IT_124 - TP numéro 0 : Les polynômes.

Rappels théoriques

On rappelle qu'un polynôme de degré n à coefficients dans un certain corps K (qui ici sera d'abord les réels $\mathbb{R}$ puis les rationnels $\mathbb{Q}$) est une fonction $K \to K$ de la forme

$$P(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 = \sum_{k=0}^{n} a_k x^k,$$

où $a_k \in K$ et $a_n \neq 0$. On a vu au cours que l'on peut additionner, soustraire, multiplier des polynômes, ainsi qu'effectuer des divisions euclidiennes (avec reste) :

$$\begin{array}{rrrrr|lll}
4x^4 & +2x^3 & -3x^2 & +6x & -1 & 2x^2 & -x & -1 \\
\cline{6-8}
-(4x^4 & -2x^3 & -2x^2) & & & 2x^2 & & \\
\cline{1-3}
 & 4x^3 & -x^2 & +6x & & & +2x & \\
 & -(4x^3 & -2x^2 & -2x) & & & & \\
\cline{2-4}
 & & x^2 & +8x & -1 & & & +\tfrac{1}{2} \\
 & & -(x^2 & -\tfrac{1}{2}x & -\tfrac{1}{2}) & & & \\
\cline{3-5}
 & & & \tfrac{17}{2}x & -\tfrac{1}{2} & & &
\end{array}$$

$2x^2 \cdot (2x^2 - x - 1) = 4x^4 - 2x^3 - 2x^2$

$2x \cdot (2x^2 - x - 1) = 4x^3 - 2x^2 - 2x$

$\frac{1}{2} \cdot (2x^2 - x - 1) = x^2 - \frac{1}{2}x - \frac{1}{2}$

Donc, $4x^4 + 2x^3 - 3x^2 + 6x - 1 = (2x^2 - x - 1) \cdot (2x^2 + 2x + \frac{1}{2}) + \frac{17}{2}x - \frac{1}{2}$.

De manière générale, on écrit :

$$A(x) = B(x) \cdot Q(x) + R(x), \text{ avec } \deg(R(x)) < \deg(B(x)).$$

On a également vu que si on se donne $n+1$ points du plan K^2 $(x_0, y_0), \ldots, (x_n, y_n)$, alors il y a un *unique* polynôme $L(x)$ de degré $\leq n$ qui passe par ces points, autrement dit pour lequel $L(x_k) = y_k$ pour $k = 0, \ldots, n$:

$$\ell_i(x) = \prod_{k=0, k\neq i}^{n} \frac{x - x_k}{x_i - x_k}, \qquad i = 0, 1, \ldots, n$$

$$L(x) = \sum_{i=0}^{n} y_i \cdot \ell_i(x)$$

Le but de ce TP est de se faire une petite librairie qui permet d'effectuer toutes ces opérations, dans un premier temps avec des coefficients réels (en utilisant les floats), puis avec des coefficients rationnels, en fabriquant une petite librairie qui permet de manipuler des fractions. Nous le ferons en Python 3.

Comment coder des polynômes

Le polynôme $P(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ sera codé sous la forme $[a_0, a_1, \ldots, a_n]$. *Attention* : on écrit les coefficients du plus petit au plus grand, et on veut que la liste soit de la bonne taille :
`[1,2,3,4]` représente bien le polynôme $4x^3 + 3x^2 + 2x + 1$,
`[1,2,3,4,0]` ne représente *pas* bien le polynôme $4x^3 + 3x^2 + 2x + 1$,
`[0,1,2,3,4]` représente bien le polynôme $4x^4 + 3x^3 + 2x^2 + x$.

De cette manière, le k-ième membre de la liste est le coefficient de x^k (les indices commencent à 0).

A faire : Partie I

Coder les fonctions suivantes pour des polynômes dont les coefficients sont des *floats* :

1. Addition de deux polynômes
2. Soustraction de deux polynômes
3. Multiplication de deux polynômes
4. Evaluation d'un polynôme en un point : étant donné une liste `P` correspondant au polynôme $P(x)$ et un nombre réel a (représenté par un float `a`), faire une fonction qui retourne la valeur $P(a)$.
5. Division euclidienne : étant donné deux polynômes sous forme de listes `A, B`, faire une fonction qui retourne les listes correspondant aux quotient et reste `Q, R`.
6. Polynôme de Lagrange : En utilisant les fonctions d'addition et de multiplication de polynômes, faire une fonction qui retourne la liste correspondant au polynôme de Lagrange $L(x)$ à partir d'une liste de paires de points `[ (x0,y0) , (x1,y1) , ... , (xn,yn) ]`.

A faire : Partie II

On veut utiliser des fractions $\frac{p}{q}$, que l'on codera sous la forme d'un couple d'entiers `(p,q)`, avec `q` différent de 0. On écrit un entier p comme $\frac{p}{1}$.
Coder les fonctions suivantes.

1. Etant donné deux entiers `p,q`, retourner leur PGCD.
2. A l'aide du PGCD, faire une fonction qui, étant donné une fraction `(p,q)`, retourne sa forme simplifiée. Par exemple, avec `(2,4)` en entrée, il faut retourner `(1,2)`.
3. Addition de deux fractions (avec l'aide de la fonction précédente).
4. Multiplication de deux fractions.
5. Division de deux fractions.

A faire : Partie III

Refaire les fonctions de la Partie I, mais pour des polynômes dont les coefficients sont des fractions, donc des couples d'entiers `(p,q)`. On utilisera bien sûr les fonctions de la Partie II pour effectuer les additions, soustractions, multiplications et divisions de fractions.

A faire en parallèle avec le TP de M. Eggenberg sur RSA : Partie IV

1. Coder l'algorithme d'Euclide étendu qui calcule les coefficients de Bezout de deux entiers a, b, c'est-à-dire trouver $u, v \in \mathbb{Z}$ tels que $a \cdot u + b \cdot v = \text{PGCD}(a, b)$.
2. Grâce aux coefficients de Bezout, coder une fonction qui donne l'inverse multiplicatif d'un entier a dans les entiers modulo un nombre premier p. Exemple : dans les entiers modulo 5, l'inverse multiplicatif de 4 est 4 (car $4 \cdot 4 = 16 \equiv 1 \mod 5$).
3. Coder le polynôme de Lagrange $L(x)$ comme dans les parties I et III, mais avec des coefficients dans les entiers modulo un premier p. Par exemple, $p = 17$. *Attention : dans ce cas, on ne peut pas avoir plus de p points.*