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

**CORRIGÉ DU PARTIEL DU LUNDI 12 NOVEMBRE 2012**

## 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 $\mathbf{F}_{13}$.

> L'ordre de $\alpha$ dans le groupe $\mathbf{F}_{13}^\times$ étant 12, on a $\alpha^k = 1$ si et seulement si 12 divise $k$.

(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 $x^4 = 1$.

> L'élément $x$ peut s'écrire $x = \alpha^k$ pour un certain entier $k \in \mathbf{Z}$. On a $x^4 = \alpha^{4k}$. D'après la question précédente, $x^4 = 1$ équivaut à $12|4k$ c'est-à-dire $3|k$.
>
> Si $x^4 = 1$, on a donc $3|k$ et on peut poser $y = \alpha^{\frac{k}{3}}$ qui vérifie bien $x = y^3$. S'il existe $y$ tel que $x = y^3$, on a $x^4 = y^{12} = 1$ car $y$ est un élément du groupe multiplicatif $\mathbf{F}_{13}^\times$ qui est d'ordre 12.

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

> $2^4 = 16 \equiv 3 \mod 13$. D'après la question précédente, le polynôme $P$ n'admet pas de racine dans $\mathbf{F}_{13}$. Comme ce polynôme est de degré 3, cela suffit pour conclure que $P$ est 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 $K$ ?

> Comme $P$ est de degré 3, les éléments $1, x, x^2$ forment une $\mathbf{F}_{13}$-base du $K$, qui est donc de dimension 3 et de cardinal $13^3 = 2197$.

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.

> D'après le cours, comme $P$ est un polynôme irréductible, $P$ est scindé à racines simples dans son corps de rupture $K$ et les trois racines distinctes sont $x, x^{13}, x^{13^2}$. Comme $x^3 = 2$, on obtient $x^{13} = x^{4\cdot 3+1} = 2^4 x = 3x$. Par suite, $x^{13^2} = (3x)^{13} = 3^{13}x^{13} = 3 \cdot 3x = 9x = -4x$.

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

> Les lignes de codes suivantes permettent de définir le corps de rupture du polynôme $X^3 - 2$ sur $\mathbf{F}_{13}$. On définit ensuite $y$ dans ce corps, ce qui permet de calculer $y^{13}$ et $y^{13^2}$.
>
> ```
> F13=GF(13)
> A.<X>=PolynomialRing(F13)
> K.<x>=GF(13**3, modulus=X^3-2)
> y=1-x-x^2
> y,y^13,y^(13^2)
> ```
>
> On obtient :
>
> $$y^{13} = 1 - 3x + 4x^2 \qquad y^{13^2} = 1 + 4x - 3x^2$$

(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 ?

> Si $Q \in \mathbf{F}_{13}[X]$ admet $y$ comme racine, il admettra aussi $y^{13}$ et $y^{13^2}$ comme racines. On considère donc le produit $(X - y)(X - y^{13})(X - y^{13^2})$ qui va s'avérer être à coefficients dans $\mathbf{F}_{13}$. Dans Sage, il est plus prudent d'utiliser une autre indéterminée que $X$ puisque l'on manipule des polynômes à coefficients dans $K$ et non plus seulement dans $\mathbf{F}_{13}$ comme plus haut :

```
B.<Y>=PolynomialRing(K)
(Y-y)*(Y-y^13)*(Y-y^(13*13))
```

On obtient $Q = X^3 - 3X^2 - 3X - 2$ qui appartient bien à $\mathbf{F}_{13}[X]$. (En demandant à Sage de calculer $Q(y) = y^3 - 3y^2 - 3y - 2$, on peut effectivement constater que cela fait 0.) Le sous-corps de $K$ engendré par $y$ est de degré (sur $\mathbf{F}_{13}$) divisant 3. Comme $y \notin \mathbf{F}_{13}$, ce degré est 3, donc $\mathbf{F}_{13}[y] = K$. Le polynôme minimal de $y$ est donc de degré 3. Comme $Q$ est un multiple de ce polynôme minimal et que ces deux polynômes sont tous les deux unitaires de degré 3, on obtient que $Q$ est le polynôme minimal de $y$. En particulier, $Q \in \mathbf{F}_{13}[X]$ est irréductible.

