Examen de M.A.O. Calcul Formel Durée : 3 heures

Juin 2020
Master 1 M.F., Orsay

Suite à l'épidémie de Covid-19, cette épreuve a lieu à distance. Les modalités sont donc différentes de celles d'un examen habituel, mais le sujet et le barême sont conçus comme si il s'agissait d'un examen dans des conditions normales.

Tous les documents sont autorisés (y compris le poly, les vidéos, les TP, ..., et évidemment le livre "Calcul mathématique avec Sage"). Il est interdit de communiquer. Au plus tard le mardi 16 juin à 20 heures vous devez m'envoyer un mail avec votre copie (scannée ou prise en photo). Vérifiez bien que l'image soit nette, et facilement lisible. Vous devez joindre à ce mail le fichier Notebook qui contient les calculs que vous aurez effectués en Sage. Cette feuille de calcul sera corrigée en même temps que votre copie ; il est donc conseillé de commenter raisonnablement vos programmes, et de veiller à leur lisibilité. Vous pouvez bien sûr créer des feuilles de calcul auxiliaires, qui ne seront pas corrigées et peuvent vous servir de brouillon électronique.

Cet examen est une épreuve de mathématiques. Avant d'utiliser l'ordinateur, il convient de se demander s'il n'est pas possible d'obtenir par un raisonnement simple ce qui pourrait être obtenu par un calcul plus complexe fait par ordinateur. A titre indicatif, dans les questions signalées par le signe ($\star$), on s'attend à une réponse utilisant de façon essentielle l'ordinateur ; pour les autres, on s'attend davantage à une réponse argumentée, utilisant éventuellement l'ordinateur mais de façon plus marginale.

Les modalités d'utilisation de Sage sont les suivantes. Pour cet examen, vous pouvez utiliser toutes les fonctions implémentées dans Sage (sauf mention explicite du contraire). Il est inutile de recopier sur votre copie les lignes de code Sage que vous avez utilisées, puisque vous m'enverrez votre code par email. En revanche vous *devez* inscrire sur votre copie le résultat du calcul, et toutes les explications utiles (notamment toute justification mathématique de la façon dont vous avez fait votre programme). Vous devez aussi, le cas échéant, faire le lien dans votre copie entre le résultat brut donné par Sage et l'interprétation mathématique qui vous est demandée.

En tout état de cause n'hésitez pas à me poser des questions par email si les consignes ne sont pas claires, ou si vous n'êtes pas sûr de bien comprendre une des questions.

Cet examen est constitué de deux problèmes indépendants. Lorsqu'on évoquera le coût d'un algorithme, il s'agira toujours de son coût en nombre d'opérations arithmétiques (dans $\mathbb{Z}$,

$\mathbb{Q}$ ou un corps fini selon le contexte). On ne cherchera *jamais* à calculer exactement le nombre d'opérations arithmétiques utilisées : la réponse attendue est toujours de la forme $O(\ldots)$ où les points de suspension désignent une fonction simple du (ou des) paramètre(s) du problème. Calculer la constante implicite dans le symbole O ne fait pas partie de la question posée.

Problème 1

Ce problème est consacré au théorème suivant, dont on va donner une preuve constructive et des applications.

Théorème 1 *Soit $n \geq 1$ un entier impair. Alors il existe un unique polynôme $V_n \in \mathbb{Z}[X]$ de degré inférieur ou égal à $\frac{n-1}{2}$ tel que*

$$X^{\frac{n-1}{2}} V_n\Big(X + \frac{1}{X}\Big) = \sum_{i=0}^{n-1} X^i. \tag{1}$$

Notons $V_n(X) = \sum_{j=0}^{(n-1)/2} a_j X^j$ et posons $\kappa_i = \frac{n-1}{2} - i$ pour tout $i \in \mathbb{Z}$.

