Université Bordeaux 1
Mathématiques

MHT814 – Courbes Elliptiques
Année 2009–2010

Devoir Surveillé, 22 Mars 2010 (8:00 – 10:00)

Durée 2 heures. Notes de cours et programmes GP autorisés.

La clarté des programmes et la pertinence des commentaires est un élément important d'appréciation.

- Pour répondre aux questions, créer **un seul** fichier pour tout le sujet et séparer les exercices. Nommer le fichier `login.gp`, où *login* est **votre identifiant informatique**. Toutes vos réponses manuscrites et vos résultats numériques doivent être saisis sous forme de commentaires dans le fichier `login.gp`.
- Pour rendre votre travail, envoyez le fichier par courriel à la fin de l'épreuve à l'adresse

$$fabien.pazuki@math.u-bordeaux1.fr.$$

Exercice 1 – Soit $y^2 = x^3 + Ax + B$ une équation affine d'une courbe E avec A et B des éléments d'un corps K vérifiant $-16(4A^3 + 27B^2) \neq 0$. Soit m un entier strictement positif. On s'intéresse dans cet exercice aux polynômes de m-division sur la courbe elliptique E.

1) On définit par récurrence sur m les quantités suivantes :

$$\begin{cases} \psi_0 = 0, \ \ \psi_1 = 1, \ \ \psi_2 = 2y \\ \psi_3 = 3x^4 + 6Ax^2 + 12Bx - A^2 \\ \psi_4 = 4y(x^6 + 5Ax^4 + 20Bx^3 - 5A^2x^2 - 4ABx - 8B^2 - A^3) \\ \psi_{2m+1} = \psi_{m+2}\psi_m^3 - \psi_{m-1}\psi_{m+1}^3 \quad (m \geqslant 2) \\ 2y\,\psi_{2m} = \psi_m(\psi_{m+2}\psi_{m-1}^2 - \psi_{m-2}\psi_{m+1}^2) \quad (m \geqslant 3) \end{cases}$$

Justifier que ce sont bien des polynômes en x, y, A, B.

2) On définit pour tout $m \geqslant 2$ les quantités :

$$\begin{cases} \varphi_m = x\psi_m^2 - \psi_{m+1}\psi_{m-1} \\ 4y\,\omega_m = \psi_{m+2}\psi_{m-1}^2 - \psi_{m-2}\psi_{m+1}^2 \end{cases}$$

Vérifier pour quelques valeurs entières de k que les quantités ψ_{2k+1}, φ_{2k+1}, $y^{-1}\omega_{2k+1}$, $(2y)^{-1}\psi_{2k}$, φ_{2k} et ω_{2k} sont des polynômes en x, y^2, A, B. Pour A, B fixés, ces quantités ne dépendent donc que de x en vertu de l'équation de la courbe E. Vérifier alors sur une liste d'exemples que $\varphi_m(x)$ et $\psi_m(x)^2$ sont premiers entre eux dans $K[x]$.

$\varphi_2 = x\psi_2^2 - \psi_3\psi_1$

$\varphi_2 =$

$n-1+2$

3) Vérifier par récurrence que si $P=(x,y)\in E(K)$ alors pour tout $m\geqslant 2$, si $[m]P\neq 0$ on a
$$[m]P=\left(\frac{\varphi_m(P)}{\psi_m(P)^2},\frac{\omega_m(P)}{\psi_m(P)^3}\right).$$

4) Exemple : Considérons la courbe définie par l'équation $y^2=x^3+x$. Posons $m=2$ et $P=(0,0)$.

(1) Calculer $P+P$.
(2) Calculer $\psi_2(P)$.
(3) Conclure sur l'utilité des racines de ψ_2 et de ψ_m plus généralement.

5) Lister tous les points de 5-torsion à coordonnées dans $\mathbb{F}_{25}$ sur la courbe donnée par $y^2=x^3+1$.

6) Compter le nombre de points de 13-torsion à coordonnées dans $\mathbb{F}_{49}$ sur la courbe donnée par $y^2=x^3+x+1$.

Exercice 2 – On se propose dans cet exercice de calculer quelques logarithmes discrets.

1) Trouver un entier n tel que l'égalité $87=23^n$ soit vraie dans $\mathbb{F}_{101}$.

2) Soit t la classe de X dans $\mathbb{F}_7[X]/(F(X))\simeq\mathbb{F}_{7^5}$, où F est donné par la commande *ffinit*. Trouver un entier n tel que $3t^3+6t^2+5=t^n$.

3) Considérons la courbe E définie par $y^2=x^3+2x+6$. Soit $P=(1,3)$ et $Q=(15967,13808)$ deux points de $E(\mathbb{F}_{20101})$. Trouver un entier n tel que $Q=[n]P$.

4) Considérons la courbe E définie par $y^2=x^3+1$. Soit $P=(t^2+5,5t^3+5t^2+8t+5)$ et $Q=(8t^4+t^3+6t^2+3t,5t^3+t^2+3t)$ deux points de $E(\mathbb{F}_{11^5})$, où t est la classe de X dans $\mathbb{F}_{11}[X]/(F(X))\simeq\mathbb{F}_{11^5}$. Trouver un entier n tel que $Q=[n]P$.

$P=\left(\frac{\varphi_2(P)}{\psi_2(P)^2},\frac{\omega_2(P)}{\psi_2(P)^3}\right)=\frac{-3x^4-6x^2+(4y^2-1)x+\ldots}{(4y^2)}$

$t,\ 3t^3+6t^2+5$

$(n-1)P+(2)P$

$P=\frac{x\psi_2^2(P)+\psi_3\psi_1}{\psi_2^2(P)}\quad\frac{\varphi_{m-1}(P)}{\psi_{m-1}(P)^2},\ \frac{\text{omega } m(P)}{\psi_{m-1}(P)^3}$

$\boxed{3t^3+6t^2+5=(n)t}$

$3Q^3+6Q+5=(n)P$