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

Lundi 18 juin 2018
Master 1 M.F.A., Orsay

L'accès à internet et l'utilisation des téléphones portables sont interdits. Les documents et notes de cours sont interdits, à l'exception du livre "Calcul mathématique avec Sage". En revanche l'aide de Sage et une version pdf de ce livre sont disponibles sur les ordinateurs.

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 ont changé par rapport au partiel. Il est maintenant inutile de recopier sur votre copie les lignes de code Sage que vous avez utilisées. 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.
Vous disposez d'une feuille de calcul Sage nommée `copie-examen-NUMERO.ipynb`. Vous devez remplacer NUMERO par le numéro d'anonymat de votre copie d'examen, aussi bien dans le nom de ce fichier qu'en tête du fichier lui-même. 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 créer des feuilles de calcul auxiliaires, *qui ne seront pas corrigées* et peuvent vous servir de brouillon électronique. En tout état de cause veuillez suivre attentivement les consignes qui vous seront données pendant l'épreuve, et en cas de doute n'hésitez pas à poser des questions.

Le sujet est composé de trois exercices indépendants. Il est possible d'admettre le résultat de certaines questions pour traiter les suivantes.

Notamment dans l'exercice 1, mais aussi dans les autres exercices, l'utilisation de l'informatique et les raisonnements mathématiques sont parfois mêlés dans une même question. Une question notée $(\star)$ peut nécessiter des arguments mathématiques (qui doivent alors être rédigés avec soin), et une question ne portant pas le symbole $(\star)$ est susceptible d'utiliser quand même un peu d'informatique.

Exercice 1.

Considérons les deux polynômes suivants dans $\mathbb{Q}[X, Y]$:

$$A(X, Y) = 2XY^2 + 4XY + 5 \qquad \text{et} \qquad B(X, Y) = XY - X - 1.$$

On note $\mathcal{C}$ l'ensemble des couples $(x, y) \in \mathbb{C}^2$ tels que $A(x, y) = B(x, y) = 0$, et $R \in \mathbb{Q}[X]$ le résultant de A et B vus dans $(\mathbb{Q}[X])[Y]$.

1. ($\star$) Calculer R, et le factoriser dans $\mathbb{Q}[X]$. *On pourra utiliser la fonction* `R.factor()` *de Sage, dans cette question et dans toute la suite de l'exercice.*

2. Démontrer que pour tout $(x, y) \in \mathcal{C}$ on a $R(x) = 0$. Comment peut-on énoncer cette propriété en termes géométriques ?

3. ($\star$) En étudiant la réciproque de la question 2, déterminer l'ensemble des couples (x, y) appartenant à $\mathcal{C}$.

4. Existe-t-il une racine x de R qui n'est l'abscisse d'aucun point de $\mathcal{C}$? Si oui, expliquer ce phénomène.

5. ($\star$) Calculer et factoriser le résultant de A et B vus dans $(\mathbb{Q}[Y])[X]$. Le phénomène de la question 4 se produit-il, et pourquoi ?

Exercice 2.

Dans cet exercice on considère le polynôme $P = X^6 + X + 1 \in \mathbb{F}_2[X]$.

1. Sans utiliser l'ordinateur, donner la liste des polynômes de $\mathbb{F}_2[X]$ de degré 2 en précisant pour chacun si il est irréductible ou pas.

2. Donner la liste des polynômes irréductibles de $\mathbb{F}_2[X]$ de degré 3 ; dans cette question également, l'utilisation de l'ordinateur est interdite.

3. ($\star$) Démontrer que P est irréductible en utilisant les deux questions précédentes, et bien sûr sans utiliser la fonction de Sage qui teste l'irréductibilité d'un polynôme.

Dans toute la suite de l'exercice on note $\mathbb{K}$ un corps de rupture de P sur $\mathbb{F}_2$, et $a \in \mathbb{K}$ une racine de P.

