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

CORRIGÉ DU PARTIEL DU LUNDI 10 NOVEMBRE 2014

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.)

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

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

> Les commandes suivantes permettent de faire les calculs voulus dans $\mathbf{F}_{31}$:
>
> ```
> F31=GF(31)
> a=F31(3)
> a^6,a^10,a^15
> ```
>
> On obtient $a^6 = 16$, $a^{10} = 25$ et $a^{15} = 30$.

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

> Montrer que a est un générateur du groupe multiplicatif $\mathbf{F}_{31}^\times$ revient à montrer que l'ordre k de a dans ce groupe est $30 = 2 \cdot 3 \cdot 5$. Cet entier k divisant 30, montrer que $k = 30$ se ramène à montrer que k ne divise aucun des entiers $\frac{30}{p}$ pour $p \in \{2, 3, 5\}$, c'est-à-dire que $a^{15} \neq 1$, $a^{10} \neq 1$ et $a^6 \neq 1$, ce qui a été obtenu à la question précédente.

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 $x^6 = 3$.

> Par définition, x est une racine du polynôme Q qui divise P, donc x est aussi racine de $P = X^6 - 3$, d'où $x^6 = 3$.

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

> $x^{31} = x^{5 \cdot 6 + 1} = \left(x^6\right)^5 \cdot x = 3^5 \cdot x.$

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

> L'élévation à la puissance 31 est l'automorphisme de Frobenius $F\colon K \to K$ du corps K. Si on note $F^{\circ i}$ le i-ème itéré de F pour tout $i \geq 0$, on peut montrer par récurrence que $x^{31^i} = F^{\circ i}(x)$. On se ramène ainsi à montrer par récurrence sur $i \geq 0$ que $F^{\circ i}(x) = 3^{5i} \cdot x$. Le cas $i = 0$ est évident et le cas $i = 1$ a été traité à la question précédente (c'est-à-dire que $F(x) = 3^5 \cdot x$). Soit $i \geq 0$, supposons que $F^{\circ i}(x) = 3^{5i} \cdot x$. Montrons ce résultat pour $i + 1$. En utilisant l'hypothèse de récurrence et le fait que F est un automorphisme du corps K, on obtient $F^{\circ i+1}(x) = F(F^{\circ i}(x)) = F(3^{5i} \cdot x) = F(3)^{5i} \cdot F(x)$. Le Frobenius induisant l'identité de $\mathbf{F}_{31}$, on a $F(3) = 3$. Comme on sait que $F(x) = 3^5 \cdot x$, on obtient $F^{\circ i+1}(x) = 3^{5i} \cdot (3^5 \cdot x) = 3^{5(i+1)} \cdot x$.

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

> D'après la question précédente, on a $x^{31^{666666666}} = 3^{5\cdot 666666666} \cdot x$. L'exposant $5 \cdot 666666666$ est multiple de 30. Comme l'ordre de 3 dans le groupe $\mathbf{F}_{31}^{\times}$ divise 30 (et est même égal à 30), on obtient $3^{5\cdot 666666666} = 1$, d'où $x^{31^{666666666}} = x$.

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

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

> Le corps Q est de cardinal 31^d, donc pour tout $z \in K$, on a $z^{31^d} = z$. Ceci vaut en particulier pour $z := x$.

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

> Il est évident que $1 \leq d \leq 6$. Les questions précédentes montrent que $x^{31^d} = 3^{5d} \cdot x = x$. Vu que $x^6 = 3$, on a $x \neq 0$, ce qui permet de déduire de l'identité précédente que $3^{5d} = 1$. L'élément $a = 3$ étant d'ordre 30 dans le groupe multiplicatif $\mathbf{F}_{31}^{\times}$, on obtient que 30 divise $5d$, ce qui revient à dire que 6 divise d. On obtient ainsi $d = 6$. Le polynôme unitaire Q divisant P et étant de même degré, il vient donc que $P = Q$. Comme Q est irréductible, on obtient que P est un polynôme irréductible.

(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 $X^6 - 3$.

> Les commandes suivantes définissent successivement l'anneau $A = \mathbf{F}_{31}[X]$, le polynôme $P = X^6 - 3 \in A$ et le corps de rupture K de P sur $\mathbf{F}_{31}$, l'élément $x \in K$ étant la racine privilégiée de P dans K :
>
> ```
> A.<X>=F31[]
> P=X^6-3
> K.<x>=GF(31^6,modulus=P)
> ```

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

> On a $x^6 = 3$, or $3^{30} = 1$, donc $x^{180} = x^{6\cdot 30} = 1$. L'ordre de x divise donc 180 (et est même très exactement égal à 180). L'ordre du groupe multiplicatif $K^{\times}$ est $31^6 - 1$ qui est certainement plus grand que 180, donc x n'est pas 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 $K^{\times}$?