1. Démontrer que la relation (1) est vérifiée si, et seulement si, on a

$$\sum_{\substack{|\kappa_i| \leq j \leq \frac{n-1}{2} \\ j \equiv \kappa_i \bmod 2}} \binom{j}{(2(i+j) - n + 1)/4} a_j = 1 \text{ pour tout } i \in \{0, \ldots, n-1\}.$$

2. Déduire de la question précédente une preuve du théorème 1, et un algorithme permettant de calculer V_n à partir de n. Quel est le coût de cet algorithme en nombre d'opérations arithmétiques dans $\mathbb{Q}$?
3. ($\star$) Implémenter l'algorithme de la question précédente sous la forme d'une fonction Sage qui prend en entrée un entier impair $n \geq 1$ et renvoie le polynôme V_n. *On pourra utiliser la fonction Sage* `binomial(n,k)`, *qui renvoie le coefficient binomial* $\binom{n}{k}$.
4. ($\star$) En utilisant la fonction définie à la question précédente, calculer V_{11}.

Soit p un nombre premier impair. Pour tout entier impair $n \geq 1$ on note $V_{n,p} \in (\mathbb{Z}/p\mathbb{Z})[X]$ le polynôme obtenu à partir de V_n en réduisant modulo p chaque coefficient.

5. Démontrer que $V_{n,p}$ est de degré $\frac{n-1}{2}$.
6. Démontrer que $V_{n,p}(2) = \overline{n}$ où $\overline{n}$ est la classe de n modulo p.
7. Soient $\mathbb{K}$ une extension de $\mathbb{F}_p$, et $x \in \mathbb{K}$ tel que $\sum_{i=0}^{p-1} x^i = 0$. Démontrer que $x = 1$.
8. En utilisant la question précédente, démontrer que $V_{p,p}(X) = (X-2)^{(p-1)/2}$.
9. Soit q un nombre premier impair. Démontrer que $\mathrm{Res}(V_{p,p}, V_{q,p}) = \overline{q}^{(p-1)/2}$ où $\overline{q}$ est la classe de q modulo p.

10. Soient $a, b \geq 1$ deux entiers impairs, premiers entre eux. Démontrer que $\mathrm{Res}(V_{a,\ell}, V_{b,\ell}) \neq 0$ pour tout nombre premier ℓ, et en déduire que $\mathrm{Res}(V_a, V_b) \in \{-1, 1\}$.

Considérons désormais deux nombres premiers impairs distincts p et q. On appelle *symbole de Legendre* la quantité, notée $\left(\frac{q}{p}\right)$, qui vaut 1 si la classe de q modulo p est un carré dans $\mathbb{Z}/p\mathbb{Z}$, et qui vaut -1 sinon. On admet que dans les deux cas on a $\left(\frac{q}{p}\right) \equiv q^{(p-1)/2} \bmod p$. Bien entendu on définit $\left(\frac{p}{q}\right)$ de façon analogue, en permutant p et q. *Dans ce sujet, aucune autre connaissance sur le symbole de Legendre n'est utile.*

11. Démontrer que $\mathrm{Res}(V_p, V_q) = \left(\frac{q}{p}\right)$.
12. En déduire l'égalité suivante, appelée *loi de réciprocité quadratique* :

$$\left(\frac{q}{p}\right) \cdot \left(\frac{p}{q}\right) = (-1)^e \text{ avec } e = \frac{(p-1)(q-1)}{4}.$$

13. On déduit des questions précédentes deux algorithmes de calcul de $\left(\frac{q}{p}\right)$: l'un fondé sur la question 11 qui le ramène à un calcul de résultant, et l'autre fondé sur la relation $\left(\frac{q}{p}\right) \equiv q^{(p-1)/2} \bmod p$ (sachant que $\left(\frac{q}{p}\right) \in \{-1, 1\}$). Comparer les complexités de ces deux algorithmes en précisant bien dans quels ensembles ont lieu les opérations que l'on compte.
14. ($\star$) Implémenter en Sage deux fonctions qui calculent le symbole de Legendre $\left(\frac{q}{p}\right)$, chacune suivant l'un des deux algorithmes évoqués à la question précédente. *Toutes les fonctions présentes dans Sage peuvent être utilisées ici, il n'est pas demandé de les reprogrammer – sauf bien sûr celle qui calcule directement le symbole de Legendre !* Mesurer les temps de calcul et illustrer la comparaison effectuée à la question précédente.

