

19 juin 2019
Master 1 M.F., Orsay

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

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 sont les suivantes. Il est 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_COPIE.ipynb`. Vous devez remplacer `NUMERO_COPIE` par le numéro d'anonymat qui figure sur votre copie, 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.

Quand on demande le coût d'un calcul, la réponse attendue est *toujours* de la forme $O(\dots)$.

Cet examen est constitué de deux exercices et d'un problème, tous indépendants.

Exercice 1

Notons $\mathcal{C}$ l'ensemble des couples $(x, y) \in \mathbb{C}^2$ pour lesquels il existe $t \in \mathbb{C} \setminus \{-i, i\}$ vérifiant :

$$\begin{cases} x = t^2 + t + 1 \\ y = \frac{t^2-1}{t^2+1} \end{cases} \tag{1}$$

1. ($\star$) Combien y a-t-il de points $(x, y) \in \mathcal{C}$ tels que $2xy^2 + x + 5y = 0$?

2. ($\star$) Déterminer un polynôme $P \in \mathbb{Q}[X, Y]$ tel que pour tout couple $(x, y) \in \mathbb{C}^2$ on ait l'équivalence suivante : $(x, y) \in \mathcal{C}$ si, et seulement si, $P(x, y) = 0$. *Dans cette question on attend à la fois un calcul avec Sage et une justification mathématique précise et rigoureuse.*
3. Notons $\mathcal{C}'$ l'ensemble des couples $(x, y) \in \mathbb{R}^2$ pour lesquels il existe $t \in \mathbb{R}$ vérifiant le système (1). Démontrer que pour tout couple $(x, y) \in \mathbb{R}^2$ on a : $(x, y) \in \mathcal{C}'$ si, et seulement si, $P(x, y) = 0$.

Exercice 2

Dans cet exercice on fixe un entier $m \geq 2$ et on considère le polynôme

$$T(X) = \sum_{i=0}^{m-1} X^{2^i} = X + X^2 + X^4 + X^8 + \ldots + X^{2^{m-1}} \in \mathbb{F}_2[X].$$

1. Soit $\mathbb{K}$ un corps de caractéristique 2. Démontrer que l'application $\mathbb{K} \to \mathbb{K}$, $x \mapsto T(x)$ est $\mathbb{F}_2$-linéaire.
2. Démontrer que dans $\mathbb{F}_2[X]$ on a $T(X)(1 + T(X)) = X^{2^m} + X$.

Dans la suite de cet exercice on s'intéresse au corps fini $\mathbb{F}_{2^m}$, où l'entier m a été utilisé dans la définition de T.

3. En utilisant ce qui précède, démontrer que pour tout $x \in \mathbb{F}_{2^m}$ on a $T(x) \in \mathbb{F}_2$, puis que pour tout $i \in \mathbb{F}_2$ on a :

$$\text{Card}\{x \in \mathbb{F}_{2^m},\ T(x) = i\} = 2^{m-1}.$$

4. Soit $x \in \mathbb{F}_{2^m}$; notons P le polynôme minimal de x sur $\mathbb{F}_2$.
   (a) Quelle relation a-t-on entre m et $\deg P$?
   (b) Supposons que $\deg P = m$. Démontrer que le coefficient de degré $m - 1$ de P est $T(x)$.
   (c) Notons $d = \deg P$; on ne suppose plus que $d = m$. Exprimer $T(x)$ en fonction du coefficient de degré $d - 1$ de P, de m et de d.
   (d) *Question facultative, non notée.* Pourquoi noter T ce polynôme ?

Problème

L'objectif de ce problème est de donner (sous une hypothèse simplificatrice) un algorithme de calcul du pgcd de deux polynômes de $\mathbb{Z}[X]$.

Partie 1

Dans cette partie on fixe un entier $q = p^\alpha$, avec p premier et $\alpha \in \mathbb{N}^*$. On note $\mathbb{F}_q$ un corps fini de cardinal q et on se donne $A, B \in \mathbb{F}_q[X]$ non nuls.

1. Rappeler le nom de l'algorithme classique qui permet de calculer le pgcd de A et B, ainsi que son coût en nombre d'opérations arithmétiques dans $\mathbb{F}_q$. *Dans cette question, aucune justification n'est demandée, et on ne demande pas non plus comment fonctionne cet algorithme.*
2. ($\star$) Programmer une fonction qui prend $A, B \in \mathbb{F}_q[X]$ en arguments et renvoie le pgcd de A et B. *On implémentera l'algorithme de la question 1, et on s'interdira évidemment d'utiliser ici la commande de Sage qui calcule directement le pgcd. Le pgcd n'étant défini qu'à association près, toute fonction renvoyant l'un des pgcd est admise.*
3. Dans cette question on considère le polynôme $P(Y) = Y^4 + 5Y + 1 \in \mathbb{F}_{13}[Y]$.
   (a) ($\star$) En utilisant simplement une fonction adéquate de Sage, vérifier que P est irréductible.
   (b) Quel est le cardinal du corps $\mathbb{K} = \mathbb{F}_{13}[Y]/(P)$?
   (c) ($\star$) Notons $y \in \mathbb{K}$ la classe de Y modulo (P), et considérons les éléments
   $$A(X) = X^4 - X^2 - y^2 - y \quad \text{et} \quad B(X) = X^4 - (y+3)X^2 + 2y + 2$$
   de $\mathbb{K}[X]$. Déterminer le pgcd de A et B en appliquant la fonction programmée à la question 2, et aussi avec la commande de Sage qui calcule directement le pgcd. Obtient-on le même résultat ? Si non, pourquoi ?

