Examen du mardi 7 septembre 2009, de 9h à 11h.
Documents autorisés.

1. Intersection d'un cercle et d'une ellipse

Soit $a > 1$ un réel, C le cercle d'équation $x^2 + y^2 - a^2 = 0$ et E l'ellipse d'équation $ax^2 + y^2 - xy - 2y - 4 = 0$ (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 entre 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 à coordonnées réelles lorsque $a = 2\sqrt{3} - 2$ (on donnera le nombre de points d'intersection, une équation exacte vérifiée par l'abscisse des points d'intersection, ainsi qu'une valeur approchée des abscisses possibles, de même pour l'ordonnée).

(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 ? (Indication : on pourra calculer les points d'intersection complexes lorsque $a = 2\sqrt{3} - 2$).

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

2. Déterminant complexe modulaire

Il s'agit dans cet exercice de calculer le déterminant d'une matrice à coefficients dans $\mathbb{Z}[i]$ (partie réelle et imaginaire sont des entiers) par une méthode modulaire.

Soit $p = 1 \pmod 4$ un nombre premier congru à 1 modulo 4. On va construire une racine carrée de -1 modulo p. On calculera ensuite le déterminant modulo p en remplacant i par la racine carrée calculée et par son opposée, puis, on en déduira la partie réelle et imaginaire du déterminant dans $\mathbb{Z}[i]$ modulo p et on reconstruira le déterminant dans $\mathbb{Z}[i]$ par l'algorithme des restes chinois.

(1) Soit $a \in \mathbb{Z}$ non multiple de p et $b = a^{(p-1)/4} \pmod p$. Que vaut $b^4 \pmod p$? En déduire les valeurs possibles de b^2.

(2) Écrire une fonction qui renvoie une racine carrée de -1 modulo p en recherchant un a correspondant à un b tel que $b^2 = -1 \pmod p$ (on admettra que a existe).

(3) Créer une matrice A de taille 7,7 à coefficients complexes dans $\mathbb{Z}[i]$ de valeur absolue majorée par 100. Choisir un premier $p = 1 \pmod 4$ de l'ordre de 2^{60} et calculer $\sqrt{-1} \pmod p$.

(4) Calculer le déterminant de A modulo p en remplacant i par chacune des racines carrées de -1. En déduire la valeur de $\det(A)$ modulo p (indication : résoudre un système de 2 équations dont les 2 inconnues sont la partie réelle et la partie imaginaire du déterminant).

(5) Faire de même pour un autre nombre premier du même ordre de grandeur.

(6) Reconstruire la valeur de $\det(A)$ à partir de ces deux valeurs.

(7) Si A est une matrice n,n à coefficients comme ci-dessus, déterminer en fonction de n le nombre de premiers nécessaires au calcul de $\det(A)$ par cet algorithme, et en déduire une majoration du temps de calcul en fonction de n.

(8) Écrire une fonction mettant en oeuvre cet algorithme.