4. Quel est le degré de $\mathbb{K}$ sur $\mathbb{F}_2$? Quel est le cardinal de $\mathbb{K}$?

5. Combien $\mathbb{K}$ admet-il de sous-corps ? Donner le cardinal de chacun d'entre eux.

6. ($\star$) Exprimer a^{21} dans la base $(1, a, a^2, \ldots, a^5)$ et démontrer que $\mathbb{F}_2(a^{21})$ est de cardinal 4.

7. ($\star$) Déterminer le cardinal de $\mathbb{F}_2(b)$, où $b = a + a^8$.

8. Faire la synthèse des questions précédentes en donnant, pour chaque sous-corps de $\mathbb{K}$, une écriture sous la forme $\mathbb{F}_2(x)$ avec $x \in \mathbb{K}$.

Notons R le polynôme minimal de a sur $\mathbb{F}_2(b)$.

9. Démontrer que R est de degré 2.

10. ($\star$) Déterminer R. *On s'interdit dans cette question d'utiliser la commande de Sage qui fournit directement le polynôme minimal d'un élément sur un corps. Par ailleurs on écrira les coefficients de R comme des polynômes de degré au plus 2 en b à coefficients dans $\mathbb{F}_2$.*

Exercice 3.

Considérons, pour $n \geq 1$ entier, la propriété $\mathcal{P}(n)$ suivante :

$$n^{17} + 9 \text{ et } (n+1)^{17} + 9 \text{ sont premiers entre eux.}$$

1. ($\star$) Vérifier que $\mathcal{P}(n)$ est vraie pour tout entier $n \leq 10^5$.

2. Etant donné un entier n, comment peut-on déterminer efficacement si $\mathcal{P}(n)$ est vraie ? Quel est le coût de ce calcul en nombre d'opérations arithmétiques dans $\mathbb{Z}$?

3. Pour N donné, on aimerait déterminer si $\mathcal{P}(n)$ est vraie pour $n = 1, 2, \ldots, N$. Quel est le coût de ce calcul en nombre d'opérations arithmétiques dans $\mathbb{Z}$? Si on dispose du temps nécessaire pour effectuer 10^{12} opérations arithmétiques dans $\mathbb{Z}$, jusqu'à quelle valeur de N (en ordre de grandeur) pourra-t-on vérifier que $\mathcal{P}(n)$ est vraie ?

4. On admet que $\mathcal{P}(n)$ est vraie pour tout $n \leq N$, où N est l'entier de la question 3. Seriez-vous enclin à conjecturer que $\mathcal{P}(n)$ est vraie pour tout n ? *Cette question ne sera pas notée, donc soyez honnête et ne lisez pas les questions suivantes !*

Dans la suite de cet exercice on note p le résultant des polynômes $X^{17} + 9$ et $(X+1)^{17} + 9$.

5. ($\star$) Calculer p, et recopier sur la copie les 5 premiers chiffres de son écriture décimale.

6. On répète 100 fois le test suivant : pour un entier a choisi au hasard entre 0 et $p-1$, on teste si $a^p - a$ est divisible par p. On dit que le test a réussi si parmi les 100 entiers il y en a au moins un pour lequel $a^p - a$ n'est pas divisible par p. Si le test a réussi, que peut-on conclure ?

7. ($\star$) Programmer le test de la question 6. Réussit-il ?

8. En ordre de grandeur, combien doit-on effectuer d'opérations arithmétiques dans $\mathbb{Z}$ (additions, multiplications, soustractions, divisions) pour mener à bien le test de la question 6 ? *On rappelle que l'entier p est toujours celui de la question 5.*

On admet désormais que p est un nombre premier (ce que Sage permet de vérifier immédiatement).

9. Démontrer que si $\mathcal{P}(n)$ est fausse alors p divise $n^{17} + 9$ et $(n+1)^{17} + 9$.

10. Démontrer que $\mathcal{P}(n)$ est fausse pour une infinité d'entiers n.

11. ($\star$) Déterminer l'ensemble des entiers n pour lesquels $\mathcal{P}(n)$ est fausse.