Courbes elliptiques
Cours de M2, mathématiques fondamentales
Université Paris Diderot Paris 7
Marc Hindry (cours), Dominique Bernardi (TD)

EXAMEN DU 6 JANVIER 2016

Les trois exercices sont essentiellement indépendants, un résultat de l'exercice 1 pouvant être admis dans l'exercice 2, question 4.

1. Exercice 1

On considère deux courbes elliptiques et une isogénie $\phi : E_1 \to E_2$ toutes définies sur un corps K.

(1) Posons $D_\phi := \phi^*(0_{E_2}) - \deg(\phi)(0_{E_1})$. Montrer que $2D_\phi$ est un diviseur principal. Est-il toujours vrai que D_ϕ est principal?

(2) On suppose maintenant que K est un corps de nombres, et on note $\hat{h}$ la hauteur de Néron-Tate sur E_1 ou E_2; montrer que

$$\hat{h}(\phi(P)) = \deg(\phi)\hat{h}(P).$$

(3) On choisit $E = E_1 = E_2$ définie par $y^2 = x^3 + x$ sur le corps $K = \mathbb{Q}(i)$. Montrer que

$$\phi(x, y) := (-x, iy)$$

est un automorphisme de E. En déduire que $\mathrm{End}(E) = \mathbb{Z}[i]$.
En considérant l'isogénie $\psi := 1 + \phi$ (i.e. $\psi(P) = P + \phi(P)$), dont on déterminera le degré, montrer que les points P et $\phi(P)$ sont orthogonaux pour l'accouplement de Néron-Tate.

2. Exercice 2

Soit p premier impair[1]. On considère la courbe elliptique E sur $\mathbb{F}_p$ d'équation

$$y^2 = x^3 + x = f(x)$$

(1) Soit $\left(\frac{u}{p}\right)$ le symbole de Legendre (qui vaut 0 pour $u = 0$, vaut $+1$ si u est un carré non nul et -1 si u n'est pas un carré). Rappeler pourquoi

$$|E(\mathbb{F}_p)| = p + 1 + S, \text{ avec } S := \sum_{x \in \mathbb{F}_p} \left(\frac{f(x)}{p}\right) \equiv -A_p \mod p$$

où A_p est le coefficient de x^{p-1} dans $f(x)^{(p-1)/2}$.

(2) Montrer que E est supersingulière (resp. ordinaire) si $p \equiv 3 \mod 4$ (resp. si $p \equiv 1 \mod 4$). En déduire que, si $p \equiv 3 \mod 4$, alors $|E(\mathbb{F}_p)| = p + 1$ et, en particulier, $|E(\mathbb{F}_p)| \equiv 0 \mod 4$.

(3) Si $p \equiv 1 \mod 4$ montrer que $E[2] \subset E(\mathbb{F}_p)$ et en déduire $|E(\mathbb{F}_p)| \equiv 0 \mod 4$.

[1] Rappel de théorie algébrique des nombres : un tel p est somme de deux carrés si et seulement si $p \equiv 1 \mod 4$ et si et seulement si p est décomposé dans l'extension quadratique $\mathbb{Q}(i)/\mathbb{Q}$

(4) On admet (voir exercice 1) que l'anneau des endomorphismes de $E/\mathbb{Q}(i)$ est $\mathbb{Z}[i]$. En déduire que, lorsque $p \equiv 1 \mod 4$, l'anneau des endomorphismes de $E/\mathbb{F}_p$ est $\mathbb{Z}[i]$. [Indication: on utilisera, en le justifiant, le fait que l'homomorphisme de réduction $\mathrm{End}(E/\mathbb{Q}(i)) \to \mathrm{End}(E/\mathbb{F}_p)$ est injectif.]
(5) Soit Fr_p le Frobenius de $E/\mathbb{F}_p$, montrer qu'il s'identifie à $a + bi \in \mathbb{Z}[i] = \mathrm{End}(E)$ tel que $a^2 + b^2 = p$, avec a impair et $|E(\mathbb{F}_p)| = p + 1 - 2a$.
(6) Les conditions $p = a^2 + b^2$ et a impair déterminent a au signe près, pouvez-vous déterminer a, en spécifiant, par exemple, $a \mod 4$?

3. Exercice 3

On se propose d'étudier quelques propriétés de la courbe elliptique E, dont on note 0_E l'origine et dont la partie affine est définie sur $\mathbb{Q}$ par l'équation

$$y^2 + y = x^3 - 4x$$

(1) Vérifier que les points $P_1 = (0, 0)$, $P_2 = (2, 0)$ et $P_3 = (-2, 0)$ appartiennent à $E(\mathbb{Q})$ et que $P_1 + P_2 + P_3 = 0_E$.
(2) Montrer que E a bonne réduction pour $p = 2, 3, 5$ [en fait hors de $p = 13$ et 313] et $\tilde{E}_2(\mathbb{F}_2) \cong \mathbb{Z}/3\mathbb{Z}$, $\tilde{E}_3(\mathbb{F}_3) \cong \mathbb{Z}/7\mathbb{Z}$.
(3) Montrer que le cardinal de $\tilde{E}_5(\mathbb{F}_5)$ est égal à 9. A-ton $\tilde{E}_5(\mathbb{F}_5) \cong \mathbb{Z}/9\mathbb{Z}$ ou $\tilde{E}_5(\mathbb{F}_5) \cong (\mathbb{Z}/3\mathbb{Z})^2$ [[Mes excuses : L'énoncé était erroné et demandait : A-ton $\tilde{E}_5(\mathbb{F}_5) \cong \mathbb{Z}/8\mathbb{Z}$ ou $\tilde{E}_5(\mathbb{F}_5) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ ou $\tilde{E}_5(\mathbb{F}_5) \cong (\mathbb{Z}/2\mathbb{Z})^3$?]]
(4) En déduire que $E(\mathbb{Q})_{tor} = \{0_E\}$ et $E(\mathbb{Q}) \cong \mathbb{Z}^r$ avec $r \geq 1$.
(5) Montrer que $E(\mathbb{R})$ possède deux composantes connexes : la composante neutre qu'on notera $\mathcal{C}_0$ et l'autre compacte dans le plan affine $\mathbb{R}^2$ qu'on notera $\mathcal{C}_1$. Vérifier que P_1 et P_3 sont dans $\mathcal{C}_1$ (resp. P_2 dans $\mathcal{C}_0$). En déduire que P_1, P_3 n'appartiennent pas à $2E(\mathbb{Q})$.
(6) En utilisant la formule de duplication (que l'on justifiera):

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

montrer que P_2 n'appartient pas à $2E(\mathbb{Q})$. [Indication : on pourra montrer que si $2P = P_2$ alors P est à coordonnées entières, avec $x(P)$ pair et considérer les valuations 2-adiques.]
(7) Conclure que P_1, P_2, P_3 engendrent un groupe isomorphe à $\mathbb{Z}^2$. [Nota : en fait ces points engendrent $E(\mathbb{Q})$ qui est donc de rang 2 – ce que l'on ne demande pas de démontrer.]