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

EXAMEN DU LUNDI 19 JANVIER 2015, 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.

Cet examen 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.

Quelques commandes Sage

Pour que de purs problèmes de syntaxes ne vous bloquent pas, voici une liste (non exhaustive) de quelques expressions Sage qu'il pourrait être intéressant d'utiliser dans ce sujet : `Integers`, `GF`, `ZZ.random_element`, `quotient`, `lift`, `resultant`, `discriminant`, `QQ.extension`. .

Problème

On s'interdira dans ce problème d'utiliser des fonctions de Sage permettant de factoriser des polynômes ou de résoudre des équations polynomiales dans les corps finis.

Certaines questions demandent d'implémenter des fonctions qui seront utilisées dans les questions suivantes. Si vous n'y arrivez pas, vous pouvez passer aux questions suivantes et pour y répondre, vous pouvez utiliser dans les codes sources Sage que vous rendez des appels à ces fonctions, même si vous ne les avez pas implémentées. Par ailleurs, pour les applications numériques des deux dernières questions, si vous n'avez pas implémenté complètement la fonction `racine_cubique`*, vous pouvez très bien traiter pas à pas ces deux cas en précisant les différentes étapes de calcul de la méthode proposée dans ce sujet.*

Soit p un nombre premier congru à 1 modulo 3. (On fera toujours cette hypothèse sur p dans ce problème.)

On fixe $x \in \mathbf{F}_p^\times$.

(1) Montrer qu'il existe $y \in \mathbf{F}_p^\times$ tel que $x = y^3$ si et seulement si $x^{\frac{p-1}{3}} = 1$.

(2) En déduire une méthode raisonnablement efficace pour déterminer si x admet une racine cubique dans $\mathbf{F}_p$. Quel est l'algorithme fondamental que l'on utilise ? (On ne demande pas de décrire cet algorithme fondamental en détail.) Estimer le coût de ce calcul en nombre d'opérations arithmétiques dans $\mathbf{F}_p$.

(3) ($\star$) Écrire une fonction dans Sage prenant en arguments un entier relatif a et un nombre premier p et renvoyant `True` si la classe x de a dans $\mathbf{F}_p$ admet une racine cubique et `False` sinon. (On ne demande pas ici d'implémenter l'algorithme fondamental mentionné dans la question précédente.)

On considère la fonction suivante dans Sage :

```
def j(p):
    while True:
        a=GF(p)(ZZ.random_element(1,p))^((p-1)/3)
        if (a!=1):
            return a
```

(4) Montrer que si le calcul `j(p)` termine, alors la valeur renvoyée est un élément $j \in \mathbf{F}_p$ tel que $j \neq 1$ et $j^3 = 1$.

(5) Justifier le fait que le calcul `j(p)` termine *presque sûrement*.

À partir de maintenant, on suppose que $x \in \mathbf{F}_p^\times$ est tel qu'il existe $y \in \mathbf{F}_p^\times$ tel que $x = y^3$. Le but est de déterminer un tel y.

(6) Admettons que l'on dispose d'un élément $y_1 \in \mathbf{F}_p^\times$ tel que $x = y_1^3$. Compte tenu des questions précédentes, expliquer comment il est possible de déterminer explicitement *tous* les éléments $y \in \mathbf{F}_p^\times$ tels que $y^3 = x$. Le polynôme $T^3 - x \in \mathbf{F}_p[T]$ est-il scindé ?

Soit $P = T^3 + aT^2 + bT - x \in \mathbf{F}_p[T]$ un polynôme unitaire de degré 3 (tel que $P(0) = -x$).

(7) Justifier le fait que P est irréductible si et seulement s'il est premier avec $T^p - T$.

(8) ($\star$) Pour calculer le pgcd de $T^p - T$ et de P, on propose l'esquisse d'algorithme suivante : on calcule la classe $R \in \mathbf{F}_p[T]_{<3}$ de T^p modulo P et on applique ensuite l'algorithme d'Euclide aux polynômes P et $R - T$. En utilisant cette idée, implémenter dans Sage une fonction `irred` prenant en argument a, b, x, p et renvoyant `True` si $P = T^3 + a^2 + bT - x$ est irréductible dans $\mathbf{F}_p[T]$ et `False` sinon. (On ne demande pas ici de réimplémenter l'algorithme d'Euclide. On fera en revanche particulièrement attention au fait que l'on souhaite que le programme soit raisonnablement efficace pour des nombres premiers p comme ceux qui interviennent dans les deux dernières questions du problème : 65539 et $\frac{10^{19}+1}{11}$.)

(9) ($\star$) Écrire une fonction `poly_irred` dans Sage prenant en argument x et p et renvoyant un polynôme irréductible de degré 3 de la forme $P = T^3 + aT^2 + bT - x \in \mathbf{F}_p[T]$. (On tirera au sort des coefficients a et b jusqu'à obtenir un polynôme irréductible. On admettra ici que la proportion des couples (a, b) tels que le polynôme P soit irréductible est non nulle.)

Supposons qu'on ait obtenu un polynôme irréductible $P = T^3 + aT^3 + bT^2 - x \in \mathbf{F}_p[T]$. Introduisons le corps de rupture K de $P \in \mathbf{F}_p[T]$; on note $t \in K$ la racine privilégiée de P dans K. On note $\varphi\colon K \to K$ l'automorphisme de Frobenius donné par la formule $\varphi(u) = u^p$ pour tout $u \in K$.

(10) Montrer que $P(t) = P(t^p) = P(t^{p^2}) = 0$. Est-il vrai que $P = (T - t)(T - t^p)(T - t^{p^2})$?

(11) Montrer que $x = t^{1+p+p^2}$.

(12) Montrer que $1 + p + p^2$ est multiple de 3.

(13) Si on pose $y := t^{\frac{1+p+p^2}{3}}$, montrer que l'on a bien $x = y^3$. Démontrer que $y \in \mathbf{F}_p \subset K$.

(14) ($\star$) Définir dans Sage une fonction `racine_cubique` prenant en argument x et p (satisfaisant implicitement aux hypothèses faites jusqu'à présent) et renvoyant $y \in \mathbf{F}_p$ tel que $y^3 = x$.

(15) ($\star$) Déterminer les racines cubiques de 63836 dans $\mathbf{F}_{65539}$.

(16) ($\star$) Posons $p = \frac{10^{19}+1}{11}$ (on admet que c'est un nombre premier). Déterminer les racines cubiques de 2 dans $\mathbf{F}_p$.

Exercice

($\star$) Déterminer les couples de réels $(x, y) \in \mathbf{R}^2$ satisfaisant aux deux équations suivantes :

$$\begin{cases} x^2 + y^2 - 1 &= 0 \\ 7x^2 - 48xy - 7y^2 + 3x + 4y - 10 &= 0 \end{cases}$$

(Une fois que vous vous serez ramené à des équations en une seule variable, vous pourrez utiliser les fonctions de Sage permettant de factoriser des polynômes en une variable à coefficients rationnels ou de déterminer leurs racines.)