MAT562 : Examen de 6 Mars 2015

Documents autorisés : poly, notes de cours, notes de PC, dictionnaires.

1. Soit E une courbe elliptique définie sur un corps fini $\mathbb{F}_q$ où q est une puissance d'un nombre premier $p \geq 5$. Peut-on avoir :
   (a) $E(\mathbb{F}_q) = \emptyset$;
   (b) $E(\mathbb{F}_q) = (\mathbb{Z}/2)^2$;
   (c) $E(\mathbb{F}_q) = (\mathbb{Z}/2)^3$;
   (d) $E(\mathbb{F}_q) = \mathbb{Z}/(q+1)$;
   (e) $E(\mathbb{F}_q) = \mathbb{Z}/3q$;
   (f) $\#E(\mathbb{F}_q) = q$ et $\#E(\mathbb{F}_{q^2}) = q^2$?

   Pour chaque réponse 'oui' donner un exemple (de corps $\mathbb{F}_q$ et d'une courbe E sur $\mathbb{F}_q$). Pour chaque réponse 'non', expliquer pourquoi.

2. Soit E une courbe elliptique définie sur $\mathbb{Q}$ par l'équation
$$y^2 = x^3 + x + 1.$$
   (a) Vérifier que $P = (0, 1)$ est sur E et calculer $2P$.
   (b) Montrer que P n'est pas un point de torsion. En déduire que $\hat{h}(P) > 0$ et que $E(\mathbb{Q})$ est infini.

3. Soit E une courbe elliptique définie sur un corps fini $\mathbb{F}_q$ où q est une puissance d'un nombre premier $p \geq 5$. Soit ℓ un nombre premier tel que $\ell | q - 1$.
   (a) Soit $Q \in E(\mathbb{F}_q)$. Montrer qu'il existe $R \in E(\overline{\mathbb{F}}_q)$ tel que $\ell R = Q$.
   (b) Soit $P \in E(\mathbb{F}_q)[\ell]$. Soit $\phi_q : E(\overline{\mathbb{F}}_q) \to E(\overline{\mathbb{F}}_q)$ le morphisme de Frobenius. Montrer que $R - \phi(R) \in E(\overline{\mathbb{F}}_q)[\ell]$.
   (c) Soit $R' \in E(\overline{\mathbb{F}}_q)$ tel que $\ell R' = Q$ et soit $T = R - R'$. Montrer que $\ell T = 0$ et que $e_\ell(P, T) \in \mathbb{F}_q$.
   (d) En déduire que $e_\ell(P, T) = e_\ell(P, \phi(T))$ et que $e_\ell(P, R - \phi(R)) = e_\ell(P, R' - \phi(R'))$.
   (e) Montrer que $e_\ell(P, R - \phi(R))$ ne depend que de la classe de Q dans $E(\mathbb{F}_q)/\ell E(\mathbb{F}_q)$. En déduire qu'on a une application bien définie
$$\tau_\ell : E(\mathbb{F}_q)[\ell] \times E(\mathbb{F}_q)/\ell E(\mathbb{F}_q), (P, Q) \mapsto e_\ell(P, R - \phi(R)).$$
   (f) Montrer que τ_ℓ est une application bilinéaire.

(g) Supposons que $E(\mathbb{F}_q)$ admet un point P d'ordre exact ℓ, mais que ℓ^2 ne divise pas $\#E(\mathbb{F}_q)$. Supposons $\tau_\ell(P,P) = 1$. En admettant que τ_ℓ est un accouplement non dégénéré, montrer qu'il existe $P_1 \in E(\mathbb{F}_q)$ tel que $P = \ell P_1$. En déduire que $\tau_\ell(P,P) = 1$ est une racine primitive ℓ-ième de l'unité.

(h) Sous les hypothèses de la question précédente montrer que l'on peut réduire le problème de logarithme discret pour $E(\mathbb{F}_q)$ au problème de logarithme discret dans $\mathbb{F}_q$.

4. Soit E une courbe elliptique définie sur $K = \mathbb{Q}$ par l'équation

$$y^2 = x(x-2)(x-10).$$

On pose $\alpha_1 = 0, \alpha_2 = 2, \alpha_3 = 10$.

(a) Déterminer $E(\mathbb{Q})[2]$.

(b) Soit S l'ensemble fini de nombres premiers qui divisent $\Delta_E = [(\alpha_1 - \alpha_2)(\alpha_1 - \alpha_2)(\alpha_2 - \alpha_3)]^2$. Déterminer $\mathcal{O}^*_{K,S}/\mathcal{O}^{*2}_{K,S}$.

(c) Soit $\phi : E(\mathbb{Q})/2E(\mathbb{Q}) \to (\mathcal{O}^*_{K,S}/\mathcal{O}^{*2}_{K,S})^3$ le plongement défini comme dans le cours :

$$\phi_i(P) = \begin{cases} x_P - \alpha_i & P \neq P_i = (\alpha_i, 0), 0_E \\ (\alpha_i - \alpha_{i-1})(\alpha_i - \alpha_{i+1}), & P = P_i \\ 1 & P = 0_E. \end{cases}$$

Determiner l'image par ϕ des points de 2-torsion.

(d) Montrer que $\#Im\phi \leq 32$.

(e) Montrer que $(1,-1,-1) \in Im\phi$. En déduire que $(1,-3) \in E(\mathbb{Q})$.

(f) Montrer que $(5,2,10) \in Im\phi$

(g) Montrer que si $\gamma_1 \not\equiv 0 (\text{mod } 5)$ et $\gamma_2 \equiv 0 (\text{mod } 5)$, alors $(\gamma_1, \gamma_2, \gamma_1\gamma_2) \notin Im\phi$.

(h) Montrer que si $(\gamma_1, \gamma_2, \gamma_1\gamma_2) \notin Im\phi$, alors $(5\gamma_1, 2\gamma_2, 10\gamma_1\gamma_2) \notin Im\phi$.

(i) En déduire que $\#Im\phi \leq 16$.

(j) Montrer que $(1,2,2) \notin Im\phi$.

(k) En déduire la valeur du rang de $E(\mathbb{Q})$.