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

On peut demander à Sage de factoriser l'entier $13^3 - 1$ (le cardinal de $K^\times$). On obtient $13^3 - 1 = 2^2 \cdot 3^2 \cdot 61$. Si $d$ est un diviseur de $13^3 - 1$ qui n'est pas $13^3 - 1$, l'entier $d$ doit donc diviser $\frac{13^3-1}{p}$ pour au moins un $p$ parmi $\{2, 3, 61\}$. Si $y$ n'était pas un générateur de $K^\times$, on aurait $y^{\frac{13^3-1}{p}} = 1$ pour au moins un de ces trois nombres premiers $p$. Le résultat du calcul suivant montre que ce n'est pas le cas, donc $y$ est bien un générateur du groupe $K^\times$.

```
factor(13^3-1)
[y^((13^3-1)/p) for p in [2,3,61]]
```

(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.)

Si $X^3 - y \in K[X]$ n'était pas irréductible, puisqu'il est de degré 3, il aurait une racine dans $K$. Il existerait donc $z \in K^\times$ tel que $y = z^3$, mais alors $y^{\frac{13^3-1}{3}} = z^{3 \cdot \frac{13^3-1}{3}} = z^{13^3-1} = 1$, ce qui montrerait que l'ordre de $y$ est strictement plus petit que ce qu'il est censé être d'après la question précédente. Le polynôme $X^3 - y$ est donc irréductible.

(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 $R(z) = 0$.

On sait que $Q(y) = 0$, donc $Q(y) = Q(z^3) = z^9 - 3z^6 - 3z^3 - 2 = 0$, ce qui montre que $R = X^9 - 3X^6 - 3X^3 - 2 \in \mathbf{F}_{13}[X]$ est un polynôme unitaire 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.

Notons $A$ la sous-$\mathbf{F}_{13}$-algèbre de $L$ engendrée par $z$. Comme $z^3 = y$, $y \in A$, puis $\mathbf{F}_{13}[y] = K \subset A$. La sous-algèbre $A$ est donc un sous-$K$-espace vectoriel de $L$, qui contient évidemment $1, z, z^2$, qui une $K$-base de $L$. On a donc bien $A = L$.

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

Notons $S$ le polynôme minimal de $z$ sur $\mathbf{F}_{13}$. On sait que le degré de $S$ est égal à $\dim_{\mathbf{F}_{13}} \mathbf{F}_{13}[z] = \dim_{\mathbf{F}_{13}} L = 9$ d'après ce qui précède. Comme $R(z) = 0$, la minimalité de $S$ fait que $S|R$. Comme ces deux polynômes sont unitaires et de même degré, on a $R = S$. Comme le polynôme minimal d'un élément dans une extension de corps est irréductible, il vient que $R$ est irréductible.

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

Pour chaque diviseur $d$ de $[L : \mathbf{F}_{13}] = 9$, on a un unique sous-corps de $L$ de degré $d$ sur $\mathbf{F}_{13}$ et on obtient ainsi tous les sous-corps de $L$. Les seuls diviseurs de 9 sont $1, 3, 9$. Il en résulte que les sous-corps de $L$ sont $\mathbf{F}_{13}$, $K$ et $L$.

## 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 :

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

La matrice $M = \begin{pmatrix} 0 & 1 \\ a & b \end{pmatrix}$ convient puisque l'on a :

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

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

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

Ceci se démontre immédiatement par récurrence sur $n$.

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

Pour calculer $x_n$, on calcule $M^n$ en utilisation l'algorithme d'exponentiation rapide dans l'anneau $M_2(\mathbf{Z})$. La matrice $M^n$ est de la forme $\begin{pmatrix} \alpha & \beta \\ \star & \star \end{pmatrix}$, on peut alors calculer $\alpha x_0 + \beta x_1$, d'après la question précédente, c'est $x_n$.

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

La partie principale du calcul est l'exponentiation $M^n$. Avec l'algorithme d'exponentiation, cela demande $O(\log_2 n)$ multiplication dans l'anneau $M_2(\mathbf{Z})$. Une multiplication dans cet anneau demande un certain nombre (constant) d'opérations arithmétiques dans $\mathbf{Z}$. On peut donc calculer $x_n$ en faisant $O(\log_2 n)$ opérations arithmétiques dans $\mathbf{Z}$.