> En utilisant la commande `factor(31^6-1)`, on obtient $\#K^{\times} = 2^6 \cdot 3^2 \cdot 5 \cdot 7^2 \cdot 19 \cdot 331$. Si y n'était pas un générateur de $K^{\times}$, son ordre diviserait un des entiers $\frac{\#K^{\times}}{p}$ pour $p \in \{2, 3, 5, 7, 19\}$, c'est-à-dire que pour au moins un de ces cinq nombres premiers on aurait $x^{\frac{31^6-1}{p}} = 1$. On peut s'assurer que ce n'est pas le cas en utilisant les commandes suivantes :
>
> ```
> y=x+x^2+x^3+x^4
> for p in [2,3,5,7,19,331]:
>     print y^((31^6-1)//p)
> ```

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

> Le degré $[K\colon \mathbf{F}_{31}]$ vaut 6. D'après le cours, on sait que si k est un sous-corps de K, alors $[k\colon \mathbf{F}_{31}]$ divise 6 et que pour tout diviseur d de 6, K possède un unique sous-corps de cardinal 31^d que l'on notera $\mathbf{F}_{31^d}$ (et bien sûr $[\mathbf{F}_{31^d}\colon \mathbf{F}_{31}] = d$). Les diviseurs de d étant $1, 2, 3, 6$, K possède quatre

sous-corps $\mathbf{F}_{31}, \mathbf{F}_{31^2}, \mathbf{F}_{31^3}$ et $\mathbf{F}_{31^6} = K$. (Les questions qui suivent visent à décrire explicitement les sous-corps $\mathbf{F}_{31^2}$ et $\mathbf{F}_{31^3}$.)

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

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

$\alpha^2 = \left(x^3\right)^2 = x^6 = 3$ et $\beta^3 = \left(x^2\right)^3 = 3$.

(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 $\mathbf{F}_{31}$.

(Il serait tout à fait possible ici de faire faire les calculs à Sage et de constater que ce qui est affirmé est bien vrai.)

Avec les notations introduites plus haut, $\alpha^{31} = F(\alpha) = F(x^3) = F(x)^3 = (3^5 \cdot x)^3 = 3^{15}\alpha \neq \alpha$ parce que $\alpha \neq 0$ et $3^{15} \neq 1$ (3 étant d'ordre 30 dans le groupe multiplicatif). Ensuite, $\alpha^{31^2} = F(F(\alpha)) = F(3^{15} \cdot \alpha) = 3^{15} \cdot F(\alpha) = 3^{15} \cdot 3^{15} \cdot \alpha = 3^{30}\alpha = \alpha$. Ces identités montrent que α appartient au sous-corps $\mathbf{F}_{31^2}$ mais pas à $\mathbf{F}_{31}$. On a donc $\mathbf{F}_{31} \subsetneq \mathbf{F}_{31}(\alpha) \subset \mathbf{F}_{31^2}$. Le degré $[\mathbf{F}_{31}(\alpha) \colon \mathbf{F}_{31}]$ divise 2 mais est différent de 1, donc est égal à 2, ce qui revient à dire que $\mathbf{F}_{31}(\alpha) = \mathbf{F}_{31^2}$. Le degré du polynôme minimal de α sur $\mathbf{F}_{31}$ est donc 2. Comme $\alpha^2 = 3$, on en déduit que le polynôme minimal de α est $X^2 - 3$.

(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 $\mathbf{F}_{31}$.

De même, $\mathbf{F}_{31}(\beta) = \mathbf{F}_{31^3}$ et le polynôme minimal de β est $X^3 - 3$.

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 :

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

On cherche M sous la forme $M := \begin{pmatrix} a & b \\ c & d \end{pmatrix}$. L'identité à satisfaire se reformule ainsi, pour tout $n \geq 0$:

$$\begin{cases} au_{n+1} + bu_n & = & u_{n+2} \\ cu_{n+1} + du_n & = & u_{n+1} \end{cases}$$

Il est clair que $a = 5$, $b = -6$, $c = 1$, $d = 0$ conviennent. On peut donc poser $M := \begin{pmatrix} 5 & -6 \\ 1 & 0 \end{pmatrix}$.

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

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

Par une récurrence évidente sur $n \geq 0$, on a :

$$\begin{pmatrix} u_{n+1} \\ u_n \end{pmatrix} = M^n \begin{pmatrix} u_1 \\ u_0 \end{pmatrix} = M^n \begin{pmatrix} 1 \\ 0 \end{pmatrix}$$

(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 $\mathbf{Z}$.

> D'après la question précédente, le coefficient en bas à gauche de M^n est étant à u_n. On peut donc déduire la valeur de u_n du calcul de M^n qui peut se faire par exponentiation rapide dans $M_2(\mathbf{Z})$. Le coût de cet algorithme est de $O(\log n)$ multiplications dans $M_2(\mathbf{Z})$. Chaque multiplication $M_2(\mathbf{Z})$ demandant un nombre borné d'additions et multiplications d'entiers, on obtient que le coût est de $O(\log n)$ opérations arithmétiques 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.)

```
def suite(n):
    M=matrix([[5,-6],[1,0]])
    return (M^n)[1,0]
```

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

> L'ensemble des suites réelles $(v_n)_{n\in\mathbf{N}}$ vérifiant la relation $v_{n+2} = 5v_{n+1} - 6v_n$ est un espace vectoriel E contenant les suites géométriques $(\lambda^n)_{n\in\mathbf{N}}$ pour $\lambda \in \mathbf{R}$ racine de l'équation caractéristique $\lambda^2 - 5\lambda + 6$. Si on pose $v_n := 3^n - 2^n$ pour tout $n \geq 0$, on a donc $(v_n)_{n\in\mathbf{N}} \in E$. Un élément de E étant déterminé par ses deux premiers termes, pour montrer $u_n = v_n$ pour tout $n \geq 0$, il suffit d'observer que $v_0 = 0 = u_0$ et $v_1 = 1 = u_1$. (Sans utiliser les résultats généraux sur les suites récurrentes linéaires d'ordre 2, on pouvait aussi établir ce résultat par récurrence sur 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 ?

> En utilisant la formule précédente, le calcul de u_n résulte de deux exponentiations rapides dans $\mathbf{Z}$ et d'une différence. Le coût est donc de $O(\log n)$ opérations arithmétiques dans $\mathbf{Z}$ tout comme l'algorithme précédent.