Université Paris-Sud 11 — M1 MFA
Année universitaire 2014/2015 — MAO Calcul formel

PARTIEL DU LUNDI 10 NOVEMBRE 2014, DURÉE : 3H

Les documents sont autorisés, notamment les notes de cours manuscrites, imprimées ou en ligne (`http://www.math.u-psud.fr/~riou/enseignement/`), sujets et corrigés de TP compris. Il est également permis de consulter la documentation de Sage ; on pourra ainsi suivre les liens vers cette aide indiqués en haut de la page `http://www.math.u-psud.fr/~riou/enseignement/`. L'utilisation d'autres dispositifs électroniques ou mécaniques (calculatrices, ordinateurs de poche, baladeurs, téléphones portables, bouliers, etc.) est interdite.

Ce partiel 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. À 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 il est également indispensable d'expliquer les calculs que vous faites faire à l'ordinateur.

Le sujet comporte deux pages.

Problème

On considère le corps $\mathbf{F}_{31} := \mathbf{Z}/31\mathbf{Z}$ à 31 éléments. Un des buts de ce problème est de montrer que le polynôme $P := X^6 - 3 \in \mathbf{F}_{31}[X]$ est irréductible. (Pour cette raison, on s'interdira ici d'utiliser les fonctions de Sage comme `factor` permettant de factoriser un polynôme, déterminer ses racines ou déterminer s'il est irréductible.)

(En cas de blocage sur certaines questions, on pourra passer directement à la question (9) en admettant le résultat des questions précédentes.)

Posons $a := 3 \in \mathbf{F}_{31}$.

(1) ($\star$) Calculer a^6, a^{10}, a^{15}.

(2) Montrer que a est un générateur du groupe multiplicatif $\mathbf{F}_{31}^\times$.

Soit $Q \in \mathbf{F}_{31}[X]$ un facteur irréductible unitaire du polynôme $P = X^6 - 3 \in \mathbf{F}_{31}[X]$. (Note : on sait que cela existe *a priori*, mais on ne demande pas ici d'en expliciter un.)

Notons K le corps de rupture de Q sur $\mathbf{F}_{31}$. Notons $x \in K$ la racine privilégiée de Q dans K.

(3) Montrer que $x^6 = 3$.

(4) Montrer que $x^{31} = 3^5 \cdot x$.

(5) En déduire que pour tout $i \in \mathbf{N}$, on a $x^{31^i} = 3^{5i} \cdot x$.

(6) Calculer $x^{31^{666666666}}$ (sans utiliser l'ordinateur).

Notons $d := [K : \mathbf{F}_{31}] = \deg Q$ le degré de K sur $\mathbf{F}_{31}$.

(7) Montrer que $x^{31^d} = x$.

(8) Déduire des questions précédentes que $d = 6$ et que $P = X^6 - 3$ est un polynôme irréductible dans $\mathbf{F}_{31}[X]$.

(9) ($\star$) On sait maintenant que $P = X^6 - 3 \in \mathbf{F}_{31}[X]$ est irréductible. Construire dans Sage le corps de rupture K de $X^6 - 3$ sur $\mathbf{F}_{31}$. On notera toujours x la racine privilégiée de $X^6 - 3$.

(10) L'élément x est-il un générateur du groupe multiplicatif $K^\times$?

(11) ($\star$) L'élément $y := x + x^2 + x^3 + x^4$ est-il un générateur du groupe multiplicatif $K^\times$?

(12) Combien de sous-corps K possède-t-il ? Quels sont leurs cardinaux et degrés (sur $\mathbf{F}_{31}$) respectifs ?

Posons $\alpha := x^3$ et $\beta := x^2$.

(13) Montrer que $\alpha^2 = 3$ et $\beta^3 = 3$.

(14) Montrer que $\alpha^{31} \neq \alpha$ et que $\alpha^{31^2} = \alpha$. En déduire le cardinal du sous-corps $\mathbf{F}_{31}(\alpha) \subset K$ engendré par α et déterminer le polynôme minimal de α sur $\mathbf{F}_{31}$.

(15) De même, montrer que $\beta^{31} \neq \beta$ et que $\beta^{31^3} = \beta$. En déduire le cardinal du sous-corps $\mathbf{F}_{31}(\beta) \subset K$ engendré par β et déterminer le polynôme minimal de β sur $\mathbf{F}_{31}$.

Exercice

On considère la suite à valeurs entières $(u_n)_{n\in\mathbf{N}}$ définie par les relations suivantes : $u_0 = 0$, $u_1 = 1$ et $u_{n+2} = 5u_{n+1} - 6u_n$.

(1) Déterminer une matrice $M \in M_2(\mathbf{Z})$ telle que pour tout $n \in \mathbf{N}$, on ait la relation suivante :

$$M \begin{pmatrix} u_{n+1} \\ u_n \end{pmatrix} = \begin{pmatrix} u_{n+2} \\ u_{n+1} \end{pmatrix}$$

(2) En déduire que pour tout $n \geq 0$, on a :

$$\begin{pmatrix} u_{n+1} \\ u_n \end{pmatrix} = M^n \begin{pmatrix} 1 \\ 0 \end{pmatrix}$$

(3) En déduire une méthode pour calculer u_n. Quel algorithme fondamental intervient ? Donner une estimation du coût du calcul de u_n en fonction de n en nombre d'opérations arithmétiques (additions, multiplications) dans $\mathbf{Z}$.

(4) ($\star$) Implémenter cet algorithme dans Sage. (On rappelle que si `N` est une matrice dans Sage, on accède à la case (i, j) avec la syntaxe `N[i,j]` et on prendra garde au fait que dans Sage la numérotation des indices commence à 0 et non à 1.)

(5) Montrer que pour tout $n \in \mathbf{N}$, on a $u_n = 3^n - 2^n$.

(6) Si on veut calculer un terme de la suite u_n en utilisant l'expression précédente, quel sera le coût du calcul de u_n en fonction de n en opérations arithmétiques dans $\mathbf{Z}$? L'ordre de grandeur est-il le même qu'avec l'algorithme précédent utilisant une matrice ?