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

Lundi 12 juin 2017
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.
Dans tous les cas, si vous utilisez l'ordinateur, vous devez recopier les lignes de code Sage que vous avez utilisées (en faisant attention à l'indentation), et ce que leur exécution a renvoyé ; il est également indispensable d'expliquer les calculs que vous faites faire à l'ordinateur. En cas de doute n'hésitez pas à poser des questions pendant l'épreuve.

Le sujet comporte 3 pages. Il est composé d'un exercice et d'un problème, qui sont indépendants. Il est possible d'admettre le résultat de certaines questions pour traiter les suivantes.

Exercice.

Dans cet exercice, les questions marquées avec le symbole $(\star)$ appellent une réponse qui combine une démonstration rigoureuse et un calcul effectué avec Sage.

Notons $\mathcal{C}_1$ l'ensemble des couples $(x, y) \in \mathbb{C}^2$ tels qu'il existe $t \in \mathbb{C}$ vérifiant

$$\begin{cases} x^2 &= 2(2t-1)t \\ y^2 &= 2(2t-1)(1-t) \end{cases} \tag{1}$$

1. $(\star)$ Déterminer un polynôme $R \in \mathbb{Q}[X, Y]$ tel que $\mathcal{C}_1$ soit l'ensemble des couples $(x, y) \in \mathbb{C}^2$ tels que $R(x, y) = 0$.

2. Démontrer que pour $(x, y) \in \mathbb{R}^2$ on a $R(x, y) = 0$ si, et seulement si, il existe $t \in \mathbb{R}$ vérifiant le système (1).

On note $S = X^2 - Y^2 - \frac{2}{9} \in \mathbb{Q}[X, Y]$ et on définit $\mathcal{C}_2$ comme étant l'ensemble des $(x, y) \in \mathbb{C}^2$ tels que $S(x, y) = 0$.

3. $(\star)$ Déterminer un polynôme $P \in \mathbb{Q}[Y]$ tel que pour tout $y \in \mathbb{C}$, on ait $P(y) = 0$ si et seulement s'il existe $x \in \mathbb{C}$ tel que $(x, y) \in \mathcal{C}_1 \cap \mathcal{C}_2$.

4. Déterminer les couples (x, y) de réels appartenant à $\mathcal{C}_1 \cap \mathcal{C}_2$.

Problème. Le but de ce problème est de donner un algorithme efficace d'extraction de racines carrées dans $\mathbb{F}_p$. On note p un nombre premier impair.

Partie 1 : Détection des carrés

1. Soient $\mathbb{K}$ un corps, x un élément de $\mathbb{K}$, et n un entier naturel. Quelle méthode efficace permet de calculer x^n ? *On demande seulement le nom de cet algorithme, pas son principe.* Quel est, en fonction de n, son coût en opérations arithmétiques (additions, multiplications, divisions) dans $\mathbb{K}$?

2. Soit x un élément non nul de $\mathbb{F}_p$. Démontrer que x est un carré dans $\mathbb{F}_p$ si, et seulement si, on a $x^{\frac{p-1}{2}} = 1$.

3. En déduire un algorithme permettant de tester si un élément $x \in \mathbb{F}_p^*$ est un carré. Quel est le coût de cet algorithme en opérations arithmétiques dans $\mathbb{F}_p$?

4. ($\star$) Implémenter l'algorithme de la question 3 sous la forme d'une fonction nommée `detection` qui prend en entrée un nombre premier impair p et un élément $x \in \mathbb{F}_p$, et renvoie 0 si $x = 0$, 1 si x est un carré non nul, et -1 si x n'est pas un carré. On pourra utiliser la commande $**$ pour calculer des puissances : il n'est pas demandé d'implémenter l'algorithme de la question 1.

Partie 2 : Construction d'un polynôme irréductible

5. Soient $\mathbb{K}$ un corps de caractéristique différente de 2, et $P = aX^2+bX+c$ un polynôme de degré 2 (avec $a, b, c \in \mathbb{K}$ et $a \neq 0$). Notons $\Delta = b^2 - 4ac$ son discriminant. Démontrer que :

   (i) Si Δ n'est pas un carré dans $\mathbb{K}$ alors P n'a aucune racine dans $\mathbb{K}$.

