(Extrait du Rapport du Jury 2015, Option C.)
Pour beaucoup de candidats le réflexe "pivot de Gauss" ne vient qu'en réponse à des questions concernant les systèmes linéaires, mais son utilisation pour le calcul de déterminants ou de rang est parfois une découverte pour les canditats - cela devrait être une connaissance de base, ou, à défaut, une acquisition indispensable d'un travail de préparation à l'épreuve de modélisation C. Notons également que le coût de cet algorithme reste inconnu de l'écrasante majorité des candidats.

Exercice I: (cf. Faddeev TP05)

Sous xcas ou sage, quel mot clef rechercher pour trouver directement une comatrice d'une matrice A ? Pourquoi xcas rend t'il une grande liste plutot qu'une simple matrice ?

Exercice II: Polynôme minimal. (Cf Problèmes de rang et applications)

Soit v un vecteur et u un endomorphisme de E (E ev de dim n sur un corps infini). On note $P_{u,v}$ un générateur de l'idéal : $\{P \in k[x], P(u)(v) = 0\}$.

1) Expliquer sur un exemple de taille n aléatoire (on commencera par $n = 8$)comment on peut trouver $P_{u,v}$ à partir d'une recherche de noyau.

2) Recommencer sur un exemple où $P_{u,v}$ est de degré inférieur à la dimension de E.

a) Pour expliquer comment la méthode évite de faire plusieurs fois les mêmes calculs, on utilisera d'abord une commande qui donne une forme échelonnée avant de faire des recherches de noyau. Etudiez les commandes de forme échelonnée et échelonnée réduite. Comment interpréter le résultat d'une telle commande avec une matrice contenant des symboles. Ex : `[[a,b],[c,d]]`. Comment connaitre la liste des éléments inversibles qui ont été utilisés ?

b) Optimiser le calcul des $A^k(v)$, et regardez si le polynôme obtenu annule A. Estimer le nombre d'opérations sur le corps de base.

c) Justifier l'intérêt de cette méthode pour trouver le polynôme minimal de u.

3) Etudiez dans la documentation de xcas les différentes options pour calculer le polynôme caractéristique. Expliquez l'intéret de l'option pmin. Illustrez sur des exemples.

Exercice III: (Travail maison, préparez une présentation orale de 15min)

Présentez/Illustrez une méthode de calcul du déterminant d'une matrice à coefficients entiers par réduction modulo des nombres premiers et méthode du pivot dans des corps finis. Expliquez les couts, illustrez sur des exemples...

Quelques questions pour aider à expliquer la méthode sur un exemple :

1) Prendre au hasard une matrice M de taille 20×20 à coefficients entiers compris entre -50 et 50.

a) Prendre deux nombres premiers p_1, p_2 de l'ordre de 2^{30} et calculez $\det(M)$ dans $\mathbb{Z}/p_i\mathbb{Z}$. (Si votre programme est trop lent, vous pouvez utiliser la commande interne).

b) En déduire un représentant de $\det(M)$ dans $\mathbb{Z}/p_1p_2\mathbb{Z}$ de valeur absolue minimale.

c) Ajoutez de nouveaux nombres premiers $p_3, \ldots, p_k$ et continuez jusqu'à ce que la valeur trouvée semble stationnaire, ou alors utilisez une majoration usuelle[2] de $|\det(M)|$ pour en déduire la valeur de $\det(M)$ dans $\mathbb{Z}$.

Exercice IV: Méthode de Berlekamp (cf. Pb de rang, corps finis, polynômes)

1) Créer une fonction `randP(n)` qui donne un polynôme unitaire au hasard de degré n à coefficients inferieurs à 20.

1. `http://webusers.imj-prg/frederic.han/agreg`
2. Hadamard

2) On considère le polynôme P obtenu en développant un produit de 5 éléments de type `randP(rand(7))`

3) Vérifier que P n'a que des racines simples dans $\mathbb{C}$, sinon recommencer.

