Université Paris-Sud 11 M1 MFA
Année universitaire 2012/2013 MAO Calcul formel

**PARTIEL DU LUNDI 12 NOVEMBRE 2012, DURÉE : 3H**

*Les documents autres que des notes de cours manuscrites, imprimées ou en ligne (`http://www.math.u-psud.fr/~riou/enseignement/`), sujets et corrigés de TP compris, sont interdits. Il est également permis de consulter la documentation de Sage ; on pourra ainsi de 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.*

***Dans ce partiel, on s'interdira d'utiliser les fonctions comme `factor` permettant de factoriser un polynôme, déterminer ses racines ou déterminer s'il est irréductible.***

## Exercice I

On considère le corps $\mathbf{F}_{13}$ à 13 éléments.

Notons $\alpha$ un élément de $\mathbf{F}_{13}^\times$ qui engendre le groupe multiplicatif $(\mathbf{F}_{13}^\times, \times)$.

(1) Soit $k \in \mathbf{Z}$. À quelle condition sur $k$ est-ce que $\alpha^k = 1$ dans $\mathbf{F}_{13}$.

(2) Soit $x \in \mathbf{F}_{13}^\times$. Montrer qu'il existe $y \in \mathbf{F}_{13}^\times$ tel que $x = y^3$ si et seulement si $x^4 = 1$.

(3) Montrer que $P := X^3 - 2 \in \mathbf{F}_{13}[X]$ est un polynôme irréductible.

On note $K$ le corps de rupture de $P$ sur $\mathbf{F}_{13}$. On note $x \in K$ la racine privilégiée de $P$.

(4) Quelle est la dimension de $K$ comme $\mathbf{F}_{13}$-espace vectoriel ? Donner une base $\mathcal{B}$ de $K$ comme $\mathbf{F}_{13}$-espace vectoriel. Quel est le cardinal de $K$ ?

Dans les questions suivantes, quand il sera demandé de calculer un élément de $K$, il faudra comprendre par là qu'il faut l'exprimer sous la forme d'une combinaison linéaire de vecteurs de la base $\mathcal{B}$.

(5) ($\star$) Combien de racines le polynôme $P$ admet-il dans $K$ ? Calculer ces racines.

(6) ($\star$) On note $y = 1 - x - x^2 \in K$. Calculer $y^{13}$ et $y^{13^2}$.

(7) ($\star$) Déterminer un polynôme unitaire $Q \in \mathbf{F}_{13}[X]$ de degré 3 tel que $Q(y) = 0$. Le polynôme $Q$ est-il irréductible ?

(8) ($\star$) L'élément $y$ est-il un générateur du groupe multiplicatif $(K^\times, \times)$.

(9) Montrer que le polynôme $X^3 - y \in K[X]$ est irréductible. (On pourra remarquer que $13^3 - 1$ est un multiple de 3.)

(10) On note $L$ le corps de rupture sur $K$ du polynôme $X^3 - y \in K[X]$. On note $z \in L$ la racine cubique privilégiée de $y$ dans $L$. Déterminer un polynôme $R \in \mathbf{F}_{13}[X]$ de degré 9 tel que $R(z) = 0$.

(11) Montrer que la sous-$\mathbf{F}_{13}$-algèbre de $L$ engendrée par $z$ est $L$ toute entière.

(12) En déduire que le polynôme $R$ est irréductible.

(13) Quels sont les sous-corps de $L$ ?

## Exercice II

On fixe des entiers $x_0, x_1, a, b$ et on considère la suite $(x_n)_{n\geq 0}$ définie par ses deux premières valeurs $x_0, x_1$ et la relation de récurrence $x_{n+2} = ax_n + bx_{n+1}$ pour tout $n \geq 0$.

