Université Paris-Sud 11 — M1 MFA
Année universitaire 2013/2014 — MAO Calcul formel

EXAMEN DU MERCREDI 22 JANVIER 2014, 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 l'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.

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. À titre indicatif, pour les questions signalées par le signe (⋆), on s'attend à une réponse utilisant l'ordinateur ; les autres devraient plutôt recevoir une réponse argumentée, utilisant éventuellement l'ordinateur de façon marginale.

Exercice 1

On considère le polynôme $P = X^4 - 2X^2 + 9 \in \mathbf{Z}[X]$. On voudrait montrer que P est irréductible dans $\mathbf{Z}[X]$, mais on s'interdira ici d'utiliser les fonctions de Sage permettant de factoriser ou de vérifier l'irréductibilité de polynômes dans $\mathbf{Z}[X]$; mais on se l'autorise pour des polynômes à coefficients dans $\mathbf{F}_p$.

(1) Supposons que P n'est pas irréductible dans $\mathbf{Z}[X]$. Montrer qu'il existe alors un polynôme unitaire $Q \in \mathbf{Z}[X]$ de degré 1 ou 2 tel que Q divise P.

(2) (⋆) Montrer que les valeurs absolues des coefficients de Q sont ≤ 37.

Posons $p := 79$. Notons $\overline{P} \in \mathbf{F}_p[X]$ et $\overline{Q} \in \mathbf{F}_p[X]$ les images de P et Q dans $\mathbf{F}_p[X]$.

(3) (⋆) Quelle est la factorisation de l'image $\overline{P}$ de P dans $\mathbf{F}_p[X]$? Donner une liste de deux polynômes $\overline{R_1}$ et $\overline{R_2}$ dans $\mathbf{F}_p[X]$ tels qu'on ait forcément $\overline{Q} = \overline{R_1}$ ou $\overline{Q} = \overline{R_2}$.

(4) Déterminer deux polynômes R_1 et R_2 dans $\mathbf{Z}[X]$ tels que l'on ait forcément $Q = R_1$ ou $Q = R_2$.

(5) (⋆) Montrer que Q est irréductible dans $\mathbf{Z}[X]$.

Exercice 2

On définit une suite $(u_n)_{n\in\mathbf{Z}}$ à valeurs dans $\mathbf{Z}$ en posant $u_0 = 1$, $u_1 = 0$ et en imposant la relation $u_{n+2} = u_n + u_{n+1}$ pour $n \geq 0$.

(6) Soit $\phi := \frac{1+\sqrt{5}}{2} \in \mathbf{R}$. Vérifier que $\phi^2 = 1+\phi$ et montrer que pour tout $n \geq 0$, on a $u_n + u_{n+1}\cdot\phi = \phi^n$.

Notons $p := 197$ et introduisons la suite $(\overline{u_n})_{n\in\mathbf{Z}}$ à valeurs dans $\mathbf{F}_{197}$ où $\overline{u_n}$ est la classe de u_n modulo 197 pour tout $n \geq 0$.

(7) L'entier 197 est-il un carré modulo 5 ? Peut-on en déduire que 5 n'est pas un carré modulo 197 ?

(8) Vérifier que le polynôme $P := X^2 - X - 1 \in \mathbf{F}_{197}[X]$ est irréductible. (On essaiera si possible de déduire ce résultat de la question précédente.)

On note K le corps de rupture de P sur $\mathbf{F}_{197}$. On note x la racine privilégiée de P dans K.

(9) Quel est le cardinal de K ? Quelle est sa dimension comme $\mathbf{F}_p$-espace vectoriel ? Donner une base de K comme $\mathbf{F}_{197}$-espace vectoriel.

(10) (⋆) Construire le corps K dans Sage.

(11) Montrer la relation $x^n = \overline{u_n} + \overline{u_{n+1}}x$ dans K pour tout $n \geq 0$.

(12) En déduire un algorithme permettant de calculer $\overline{u_n} \in \mathbf{F}_{197}$ en fonction de n. (Il convient d'indiquer le ou les algorithmes fondamentaux vus en cours qui entrent en jeu.)

(13) Donner une estimation du coût de l'algorithme de la question précédente en nombre d'opérations arithmétiques dans $\mathbf{F}_{197}$.

(14) (⋆) Définir une fonction prenant en argument un entier n et renvoyant $\overline{u_n} \in \mathbf{F}_{197}$ [1].

(15) (⋆) Calculer $\overline{u_{1000}}$.

1. Si y est un élément d'un corps fini dans Sage, `y.polynomial()` renvoie la représentation de y sous la forme d'un polynôme.

Problème

Dans ce problème, on s'interdira d'utiliser les fonctions de Sage permettant de factoriser ou de tester l'irréductibilité de polynômes à coefficients dans un corps fini.