   (ii) Si $\Delta = 0$ alors P a une racine double dans $\mathbb{K}$, qu'on explicitera.

   (iii) Si Δ est un carré non nul dans $\mathbb{K}$ alors P a deux racines distinctes dans $\mathbb{K}$, qu'on déterminera.

6. Soient $u, a \in \mathbb{F}_p$. Démontrer que le polynôme $X^2 + uX + a$ est irréductible dans $\mathbb{F}_p[X]$ si, et seulement si, $u^2 - 4a$ n'est pas un carré dans $\mathbb{F}_p$.

7. ($\star$) En utilisant la question précédente et la fonction `detection` de la question 4, implémenter une fonction nommée `construction` qui prend en entrée un nombre premier impair p et un élément $a \in \mathbb{F}_p$, et renvoie un élément $u \in \mathbb{F}_p$ tel que $X^2 + uX + a$ soit irréductible dans $\mathbb{F}_p[X]$. On procèdera en choisissant u aléatoirement, autant de fois que nécessaire, jusqu'à trouver une valeur qui convienne.

8. (⋆) En appliquant la fonction `construction` implémentée à la question précédente, déterminer un élément $u \in \mathbb{F}_{13}$ tel que le polynôme $X^2 + uX + 5$ soit irréductible dans $\mathbb{F}_{13}[X]$.

Partie 3 : Calculs dans une extension

Dans cette partie on se donne $a, u \in \mathbb{F}_p$ tels que :

- a est un carré non nul dans $\mathbb{F}_p$;
- le polynôme $P(X) = X^2 + uX + a$ est irréductible dans $\mathbb{F}_p[X]$.

On note $\mathbb{K} = \mathbb{F}_p[T]/(T^2 + uT + a)$ le corps de rupture de P sur $\mathbb{F}_p$, et $t \in \mathbb{K}$ la classe du polynôme $T \in \mathbb{F}_p[T]$.

9. Démontrer que t et t^p sont les deux racines de P dans $\mathbb{K}$, et qu'elles sont distinctes.

10. En déduire que $t^{p+1} = a$, puis exhiber un entier k tel qu'en posant $b = t^k$ on ait $b^2 = a$. Pourquoi b est-il un élément de $\mathbb{F}_p$?

11. (⋆) En utilisant la question précédente et les fonctions `detection` et `construction` des questions 4 et 7, implémenter une fonction nommée `racinecarree` qui prend en entrée un nombre premier impair p et un élément $a \in \mathbb{F}_p$, et renvoie un élément $b \in \mathbb{F}_p$ tel que $b^2 = a$ si il en existe, et 0 sinon.

12. (⋆) En utilisant la fonction `racinecarree` de la question précédente et en admettant que $p_0 = 2^{17} - 1$ est premier, déterminer un entier b compris entre 1 et $p_0/2$ tel que $b^2 \equiv 80975 \bmod p_0$.

Partie 4 : Complexité

13. Pour tout $t \in \mathbb{F}_p^*$ on note H_t l'ensemble des couples $(x, y) \in \mathbb{F}_p^2$ tels que $x^2 - y^2 = t$. Démontrer que $\operatorname{Card} H_t = p - 1$.

14. Soit t un carré non nul de $\mathbb{F}_p$. En utilisant la question précédente, démontrer que l'ensemble des $x \in \mathbb{F}_p$ tels que $x^2 - t$ soit un carré de $\mathbb{F}_p$ est de cardinal $\frac{p+1}{2}$.

15. Soit a un carré non nul de $\mathbb{F}_p$. En utilisant la question précédente, démontrer que la fonction `construction` de la question 7 termine presque sûrement, et déterminer son coût en nombres d'opérations arithmétiques dans $\mathbb{F}_p$ dans 99 cas sur 100. En déduire, dans les mêmes conditions, le coût de la fonction `racinecarree` de la question 11.