(14) Construire une matrice $M \in M_2(\mathbf{Z})$ telle que pour tout $n \geq 0$, on ait :

$$\begin{pmatrix} x_{n+1} \\ x_{n+2} \end{pmatrix} = M \begin{pmatrix} x_n \\ x_{n+1} \end{pmatrix}$$

(15) Montrer que pour tout $n \geq 0$, on a :

$$\begin{pmatrix} x_n \\ x_{n+1} \end{pmatrix} = M^n \begin{pmatrix} x_0 \\ x_1 \end{pmatrix}$$

(16) En déduire un algorithme, étant donné un entier $n \geq 0$, pour calculer $x_n$. On indiquera les algorithmes fondamentaux qui interviennent.

(17) Donner une estimation en fonction de $n$ du nombre d'opérations arithmétiques dans $\mathbf{Z}$ (additions, multiplications, soustractions).

(18) ($\star$) Implémenter votre algorithme sous la forme d'une fonction prenant en arguments $x_0, x_1, a, b, n$, c'est-à-dire commençant par :

```
def suite(x0,x1,a,b,n):
    ...
```

On fixe un nombre premier $p$ différent de 2. En conservant les notations précédentes, on définit $(\overline{x_n})_{n\geq 0}$ la suite de $\mathbf{F}_p = \mathbf{Z}/p\mathbf{Z}$ formée des classes modulo $p$ des termes de la suite $(x_n)_{n\geq 0}$. On note de même $\overline{a}, \overline{b}$ les classes de $a$ et $b$ modulo $p$, et $\overline{M}$ l'image de $M$ dans $M_2(\mathbf{F}_p)$. On suppose que $\overline{a} \neq 0$.

(19) Soit $u \in \mathbf{F}_p^2 - \{0\}$ un vecteur non nul du $\mathbf{F}_p$-espace vectoriel $\mathbf{F}_p^2$ de dimension 2. Combien existe-t-il de vecteurs $v$ tels que la famille $(u, v)$ soit liée ? Combien existe-t-il de vecteurs $v$ tels que la famille $(u, v)$ soit une $\mathbf{F}_p$-base de $\mathbf{F}_p^2$.

(20) En déduire le cardinal de $\mathrm{GL}_2(\mathbf{F}_p)$.

On note $N := \#\,\mathrm{GL}_2(\mathbf{F}_p)$ ce cardinal.

(21) Montrer que la suite $(\overline{x_n})_{n\geq 0}$ est $N$-périodique, c'est-à-dire que $x_{n+N} = x_n$ pour tout $n \geq 0$.

On note $\overline{P} = X^2 - \overline{b}X - \overline{a} \in \mathbf{F}_p[X]$. Dans les questions suivantes, on suppose que $\overline{P} \in \mathbf{F}_p[X]$ est irréductible. On note $K$ le corps de rupture de $\overline{P}$ sur $\mathbf{F}_p$ et on note $\lambda \in K$ la racine priviliégiée de $P$ dans $K$.

(22) Montrer que $\lambda^{p^2-1} = 1$.

(23) En déduire que l'on a la congruence de polynômes $X^{p^2-1} \equiv 1 \mod \overline{P}$.

(24) Est-il vrai que $\overline{M}^2 - \overline{b} \cdot \overline{M} - \overline{a} = 0$ dans $M_2(\mathbf{F}_p)$ ?

(25) Montrer que $\overline{M}^{p^2-1} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$.

(26) En déduire que la suite $(\overline{x_n})_{n\geq 0}$ est $p^2 - 1$-périodique.

(27) En déduire une méthode pour calculer $\overline{x_n}$ quand $n$ est grand.

À partir de maintenant, on suppose que $p = 7$, $\overline{a} = \overline{b} = 2$, $x_0 = 0$, $x_1 = 1$.

(28) Déterminer un entier $k \geq 1$ tel que $x_{n+k} = x_n$ pour tout $n \geq 0$.

(29) ($\star$) Calculer $\overline{x_n}$ pour $n = 5^{10000}$.

(30) ($\star$) L'entier $k$ est-il le plus petit entier qui convienne ?

## Sage

On pourra utiliser les pages d'aide signalées en haut de la page `http://www.math.u-psud.fr/~riou/enseignement/`, et des informations utiles pourront aussi être obtenus dans l'aide de Sage, en tapant par exemple `GF?`, `Integers?` ou `matrix?`.