EXERCICES SUR LES COURBES SUPER-SINGULIÈRES

Convention : la locution « la courbe elliptique d'équation $f(x, y) = 0$ » sous-entend que la courbe donnée par l'équation $f(x) = 0$ est non singulière.

Exercice 0.1. Soient k un corps de caractéristique 2 et E la courbe elliptique d'équation
$$y^2 + ay + bxy = f(x),$$
où $a, b \in k$ et $f \in k[x]$ est un polynôme de degré 3.

(1) Pour tout point $p \in E$ calculer $2p$.

(2) Montrer que E est super-singulière si et seulement si $b = 0$.

(3) Si k est algébriquement clos et $b = 0$, montrer qu'il existe un changement de coordonnée tel que E a équation $y^2 + y = x^3$. En particulier, toutes les courbes elliptiques super-singulières sur k sont isomorphes.

(4) On considère les courbes elliptiques super-singulières sur $k = \mathbb{F}_2$ données par les équations suivantes :
$$y^2 + y = x^3 + x + 1, \qquad y^2 + y = x^3 + 1, \qquad y^2 + y = x^3 + x.$$
Montrer que deux à deux elles ne sont pas isomorphes sur $\mathbb{F}_2$.

(5) Montrer que toute courbe super-singulière sur $\mathbb{F}_2$ est isomorphe à une des courbes de la question précédente.

On rappelle que si k est un corps de caracéristique $p > 2$ une courbe elliptique d'équation $y^2 = f(x)$ est super-singulière si et seulement si le coefficient de x^{p-1} dans $f(x)^{\frac{p-1}{2}}$ est nul.

Exercice 0.2. Soient k un corps de caractéristique 3 et E la courbe elliptique d'équation $y^2 = x^3 + ax^2 + bx + c$ avec $a, b, c \in k$. Montrer les faits suivants :

(1) La courbe elliptique E est super-singulière si et seulement si $a = 0$ et $b \neq 0$.

(2) Si $a = 0$, $b \neq 0$ et k algébriquement clos, il existe un changement de coordonnées tel que E est d'équation $y^2 = x^3 + x$. En particulier, toutes les courbes super-singulières sur k sont isomorphes.

(3) Calculer l'invariant j de la courbe $y^2 = x^3 + x$.

(4) Les courbes elliptiques super-singulières sur $k = \mathbb{F}_3$ données par les équations suivantes,
$$y^2 = x^3 - x, \qquad y^2 = x^3 - x + 1, \qquad y^2 = x^3 - x + 2, \qquad y^2 = x^3 + x,$$
sont deux à deux non isomorphes sur $\mathbb{F}_3$.

(5) Les courbes elliptiques précédentes forment une liste complète des courbes elliptiques super-singulière sur $\mathbb{F}_3$.

Exercice 0.3. Soit k un corps de caractéristique $p \geqslant 5$. On considère les courbes elliptiques suivantes :
$$E_0 : \quad y^2 = x^3 + 1, \qquad\qquad E_{1728} : \quad y^2 = x^3 + x.$$
Montrer les faits suivants :

(1) E_0 est super-singulière si et seulement si $p \equiv 2 \pmod 3$.

(2) E_{1728} est super-singulière si et seulement si $p \equiv 3 \pmod 4$.

Soient $p \neq 2$ un nombre premier et $H_p(t) \in \mathbb{F}_p[t]$ le polynôme

$$H_p(t) = \sum_{i=0}^{m} \binom{m}{i}^2 t^i,$$

où $m = \frac{p-1}{2}$. On rappelle que la courbe elliptique E_λ d'équation $y^2 = x(x-1)(x-\lambda)$ est super-singulière si et seulement si $H_p(\lambda) = 0$. Soit D l'opérateur différentiel

$$Df = 4t(1-t)f'' + 4(1-2t)f' - f.$$

Exercice 0.4. Montrer l'égalité suivante :

$$DH_p(t) = p\sum_{i=0}^{m}(p-2-4i)\binom{m}{i}^2 t^i.$$

(1) Déduire de l'égalité précédente que les seules racines multiples possibles de H_p dans $\bar{\mathbb{F}}_p$ sont 0 et 1.

(2) Montrer que 0 et 1 ne sont pas des racines de H_p.

Exercice 0.5. Montrer les faits suivants :

(1) L'application $\lambda \mapsto j(\lambda) = 256\frac{(\lambda^2-\lambda+1)^3}{\lambda^2(\lambda-1)^2}$, a exactement 6 antécedents pour $j \neq 0, 1728$, 2 pour $j = 0$ et 3 pour $j = 1728$.

(2) En caractéristique $p \geqslant 5$, le nombre de courbes elliptiques super-singulières est

$$\frac{1}{6}\left(\frac{p-1}{2} - 2\varepsilon_p(0) - 3\varepsilon_p(1728)\right) + \varepsilon_p(0) + \varepsilon_p(1728),$$

où $\varepsilon_p(j) = 1$ si la courbe elliptique d'invariant j est super-singulière et 0 sinon.

(3) En caractéristique $p > 2$ le nombre de courbes elliptiques super-singulières est

$$\begin{cases} 1 & \text{si } p = 3 \\ [p/12] & \text{si } p \equiv 1 \pmod{12} \\ [p/12]+1 & \text{si } p \equiv 5 \pmod{12} \\ [p/12]+1 & \text{si } p \equiv 7 \pmod{12} \\ [p/12]+2 & \text{si } p \equiv 11 \pmod{12}. \end{cases}$$

(4) On a la formule suivante de Eichler et Deuring :

$$\sum_{\substack{E/\bar{\mathbb{F}}_p \\ \text{super-singulière}}} \frac{1}{\#\operatorname{Aut}(E)} = \frac{p-1}{24}.$$