Université Bordeaux 1 **MHT814 – Courbes Elliptiques**
Mathématiques Année 2010–2011

Devoir Surveillé, 30 Mars 2011 (10:00 – 12:00)

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 $p \geqslant 5$ un nombre premier et soit q une puissance de p. Soit E une courbe elliptique définie sur $\mathbb{F}_q$. Soit m un entier strictement positif. On note $E[m]$ l'ensemble des points P de la courbe E qui vérifient $[m]P = 0$.

1) Montrer que $E[m]$ est non vide.

2) Donner un exemple de courbe sur $\mathbb{F}_5$ telle que $E[2]$ contient au moins deux points.

3) Donner un exemple de courbe sur $\mathbb{F}_{49}$ telle que $E[4]$ contient au moins deux points.

4) On s'intéresse à présent au cas particulier $m = p$. Regardons la courbe E définie sur $\mathbb{F}_7$ par l'équation affine $y^2 = x^3 + x$. Calculer $\mathrm{Card}(E(\mathbb{F}_7))$. Calculer $\mathrm{Card}(E[7])$.

Lorsqu'une courbe E définie sur $\mathbb{F}_p$ vérifie $\mathrm{Card}(E(\mathbb{F}_p)) = p+1$, on dit que c'est une courbe **supersingulière** en p.

5) Montrer que la courbe E définie sur $\mathbb{F}_{23}$ par l'équation $y^2 = x(x-1)(x+2)$ est supersingulière en 23. Calculer $\mathrm{Card}(E[23])$.

6) Considérons la courbe E définie sur $\mathbb{Z}$ par l'équation affine $y^2+y = x^3-x^2-10x-20$. Donner le discriminant de E. Si on réduit l'équation de E modulo un nombre premier p qui ne divise pas le discriminant, on obtient donc une courbe elliptique sur $\mathbb{F}_p$. Trouver tous les nombres premiers p compris entre 5 et 100 tels que E est supersingulière en p.

7) Reprenons la courbe E définie sur $\mathbb{Z}$ par l'équation affine $y^2+y = x^3-x^2-10x-20$. Calculer $\mathrm{Card}(E[p])$ pour tous les nombres premiers p inférieurs à 100. Que remarque-t-on ?

Exercice 2 – On étudie dans cet exercice la notion de **courbe anormale**. Soit p un nombre premier. Une courbe elliptique E définie sur $\mathbb{F}_p$ est dite **anormale en** p si elle vérifie $\mathrm{Card}(E(\mathbb{F}_p)) = p$.

1) Montrer que la courbe E définie sur $\mathbb{F}_{11}$ par l'équation $y^2 = x^3 + x + 5$ est anormale.

2) Quelle est la structure d'un groupe de cardinal p ? Que peut-on en déduire pour $E(\mathbb{F}_p)$?

3) Donner un exemple de courbe anormale pour $p = 19$.

Exercice 3 – On se propose dans cet exercice de calculer quelques logarithmes discrets.

1) Trouver un entier n tel que l'égalité $933 = 59^n$ soit vraie dans $\mathbb{F}_{2011}$.

2) Soit t la classe de X dans $\mathbb{F}_{13}[X]/(F(X)) \simeq \mathbb{F}_{13^3}$, où F est donné par la commande $ffinit$. Trouver un entier n tel que $3t^2 + 10t + 4 = t^n$.

3) Considérons la courbe E définie par $y^2 = x^3 + 3x + 4$. Soit $P = (17, 1238)$ et $Q = (3317, 13320)$ deux points de $E(\mathbb{F}_{20101})$. Trouver un entier n tel que $Q = [n]P$.

4) Considérons la courbe E définie par $y^2 = x^3 + x$. Soit $P = (t^4 + 9, 5t^3 + t^2 + 3t + 6)$ et $Q = (6t^4 + t^3 + 8, 8t^4 + 4t^3 + 2t + 5)$ 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 $Q = [n]P$.