UFR de Mathématiques et Informatique
Université Bordeaux I

Année 2003–2004

Mastère de Mathématiques

Arithmétique 2

Examen du 24 mai 2003

Durée 3 heures

Documents manuscrits et calculettes autorisés.

Exercice I

On considère la courbe plane E d'équation affine $y^2 = x^3 + 3x$.

1) Calculer le discriminant de cette courbe, et en déduire que c'est une courbe elliptique sur tout corps de caractéristique différente de 2 et 3.

2) On considère les points $T = (0,0)$ et $P = (1,2)$ qui appartiennent visiblement à E.

a) Expliquer rapidement pourquoi T est un point d'ordre 2.

b) Calculer explicitement les points $2P$, $3P$, $T + P$ et $T + 2P$ (il n'est pas demandé de calculer $T + 3P$).

3) On considère maintenant la courbe E sur le corps $\mathbb{F}_7 = \mathbb{Z}/7\mathbb{Z}$, et on appelle N le nombre de points de $E(\mathbb{F}_7)$, y compris le point à l'infini.

a) Donner l'inégalité à priori que doit vérifier N (entre deux entiers bien entendu).

b) En se servant des calculs de la question 2b), montrer sans calcul supplémentaire que le point P est d'ordre 4 dans $E(\mathbb{F}_7)$.

c) En utilisant le fait que T n'est pas un multiple de P modulo 7, en déduire que $N = 8$ ou $N = 12$.

d) En remplaçant x par les valeurs de 0 à 6, calculer directement N (remarque : le fait de faire cette question ne vous dispense pas de faire les précédentes).,

Exercice II

La fonction
$$f(x,y,z) = x^3y + y^3z + z^3x + xy^3 + yz^3 + zx^3$$
est visiblement un polynôme symétrique en 3 variables. Exprimer ce polynôme comme polynôme des fonctions symétriques élémentaires σ_1, σ_2 et σ_3. On pourra, soit le faire “à la main”, mais avec risque de ne pas y arriver, soit mieux, en utilisant la méthode algorithmique décrite dans le cours.

Exercice III

On rappelle que si A et B sont deux polynômes de degré respectifs m et n et de coefficients dominants respectifs a et b, le résultant de A et de B est égal à

$$R(A,B) = a^n b^m \prod_{i,j}(\alpha_i - \beta_j) = a^n \prod_i B(\alpha_i) = (-1)^{mn} b^m \prod_j A(\beta_i) \ ,$$

où les α_i et β_j sont les racines de A et B respectivement.

1) a) Calculer $R(B,A)$ en fonction de $R(A,B)$, calculer $R(A,1)$, et si B_1 et B_2 sont deux polynômes calculer $R(A,B_1B_2)$ en fonction de $R(A,B_1)$ et $R(A,B_2)$.

b) Si Q est un polynôme et $C = A - BQ$, calculer $R(C,B)$ en fonction de $R(A,B)$ et du degré de C.

2) On considère les polynômes $P_k(X) = X^k - 1$ et $Q_k(X) = P_k(X+1) = (X+1)^k - 1$, et on appelle R_k le résultant de $P_k(X)$ et $Q_k(X)$.

a) En utilisant les questions précédentes (ou directement si vous le souhaitez) calculer R_k pour $k = 1$, 2 et 3 sous forme factorisée.

b) (Facultatif, à ne faire que si vous avez le temps). De même calculer R_4 sous forme factorisée.

c) Montrer directement que $R_6 = 0$ sans faire de calculs longs.

d) Plus généralement, montrer que $R_{6k} = 0$ pour tout $k \geq 1$.

Exercice IV

On a la factorisation évidente $2^{2n} - 1 = (2^n - 1)(2^n + 1)$. Par contre, $2^{2n} + 1$ n'a a priori pas de factorisation “évidente”. Or on remarque que par exemple $2^6 + 1 = 13 \cdot 5$, $2^{10} + 1 = 41 \cdot 25$, $2^{14} + 1 = 145 \cdot 113$, et qu'il semble y avoir une régularité dans ces factorisations.

1) Montrer que effectivement tout nombre de la forme $2^{2n}+1$ avec n **impair** est un produit de deux nombres plus petits qui peuvent facilement s'exprimer en fonction de n.

2) En généralisant, en déduire une décomposition du polynôme $X^{2n}+1$ pour n impair en produit de deux polynômes de degrés plus petits.. Vous êtes autorisés à résoudre cette question avant la première si vous préferez.

Exercice V

Trouver l'ensemble des points d'intersection des deux courbes planes d'équations respectives $f_1(x,y)=0$ et $f_2(x,y)=0$ avec

$$f_1(x,y)=(y^2+6)(x-1)-y(x^2+1) \quad \text{et} \quad f_2(x,y)=(x^2+6)(y-1)-x(y^2+1)\ .$$

On pourra, soit calculer un résultant, soit (mieux) calculer la base de Gröbner réduite correspondant à (f_1,f_2) pour l'ordre lexicographique (non gradué) $x<y$, et observer que le dernier élément de cette base est un polynôme en y seul ayant deux racines évidentes. Noter qu'il faut donner les valeurs des points (x,y), ni trop ni trop peu.