similairement à la division euclidienne d'entiers. À chaque étape, on *élimine* le terme de plus haut degré du dividende. Par exemple, pour diviser $A = 3X^4 - 5X^3 + 2X^2 + 7X + 1$ par $B = X^2 - 3X + 2$, on effectue les étapes suivantes :

— on élimine $3X^4$ en ajoutant le terme $3X^2$ au quotient, et on met à jour A en retranchant $3X^2 \times B$; A vaut maintenant $4X^3 - 4X^2 + 7X + 1$;
— on élimine $4X^3$ en ajoutant $4X$ au quotient, et on ajuste A qui devient $8X^2 - X + 1$;
— on élimine enfin $8X^2$ en ajoutant 8 au quotient, et on obtient le reste final $23X - 15$. Ainsi, la division de A par B donne un quotient $3X^2 + 4X + 8$ et un reste $23X - 15$.

1. Diviser avec le même algorithme $3X^4 + X^3 + 5X^2 + 3X + 4$ par $2X^2 + 2X + 6$, vus comme des polynômes de $\mathbb{F}_7$.
2. Écrire formellement l'algorithme ci-dessus.
3. Analyser sa complexité en nombre d'opérations sur les coefficients.

Exercice 2. *Algorithme de Gauss*

L'algorithme de Gauss est un algorithme classique de résolution de systèmes linéaires. On l'explique sur l'exemple (S_1) où tous les calculs sont faits *modulo* 11.

$$(S_1) = \begin{cases} 4x + 7y + 8z = 9 \\ 3x + 2y + z = 10 \\ 2x + 8y + 9z = 1 \end{cases}$$

— On cherche une équation où x apparaît (ici la première par exemple) et on l'utilise pour *éliminer* x des autres équations : on divise la première équation par 4, puis on la retranche 3 fois à la deuxième et 2 fois à la troisième. On obtient le nouveau système (S_2), équivalent à (S_1), dans lequel x n'apparaît plus que dans une équation.

$$(S_2) = \begin{cases} x + 10y + 2z = 5 \\ 5y + 6z = 6 \\ 10y + 5z = 2 \end{cases}$$

— On réitère le processus pour que y n'apparaisse que dans la deuxième équation et z que dans la troisième, c'est-à-dire qu'on construit les systèmes (S_3) et (S_4) équivalents à (S_1).

$$(S_3) = \begin{cases} x + z = 4 \\ y + 10z = 10 \\ 4z = 1 \end{cases} \qquad (S_4) = \begin{cases} x = 1 \\ y = 2 \\ z = 3 \end{cases}$$

— On vérifie bien que le dernier système obtenu donne la solution.

1. On considère un code de Reed-Solomon $[4, 2, 3]_5$: on considère donc des polynômes de degré < 2 évalués sur les 4 points d'évaluation 1, 2, 3 et 4 dans $\mathbb{F}_5$. On reçoit le mot $(0, 2, 1, 4)$. Retrouver le message envoyé. *Indication. Construire la matrice correspondante, résoudre le système grâce à l'algorithme de Gauss, puis retrouver F en divisant N par E.*
2. Estimer la complexité de l'algorithme de Gauss, en nombre d'opérations sur les coefficients.
3. Comment écrire en pratique l'algorithme de Gauss (structures de données, opérations élémentaires, ...) ?