Partie 2

Dans cette partie on note $\mathcal{P}$ l'ensemble des polynômes irréductibles de $\mathbb{Z}[X]$ dont le coefficient dominant est strictement positif. On rappelle que tout polynôme $S \in \mathbb{Z}[X]$ non nul admet une écriture, unique à l'ordre près des facteurs, sous la forme $\varepsilon P_1^{\alpha_1} \dots P_r^{\alpha_r}$ avec $\varepsilon \in \{-1, 1\}$, $r \geq 0$, $P_1, \dots, P_r \in \mathcal{P}$ deux à deux distincts, et $\alpha_1, \dots, \alpha_r \in \mathbb{N}^*$. En posant $v_S(P) = \alpha_i$ si $P = P_i$ pour un certain indice i, et $v_S(P) = 0$ pour tout $P \in \mathcal{P} \setminus \{P_1, \dots, P_r\}$, on peut écrire cette décomposition sous la forme $S = \varepsilon \prod_{P \in \mathcal{P}} P^{v_S(P)}$. Il s'agit d'un produit infini, mais tous les facteurs sauf un nombre fini sont égaux à 1.

Pour $S, T \in \mathbb{Z}[X] \setminus \{0\}$ on définit alors leur pgcd *dans* $\mathbb{Z}[X]$, noté $\mathrm{pgcd}_{\mathbb{Z}[X]}(S, T)$, par :

$$\mathrm{pgcd}_{\mathbb{Z}[X]}(S, T) = \prod_{P \in \mathcal{P}} P^{\min(v_S(P), v_T(P))}.$$

4. Rappeler comment, à partir des $v_S(P)$ pour $P \in \mathcal{P}$, on peut écrire la décomposition de $S \in \mathbb{Z}[X] \setminus \{0\}$ en produit de polynômes irréductibles *dans* $\mathbb{Q}[X]$. En déduire que $\mathrm{pgcd}_{\mathbb{Z}[X]}(S, T)$ est (à association près) le pgcd de S et T dans $\mathbb{Q}[X]$.
5. Donner un exemple de polynômes $S, T \in \mathbb{Z}[X] \setminus \{0\}$ pour lesquels il n'existe pas de polynômes $U, V \in \mathbb{Z}[X]$ vérifiant $US + VT = \mathrm{pgcd}_{\mathbb{Z}[X]}(S, T)$.

On fixe maintenant $S, T \in \mathbb{Z}[X] \setminus \{0\}$ et on pose $D = \mathrm{pgcd}_{\mathbb{Z}[X]}(S, T)$. On note p un nombre premier qui ne divise pas le pgcd des coefficients dominants de S et T. Pour tout $Q \in \mathbb{Z}[X]$ on note $\overline{Q} \in \mathbb{F}_p[X]$ sa réduction modulo p. On suppose $\overline{S} \neq 0$ et $\overline{T} \neq 0$.

6. Démontrer que les polynômes D et $\overline{D}$ ont le même degré.
7. Démontrer que $\overline{D}$ divise le pgcd de $\overline{S}$ et $\overline{T}$.
8. Dans cette question on suppose en outre que p ne divise pas le résultant de S/D et T/D. Démontrer que $\overline{D}$ est (à association près) le pgcd de $\overline{S}$ et $\overline{T}$.
9. Définir un nombre réel M, calculable directement à partir des coefficients de S et/ou de ceux de T, tel que tous les coefficients de D soient compris entre $-M$ et M.

Dans la suite on suppose que S et T sont primitifs, et qu'on connaît des nombres premiers $p_1, \ldots, p_k$ deux à deux distincts vérifiant les conditions suivantes :

— On a $p_1 \ldots p_k > 2\ell M$ en notant ℓ le pgcd des coefficients dominants de S et T.
— Aucun des p_i ne divise ℓ.
— Aucun des p_i ne divise le résultant de S/D et T/D.

En pratique la troisième condition n'est pas facile à vérifier car on ne connaît pas D ; il s'agit ici d'une hypothèse destinée à simplifier l'algorithme.

10. Montrer qu'il existe un entier c tel que le coefficient dominant de cD soit égal à ℓ.
11. En utilisant ce qui précède, comment peut-on déterminer cD efficacement ? *On ne demande pas d'évaluer la complexité de ce calcul mais juste d'indiquer la méthode utilisée.*
12. Une fois le polynôme cD calculé, comment peut-on trouver D ?