Université de Versailles – Saint-Quentin-en-Yvelines — Année 2012 – 2013
L2 – MA 350 — Automne

TD 8

Lancer Firefox et aller sur sagemath.ens.uvsq.fr. Se connecter sur Sage, et créer une nouvelle feuille sous le nom habituel. Commencer par rentrer la commande `automatic_names(True)`.
Vous devez mettre des commentaires pour indiquer tout ce qu'on fait.

Exercice 1 (Interpolation)**.** On va chercher à approcher une fonction f par des fonctions polynomiales.

1. On commence par la construction du polynôme interpolateur de Lagrange.
   a. Écrire une fonction Sage qui prend en entrée une liste de nombres $x_0, \dots, x_n$ distincts deux à deux, un entier $0 \leq i \leq n$ et qui renvoie un polynôme L_i de degré au plus n tel que $L_i(x_i) = 1$ et pour tout $j \neq i$, $L_i(x_j) = 0$. Tester votre fonction sur plusieurs exemples.
   b. En déduire une fonction Sage qui prend en entrée une liste de $n+1$ couples (x_i, y_i) distincts deux à deux et qui renvoie un polynôme L de degré au plus n tel que pour tout i, $L(x_i) = y_i$. Ce polynôme est appelé polynôme interpolateur de Lagrange.
   c. Votre choix de polynôme est-il le seul possible ?
   d. Trouver un exemple où le polynôme interpolateur passant par $n+1$ points est de degré $< n$.
2. Soit $f\colon [a,b] \longrightarrow \mathbb{R}$. Nous allons utiliser le polynôme interpolateur de Lagrange pour approcher f par des fonctions polynomiales.
   a. Écrire une fonction `distrib_reguliere` qui prend en argument a, b, n et qui renvoie la liste des $n+1$ réels qui permettent de découper l'intervalle $[a,b]$ en n sous-intervalles de même longueur.
   b. En utilisant la fonction `distrib_reguliere`, écrire une fonction qui prend en argument f, a, b et n et qui renvoie un polynôme de degré au plus n qui approche f sur l'intervalle $[a,b]$.
   c. Écrire une fonction prenant pour arguments une fonction f et une liste de nombres $x_0, \dots, x_n$ et qui renvoie la liste des points $(x_i, f(x_i))$ de manière à pouvoir les afficher sur un graphique (en utilisant la fonction `point`).
   d. Pour chacun des exemples suivants, on représentera sur un même graphe la fonction f, son approximation pour plusieurs valeurs de n et les points où f et son approximation coïncident :
   $$x \mapsto x^4 - x^2 + \frac{1}{10} \text{ sur } [-1,1]\,; \quad x \mapsto e^x \text{ sur } [0,1]\,; \quad x \mapsto \frac{1}{1+x^2} \text{ sur } [-5,5]\,.$$
   e. Pensez-vous qu'augmenter la valeur de n donne toujours une approximation plus précise ?
   f. Refaire les questions 2b et 2d en remplaçant `distrib_reguliere` par la fonction `distrib_chebychev`, qui renvoie la liste des $x_k = \dfrac{a+b}{2} - \dfrac{b-a}{2}\cos\left(\dfrac{(k+1/2)\,\pi}{n+1}\right)$, pour $0 \leq k \leq n$.

Exercice 2 (Instabilité numérique)**.** Dans cet exercice, nous allons perturber des matrices pour voir comment se propagent les erreurs d'arrondi. Soit H_n la matrice de Hilbert, qui a pour coefficients les $B_{ij} = 1/(i+j-1)$.

1. En choisissant des valeurs pour n, calculer l'inverse de H_n.
2. Soit $\widetilde{H}_n$ la matrice obtenue en tronquant chaque coefficient de H_n à 10^{-4}. Calculer $\widetilde{H}_n^{-1}$. Le résultat est-il très différent de H_n^{-1} ?
3. Soit b le vecteur dont la i-ème coordonnée est $(-1)^{i+1}$. Comparer la solution du système $H_n X = b$ avec celle du système $\widetilde{H}_n X = b$.

Exercice 3 (Calcul numérique d'intégrales)**.** On s'intéresse au calcul approché d'intégrales.

1. On commence par la méthode des rectangles.
   a. Rappeler en quoi consiste la méthode des rectangles pour calculer la valeur approchée d'une intégrale.
   b. Écrire une fonction qui prend en arguments f, a, b, n et qui renvoie une valeur approchée de $\displaystyle\int_a^b f(t)\,\mathrm{d}t$ calculée par la méthode des rectangles *à gauche* à n pas.
   c. Même question pour la méthode des rectangles à droite et au point milieu.
   d. Tester les trois fonctions précédentes sur différents exemples (par exemples avec des applications linéaires, polynomiales de degrés 2, $\cos\left(x^2+x+1\right)\mathrm{e}^{\pi/x}$, etc).
   e. Ces méthodes sont-elles exactes pour certains cas particuliers (on pourra penser aux cas «simples» des fonctions constantes, affines, polynomiales de degré 2, etc) ?