Soit k un corps. Soit n un entier naturel. Soit $\sigma \in \mathfrak{S}_n$ une permutation de l'ensemble $\{1, \dots, n\}$. On note E le k-espace vectoriel des applications $\{1, \dots, n\} \to k$. On définit une application k-linéaire $S\colon E \to E$ de la façon suivante : si $f \in E$, c'est-à-dire que f est une application $\{1, \dots, n\} \to k$, on note $S(f)$ l'application $\{1, \dots, n\} \to k$ définie par $S(f)(i) = f(\sigma^{-1}(i))$ pour tout $i \in \{1, \dots, n\}$.

(Les questions (16) et (17) sont indépendantes. On notera aussi que le résultat énoncé dans la question (24) permet d'aborder les questions suivantes.)

(16) Pour $i \in \{1, \dots, n\}$, on note $e_i \in E$ la fonction caractéristique du singleton $\{i\}$. Déterminer $S(e_i)$. En déduire la forme de la matrice de S dans la k-base $(e_1, \dots, e_n)$ de E.

(17) Exprimer la dimension de $F := \{f \in E, S(f) = f\}$ en termes de la décomposition de la permutation σ en produit de cycles à supports disjoints ou en termes des orbites de σ.

On suppose maintenant que $n \geq 2$. On se donne un nombre premier p. On pose $k := \mathbf{F}_p$ et on pose $P := X^n - 1 \in \mathbf{F}_p[X]$. On fait l'hypothèse que p ne divise pas n.

(18) Montrer que P et P' sont des polynômes premiers entre eux dans $\mathbf{F}_p[X]$.

On pose $A := \mathbf{F}_p[X]/(X^n - 1)$. On note $x \in A$ la classe de X.

(19) Quelle est la dimension du $\mathbf{F}_p$-espace vectoriel A ? En donner une base $\mathcal{B}$.

(20) On note $\varphi\colon A \to A$ l'application définie par $\varphi(a) = a^p$ pour tout $a \in A$. L'application φ est-elle $\mathbf{F}_p$-linéaire ?

(21) Quel est le lien entre la dimension de $\ker(\varphi - Id_A)$ et la factorisation éventuelle de $X^n - 1$ en produit de polynômes irréductibles dans $\mathbf{F}_p[X]$?

(22) Décrire la matrice de φ dans la base $\mathcal{B}$.

On note $\overline{p}$ la classe de p dans $\mathbf{Z}/n\mathbf{Z}$. Si i et j sont deux éléments de $\mathbf{Z}/n\mathbf{Z}$, on note $i \sim j$ s'il existe $k \in \mathbf{Z}$ tel que $i = j \cdot \overline{p}^k$.

(23) Montrer que $\sim$ est une relation d'équivalence sur $\mathbf{Z}/n\mathbf{Z}$.

(24) Montrer que le nombre de facteurs irréductibles de $X^n - 1$ dans $\mathbf{F}_p[X]$ est égal au nombre de classes d'équivalences d'éléments de $\mathbf{Z}/n\mathbf{Z}$ pour la relation $\sim$.

(25) Dans cette question, on suppose que $n = 6$. Sous les hypothèses faites, à quelles classes de congruence modulo 6 le nombre premier p peut-il appartenir ? Montrer que si $p \equiv 1 \mod 6$, le polynôme $X^6 - 1$ est scindé dans $\mathbf{F}_p[X]$. Combien de facteurs irréductibles $X^6 - 1$ possède-t-il dans $\mathbf{F}_p[X]$ si $p \not\equiv 1 \mod 6$?

Soit ℓ un nombre premier différent de p. On suppose que $n = \ell$.

(26) On note e l'ordre de $\overline{p}$ dans le groupe $\mathbf{F}_\ell^\times$. Montrer que le nombre de facteurs irréductibles de $X^\ell - 1$ dans $\mathbf{F}_p[X]$ est $1 + \frac{\ell-1}{e}$.

(27) En déduire que le nombre de facteurs irréductibles de $1 + X + X^2 + \cdots + X^{\ell-1}$ dans $\mathbf{F}_p[X]$ est $\frac{\ell-1}{e}$.

(28) Déterminer le nombre de facteurs irréductibles de $X^\ell - 1$ dans $\mathbf{F}_p[X]$ dans les cas suivants : $(p, \ell) = (2, 5)$, $(p, \ell) = (11, 5)$, $(p, \ell) = (29, 5)$, $(p, \ell) = (5, 7)$.

(29) Montrer que $1 + X + X^2 + \cdots + X^{\ell-1}$ est irréductible dans $\mathbf{F}_p[X]$ si et seulement si $\overline{p}$ engendre le groupe $\mathbf{F}_\ell^\times$.

(30) ($\star$) Le polynôme $\sum_{i=0}^{23250} X^i$ est-il irréductible dans $\mathbf{F}_2[X]$?

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 `len?`, `range?`, `GF?`, `ZZ?`, `Integers?`.