Problème 2

Dans ce problème on fixe un nombre premier p et un entier $d \geq 1$; on note $q = p^d$ et on travaille dans un corps à q éléments, noté $\mathbb{F}_q$. Soit $P \in \mathbb{F}_q[X]$ un polynôme de degré $n \geq 1$.

1. Démontrer que P est irréductible dans $\mathbb{F}_q[X]$ si, et seulement si, on a $\mathrm{pgcd}(P(X), X^{q^k} - X) = 1$ pour tout entier k tel que $1 \leq k \leq \frac{n}{2}$.

On déduit de la question 1 un algorithme pour tester l'irréductibilité de P, en calculant $\mathrm{pgcd}(P(X), X^{q^k} - X)$ pour k allant de 1 à la partie entière de $n/2$.

2. En utilisant directement ce qui a été vu en cours, calculer le coût de cet algorithme en nombre d'opérations arithmétiques dans $\mathbb{F}_q$. Semble-t-il raisonnable de l'utiliser si $q = 19$ et $n = 40$?

3. Montrer que la première étape de l'algorithme classique de calcul de $\mathrm{pgcd}(P(X), X^{q^k} - X)$ peut être réalisée de façon différente (en tirant profit du fait que l'un des polynômes est de la forme $X^{q^k} - X$). Calculer le coût de cet algorithme modifié, en nombre d'opérations arithmétiques dans $\mathbb{F}_q$. Peut-on maintenant l'utiliser si $q = 19$ et $n = 40$?

Notons $\mathcal{E}_{q,n}$ l'ensemble des polynômes $P \in \mathbb{F}_q[X]$ unitaires de degré n pour lesquels il existe une extension $\mathbb{K}$ de $\mathbb{F}_q$, de degré n, et une racine x de P dans $\mathbb{K}$ telle que x soit un générateur du groupe cyclique $\mathbb{K}^*$.

4. Soit $P \in \mathcal{E}_{q,n}$. Démontrer que P est irréductible dans $\mathbb{F}_q[X]$, et que dans une extension $\mathbb{K}$ de $\mathbb{F}_q$ de degré n, toutes ses racines sont des générateurs du groupe cyclique $\mathbb{K}^*$.
5. ($\star$) Démontrer que $X^4 + X + 1$ appartient à $\mathcal{E}_{2,4}$. *Dans cette question comme dans les suivantes, la réponse attendue combine des calculs en Sage et des arguments théoriques. Vous écrirez donc sur votre copie toute la partie théorique, notamment les résultats que vous donne Sage et l'interprétation que vous en faites.*
6. ($\star$) Démontrer que $X^4 + X^2 + X + 1$ n'appartient pas à $\mathcal{E}_{2,4}$.

Dans les deux questions qui suivent, on s'intéresse à des polynômes de degré 2 sur $\mathbb{F}_4$.

7. ($\star$) Faire la liste des polynômes irréductibles unitaires de degré 2 sur $\mathbb{F}_4$; combien y en a-t-il ? *Pour cette question uniquement, il est interdit d'utiliser la fonction de Sage qui teste si un polynôme est irréductible.*
8. ($\star$) Parmi les polynômes irréductibles unitaires de degré 2 sur $\mathbb{F}_4$, faire la liste de ceux qui appartiennent à $\mathcal{E}_{4,2}$. Combien y en a-t-il ?
9. Déterminer, en fonction de q et n, le cardinal de l'ensemble $\mathcal{E}_{q,n}$. Vérifier la cohérence du résultat obtenu avec le cas particulier de la question précédente.
10. Proposer un algorithme qui teste si un polynôme unitaire $P \in \mathbb{F}_q[X]$ de degré n appartient ou non à $\mathcal{E}_{q,n}$. Calculer le coût de cet algorithme en nombre d'opérations arithmétiques dans $\mathbb{F}_q$.
11. ($\star$) Implémenter l'algorithme de la question précédente sous la forme d'une fonction Sage, et l'appliquer aux exemples précédents.