2. Mêmes questions en remplaçant la méthode des rectangles par la méthode des trapèzes. Comparer les résultats obtenus avec la méthode des rectangles au point milieu.
3. On va maintenant approcher f par interpolation. Soient $a < b$ et $m = (a+b)/2$.
   a. Soit P le polynôme interpolateur de Lagrange qui coïncide avec f en a, m et b. Montrer (éventuellement avec Sage) que $\displaystyle\int_a^b P(t)\,\mathrm{d}t = \frac{b-a}{6}\left(f(a) + 4f(m) + f(b)\right)$.
   b. En déduire une fonction prenant en arguments f, a, b et n et qui renvoie une valeur approchée de $\int_a^b f(d)\,\mathrm{d}t$ calculée en découpant $[a,b]$ en n sous-intervalles de même longueur et en remplaçant f par P sur chacun de ces sous-intervalles.
   c. Reprendre les exemples des questions précédentes. La méthode est-elle exacte dans certains cas ?

Exercice 4 (Loi de groupe sur une courbe elliptique)**.** On définit une courbe elliptique comme l'ensemble des solutions d'une équation de la forme $y^2 = x^3 + ax + b$ où $4a^3 + 27b^2 \neq 0$ pour des raisons techniques. Dans toute la suite, une courbe elliptique sera représentée par une liste `[a,b]`.

1. a. Écrire une fonction qui prend en entrée une liste `[a,b]` et qui renvoie `True` si $y^2 = x^3 + ax + b$ est une courbe elliptique, `False` sinon.
   b. Écrire une fonction qui prend en argument une liste `[a,b]` et qui renvoie une représentation graphique de la courbe $y^2 = x^3 + ax + b$ si c'est une courbe elliptique, une erreur sinon (on pourra utiliser `implicit_plot` en faisant varier x et y entre -5 et 5).
   c. Tester la fonction précédente pour visualiser les courbes elliptiques $y^2 = x^3 + x + 2$, $y^2 = x^3 - x + 2$, $y^2 = x^3 - 2x + 2$, $y^2 = x^3 - 2x + 1$ et $y^2 = x^3 - 2x$.
   d. Écrire une fonction qui prend en entrée un point et une courbe et renvoie `True` si le point est bien sur la courbe, `False` sinon. Tester cette fonction sur des exemples vérifiables à la main.
   e. En général, si on prend deux points P et Q « au hasard » sur une courbe elliptique et qu'on trace la droite (PQ), combien y a-t-il de points d'intersections avec la courbe ?
2. On se donne une courbe elliptique et on cherche à définir une addition $\oplus$ sur l'ensemble de ses points. On suppose que P et Q sont deux points de la courbe tels que la droite (PQ) rencontre la courbe elliptique en 3 points distincts, P, Q et R.
   a. Montrer que si on définit $P \oplus Q = R$ alors la loi $\oplus$ n'est pas associative.
   b. Vérifier sur des exemples qu'en revanche, en définissant $P \oplus Q$ comme le symétrique de R par rapport à l'axe des abscisses, la loi semble être associative. Peut-on le vérifier en toute généralité avec Sage ? L'addition ainsi définie est-elle commutative ?
   c. Écrire une fonction qui prend en arguments une courbe elliptique, deux points P et Q sur la courbe et qui renvoie le point $P \oplus Q$.
3. Comment peut-on définir « naturellement » le point $P \oplus P$? Cette définition est-elle toujours possible ? Écrire une fonction qui prend en entrée un point P tel que la définition précédente soit possible et qui renvoie le point $P \oplus P$.
4. Pour définir l'addition de deux points distincts qui forment une droite verticale ou pour calculer $P \oplus P$ pour P de coordonnées $(x_P, 0)$, on va rajouter un point à la courbe : en plus des points « normaux » de la courbe, on dit qu'on a un autre point « à l'infini », qu'on note $\mathcal{O}$. Comment est-il raisonnable de définir $\oplus$ dans les deux cas cités précédemment (on pourra faire des dessins…) ?
5. Soit P un point de la courbe. Que vaut $P \oplus \mathcal{O}$ (on pourra encore faire des dessins…) ?
6. En utilisant ce qui précède, compléter la fonction de la question 2c pour qu'elle prennent en compte tous les cas possibles.
7. L'opposé d'un point P est un point Q tel que $P \oplus Q = Q \oplus P = \mathcal{O}$. On note alors $Q = -P$. Soit P un point de la courbe, de coordonnées (x_P, y_P). Quelle sont les coordonnées de $-P$?
8. Écrire une fonction *récursive* prenant en entrée une courbe elliptique, $k \in \mathbb{N}^*$ et P sur la courbe et qui renvoie $kP = \underbrace{P \oplus \cdots \oplus P}_{k \text{ fois}}$. Elle devra donner la réponse en temps raisonnable pour k de l'ordre de 500.
9. a. Soit p un nombre premier et $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ le corps fini à p éléments. À l'aide d'exemples, conjecturer la valeur de x^{p-1} pour $x \in \mathbb{F}_p$. Pouvez-vous prouver ce résultat avec des outils de terminale S ?
   b. Montrer que si $x \in \mathbb{F}_p$ est un carré alors $x^{\frac{p-1}{2}} = 1$.
   c. On suppose $p \equiv 3 \mod 4$. Montrer que si $x \in \mathbb{F}_p$ est un carré alors $x^{\frac{p+1}{4}}$ est une racine carrée de x.
   d. En déduire une fonction qui prend une courbe et un nombre premier $p \equiv 3 \mod 4$ et qui renvoie un point de cette courbe.
10. Peut-on utiliser ce qui précède pour mettre en place un échange de clés Diffie-Hellman ?