(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):
    ...
```

D'après les questions précédentes, on peut procéder comme suit :

```
def suite(x0,x1,a,b,n):
    M=matrix(2,2,[0,1,a,b])
    N=M^n
    return N[0,0]*x0+N[0,1]*x1
```

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 $\mathbf{F}_p^2$.

Comme $u$ est non nul, les vecteurs $v$ tels que $(u, v)$ soit liée sont les vecteurs appartenant à la droite engendrée par $u$, qui est de cardinal $p$. Le nombre de vecteurs $v$ tels que $(u, v)$ soit libre est donc $p^2 - p = p(p-1)$.

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

Le nombre de vecteurs non nuls $u$ dans $\mathbf{F}_p^2$ est $p^2 - 1$. Pour chacun de ces $u$, il existe $p(p-1)$ vecteurs $v$ tels que $(u, v)$ soit une base. Il en résulte que le nombre de bases, c'est-à-dire le cardinal de $\mathrm{GL}_2(\mathbf{F}_p)$ vaut $p(p-1)^2(p+1)$.

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 $n \geq 0$.

Comme $\overline{a} \neq 0$, la matrice $\overline{M}$ est inversible. Comme c'est un élément de $\mathrm{GL}_2(\mathbf{F}_p)$, $M^N$ est la matrice identité pour $N = p(p-1)^2(p+1)$. On a la relation :

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

Comme $M^{n+N} = M^n M^N = M^n$, il vient aussitôt 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 $\lambda^{p^2-1} = 1$.

$\lambda$ est un élément de $K$ qui est non nul (vu que $\overline{a} \neq 0$). Comme $K^\times$ est de cardinal $p^2 - 1$, on a $\lambda^{p^2-1} = 1$.

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

Le polynôme minimal de $\lambda$ est $\overline{P}$, or $\lambda$ est racine du polynôme $X^{p^2-1} - 1$ d'après la question précédente, donc $\overline{P}$ divise $X^{p^2-1}-1$, ce qui est équivalent à la congruence que l'on souhaite démontrer.

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

Oui, c'est le théorème de Cayley-Hamilton, qui peut aussi se vérifier à la main dans ce cas particulier.

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

Comme $\overline{P}$ est une polynôme annulateur de $\overline{M}$, la matrice $R(\overline{M})$ obtenue en appliquant un polynôme $R$ à $\overline{M}$ ne dépend que de la classe de congruence de $R$ modulo $\overline{P}$. Les questions précédentes permettent donc de conclure.

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

L'argument est identique à celui de la question 21.

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

On commence par calculer le reste $r$ de la division euclidienne de $n$ par $p^2 - 1$. On calcule ensuite $\overline{x_r}$ comme dans l'algorithme de calcul de $x_n$, à la différence près que l'on peut faire les calculs dans $M_2(\mathbf{F}_p)$ plutôt que dans $M_2(\mathbf{Z})$.

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 $n \geq 0$.

Dans $\mathbf{F}_7[X]$, $X^2 - 2X - 2 = (X-1)^2 - 3$. Les carrés dans $\mathbf{F}_7$ sont $0, 1, 4, 2$, donc 3 n'est pas un carré. Ainsi, $X^2 - 2X - 2$ est irréductible sur $\mathbf{F}_7$. D'après ce qui précède, la suite $\overline{x_n}$ est $7^2 - 1 = 48$-périodique.

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

La suite $\overline{x_n}$ étant 48-périodique, $\overline{x_n} = \overline{x_r}$ où $r$ est le reste de la division euclidienne de $n$ par 48. Pour $n = 5^{10000}$, on peut calculer ce reste par exponentiation rapide modulo 48 :

```
Integers(48)(5)^10000
```

On obtient $r = 1$, donc $\overline{x_n} = \overline{x_1} = 1$.

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

Le plus petit entier $d$ vérifiant $x_{n+d} = x_n$ pour tout $n \geq 0$ doit être un diviseur de $48 = 2^4 \cdot 3$. Pour conclure que $d = k = 48$, il suffit donc de vérifier que la suite $\overline{x_n}$ n'est ni 16-périodique ni 24-périodique. On peut observer que $\overline{x_{17}} = 4 \neq \overline{x_1}$ et $\overline{x_{25}} = 6 \neq \overline{x_1}$.

```
Integers(48)(5)^10000
```