Examen du lundi 3 janvier 2011 à 13h30.
Documents autorisés.

1. PGCD COMPLEXE MODULAIRE

On cherche à calculer des PGCD de polynômes à coefficients dans $\mathbb{Z}[i]$ avec des méthodes modulaires comme on le fait avec $\mathbb{Z}$.

(1) Montrer que si p est un nombre premier tel que $p = 3 \pmod 4$, alors -1 n'est pas un carré modulo p. On peut alors travailler dans $\mathbb{Z}/p\mathbb{Z}[i]$ qui est un corps (défini comme étant $Z/p\mathbb{Z}[Y]/(Y^2+1)$).

(2) Calculer l'inverse de $2-4i$ modulo 11. Écrire un algorithme de calcul de l'inverse de $a+ib \pmod p$ et testez-le avec l'inverse de $2-4i$ modulo 11.

(3) Donner les détails de l'algorithme d'Euclide pour calculer le PGCD des 2 polynômes
$$P = x^2 + (3+3i)x + 9i, \quad Q = x^2 + (1-4i)x - 4i$$
modulo 7 et 11. Que peut-on en déduire sur ces polynômes dans $\mathbb{Z}[i][X]$?

(4) Décrire un algorithme de calcul de pgcd modulaire dans $\mathbb{Z}[i][X]$ utilisant des premiers congrus à 3 modulo 4, en supposant que les instructions polynomiales modulaires `quo, rem, gcd, lcoeff, ...` fonctionnent dans $\mathbb{Z}/p\mathbb{Z}[i]$.

(5) On suppose que les polynômes sont de degrés au plus n et premiers entre eux, estimer en fonction de n le temps nécessaire pour calculer leur PGCD par cet algorithme. Si les polynômes ont un PGCD de degré non nul, que devient cette estimation ?

2. RÉSULTANT

Soit P un polynôme à coefficients réels et C la courbe représentative de P dans le plan. On cherche à savoir si une même droite du plan peut être tangente à C en deux points distincts d'abscisse respectives x_0 et x_1.

(1) Montrer que cela se produit s'il existe x_0 et x_1 distincts tels que
$$P'(x_0) = P'(x_1), \quad P(x_0) - x_0 P'(x_0) = P(x_1) - x_1 P'(x_1)$$

(2) En déduire, après division par la solution "évidente" $x_0 = x_1$, une condition sur P et x_0 en éliminant x_1 avec un résultant.

(3) Résoudre cette équation pour P quelconque de degré 2, 3 et 4. Quel est le plus petit degré pour lequel une solution existe ?

(4) Donner un exemple de polynôme de degré minimal pour lequel le problème a une solution, ainsi que les valeurs des points et l'équation de la droite bi-tangente.

(5) Peut-on généraliser à une courbe d'équation cartésienne polynômiale en 2 variables $E(x,y) = 0$? (on rappelle que la tangente à la courbe a comme vecteur normal $(\partial_x E, \partial_y E)$). On pourra essayer sur un exemple de courbe de degré total 4, par exemple la courbe de Trott :
$$E(x,y) = 144(x^4+y^4) - 225(x^2+y^2) + 350x^2y^2 + 81 = 0$$