4) On considère un nombre premier p.

a) Créer une fonction `berl(p,P)` qui calcule la matrice (de Berlekamp) `F` de l'application $\mathbb{Z}/p\mathbb{Z}[x]/(P) \to \mathbb{Z}/p\mathbb{Z}[x]/(P)$ $f \mapsto f^p - f$ dans la base $(x^i)_{0,\ldots,\deg P-1}$. On utilisera une fonction explicite d'xcas/sage pour les puissances rapides.

b) Tester pour différentes valeurs de p si votre polynôme P est dans facteurs multiples dans $\mathbb{F}_p[x]$, et si c'est le cas, calculez le rang de F. Illustrer/Conjecturer un lien entre la dimension du noyau de F, et la factorisation de P sans $\mathbb{Z}/p\mathbb{Z}$.

5) Corps finis non premier.

a) Dans xcas ou sage, quel nom faut il chercher pour construire un corps fini non premier ? Par exemple comment construire et travailler avec des éléments de $\mathbb{F}_{27}$? On notera a la classe de x dans ce corps de rupture. Quel est l'ordre multiplicatif du a lorsque le logiciel choisit lui même le polynome irréductible ? (On pourra lire dans l'aide : `Menu Aide>Algorithmes` la partie sur la représentation des corps non premiers.

b) Trouver (on peut piocher au hasard) un polynôme irreductible de degré 6 dans $\mathbb{F}_3[x]$. Faites le factoriser dans $\mathbb{F}_{27}[x]$ (dans certaines version d'xcas il vaut mieux remonter le polynôme dans $\mathbb{Z}[x]$ avant de l'envoyer dans $\mathbb{F}_{27}[x]$). A quelle condition a t'il une racine dans $\mathbb{F}_{3^n}$?

6) Application pour Factoriser.

a) Choisir un nombre premier impair de préférence[3] plus petit que 20 où le nombre de facteurs de P dans $\mathbb{Z}[x]$ est assez petit, et tel que P ait peu de facteurs dans $\mathbb{Z}/p\mathbb{Z}[x]$, et soit encore sans facteurs multiples dans $\mathbb{Z}/p\mathbb{Z}[x]$ pour cette valeur de p. Le nombre de facteurs est il forcément le nombre de facteurs dans $\mathbb{Z}[x]$? (illustrez)

b) Choisissez au hasard un élément Q du noyau de F pour la valeur de p choisie. Vérifier qu'il convient, et trouver un facteur non trivial de P en remaquant que l'un des 3 pgcd suivant est non trivial dans $\mathbb{Z}/p\mathbb{Z}[x]$: $Q \wedge P$, $Q^{\frac{p-1}{2}} - 1 \wedge P$, $Q^{\frac{p-1}{2}} + 1 \wedge P$.

c) En déduire une méthode pour factoriser un polynôme réduit sur un corps fini.

Exercice V: Remontée Henselienne

On peut prendre le polynôme P précédent ou un autre.

1) Prendre un diviseur A de P dans $\mathbb{Z}/p\mathbb{Z}[X]$. On note $B = P/A$ dans $\mathbb{Z}/p\mathbb{Z}[X]$. Trouver U, V tels que $A.U + B.V = 1[p]$

2) Obtenir un diviseur de P dans $\mathbb{Z}/p^2\mathbb{Z}[X]$ congru à A modulo p. Puis illustrer une remontée aboutissant à un facteur de P dans $\mathbb{Z}[x]$.

3) Illuster que certaines remontées ne donnent pas un facteur dans $\mathbb{Z}[x]$

4) Quel est $max_i C_m^i$? Faire une procédure de m, P : `borne` qui calcule une valeur flottante de ce nombre multiplié par la norme de $P = \sum_i a_i.x^i$: $||P|| = \sqrt{\sum_i |a_i|^2}$.

5) Avec les notations précédentes, on a le Théorème (cf Knuth T2 p 457 ou BPR p147) :

$$Q, P \in \mathbb{Z}[x],\ \deg Q = m, Q = \sum_j b_j x^j, \text{ alors}$$

$$|b_j| \leq ||P||.C_m^j$$

(pour le démontrer on pourra utiliser le lemme :

$$||(z-\alpha).P(z)|| = ||(\bar{\alpha}.z - 1).P(z)||$$

et remarquer que le produit des modules des racines complexes de P de module > 1 est inférieur à $||P||/a_n$.

3. On le prend petit pour éventuellement illustrer la remontée Henselienne ensuite.