Examen du lundi 4 janvier, de 15h à 17h.
Documents autorisés.

1. EXERCICE : INTERSECTION D'UN CERCLE ET D'UNE ELLIPSE

Soit $a > 0$ un réel, C le cercle d'équation $x^2 + y^2 - a^2 = 0$ et E l'ellipse d'équation $ax^2 + y^2 + xy + y - 3 = 0$ (pour une valeur de a fixée, on peut représenter graphiquement E et C dans Xcas avec les instructions `ellipse` et `cercle`). On s'intéresse à l'intersection (dans $\mathbb{R}^2$) de E et C en fonction de a.

(1) Soit $M(x,y)$ un point de $E \cap C$. Déterminer une équation polynômiale $P_a(x) = 0$ vérifiée par x (paramétrée par a) en éliminant y avec les deux équations.

(2) Montrer en utilisant les suites de Sturm que l'intersection est vide lorsque $a = 1$.

(3) Déterminer l'ensemble des points d'intersection lorsque $a = \frac{-1+\sqrt{13}}{2}$.

(4) Pour quelles valeur(s) de a l'équation polynômiale $P_a(x) = 0$ admet-elle une racine multiple ? Que se passe-t-il graphiquement pour cette(ces) valeur(s) de a ?

(5) Esquisser rapidement un raisonnement donnant le nombre de points d'intersection (à coordonnées réelles) en fonction de $a > 0$.

2. PROBLÈME : BEZOUT MODULAIRE (BIS)

Soient A et B deux polynômes à coefficients dans $\mathbb{Z}[X]$, premiers entre eux, de degrés respectifs a et b avec $a \geq b$. Dans cet exercice on veut calculer les polynômes U et V dans $\mathbb{Z}[X]$ tels que

$$AU + BV = \text{resultant}(A,B), \quad \deg(U) < \deg(B), \quad \deg(V) < \deg(A) \tag{1}$$

sans calculer auparavant le résultant de A et B dans $\mathbb{Z}$.

(1) Soit p un nombre premier. On calcule le résultant des polynômes A et B réduits modulo p comme le déterminant d'une matrice à coefficients dans $\mathbb{Z}/p\mathbb{Z}$ (on utilisera `sylvester` avec Xcas). Quelle condition doit vérifier le nombre p pour qu'on puisse l'utiliser pour résoudre (1) dans $\mathbb{Z}$?

(2) On résoud l'équation modulaire pour plusieurs nombres premiers p_i vérifiant la condition ci-dessus et proches de $\sqrt{2^{31}}$. Puis on construit les polynômes $\tilde{U}$ et $\tilde{V}$ en appliquant le théorème des restes chinois aux polynômes solution de (1) modulo p_i, et en les écrivant en représentation symétrique. Donner une condition que doivent vérifier les p_i qui implique que $\tilde{U} = U$ et $\tilde{V} = V$ (justifier très rapidement). Écrire un algorithme permettant de résoudre (1) par cette méthode. Testez-le avec un polynôme A de degré 4 et un polynôme B de degré 3.

(3) Donner un majorant en $O(.)$ du temps de calcul du résultant de A et B modulo p en fonction de a et b.

(4) Quel est le temps nécessaire pour effectuer la division euclidienne d'un polynôme de degré d par un polynôme de degré d' modulo p ? En déduire une majoration du temps nécessaire pour résoudre l'équation de Bézout modulo p en fonction de a et b (lorsqu'on divise R_n par R_{n+1}, où R_n est la suite des restes de l'algorithme d'Euclide, on pourra majorer le degré de R_n par a). Donner une estimation du nombre de nombres premiers nécessaires pour satisfaire à la condition permettant de reconstruire U et V dans $\mathbb{Z}[X]$, en déduire une estimation du temps nécessaire à la résolution de l'équation de Bézout par cette méthode.

(5) Au lieu de résoudre (1) dans $\mathbb{Z}$, on se propose de résoudre $AU + BV = 1$ dans $\mathbb{Q}$ en écrivant le système linéaire correspondant et en lui appliquant une méthode de résolution p-adique. Donner une estimation du temps nécessaire à la résolution de $AU + BV = 1$ par cette méthode et comparer avec l'algorithme modulaire.