**ARITHMÉTIQUE DES COURBES ELLIPTIQUES**
**FEUILLE DE TD 6**

**Exercice 1.** Soit $p$ un premier impair et C la courbe sur $\mathbb{Q}_p$ avec équation

$$\mathrm{C}: \qquad y^2 = x^3 + x^2 - 3x - 2.$$

(1) Trouver des coordonnées dans lesquelles l'équation de C devient

$$y^2 = x^3 - 5x^2 + 5x.$$

(2) Montrer que la réduction modulo $p$ de C est non-singulière si et seulement si $p \neq 5$.

(3) Montrer que l'équation de Weierstrass ci-dessus est minimale sur $\mathbb{Q}_5$.

(4) Est-ce que C a réduction additive ou multiplicative modulo 5 ?

(5) Montrer que C a bonne réduction sur $\mathbb{Q}_5(\sqrt[4]{5})$.

**Exercice 2.** On considère la courbe elliptique E sur $\mathbb{Q}$ avec équation de Weierstrass

$$\mathrm{E}: \qquad y^2 = x^3 - 43x + 166.$$

(1) Montrer que pour $p \neq 2, 13$ l'équation ci-dessus est non-singulière modulo $p$. (On acceptera que $27 \times 166^2 - 4 \times 43^3 = 106496$.)

(2) Y a-t-il des points de 2-torsion non nuls définis sur $\mathbb{Q}$ ?

(3) Calculer $|\mathrm{E}(\mathbb{F}_p)|$ pour $p = 3, 5$.

(4) Montrer que $(3, 8)$ est un point de torsion de E.

(5) Déterminer $\mathrm{E}(\mathbb{Q})_{\mathrm{tors}}$.

(6) Montrer que si la réduction modulo $p$ de E est supersingulière, alors $p \equiv -1 \pmod 7$.

Soit $k$ un corps algébriquement clos de caractéristique $\neq 2, 3$. Le *birapport* d'un quadruplet ordonné $(z_1, \ldots, z_4)$ de points deux à deux distincts de $\mathbb{P}^1(k)$ est

$$(z_1, z_2, z_3, z_4) = \frac{z_3 - z_1}{z_3 - z_2} \cdot \frac{z_4 - z_2}{z_4 - z_1} \in \mathbb{P}^1(k) \smallsetminus \{0, 1, \infty\},$$

avec le sens évident quand $z_i = \infty$ pour un certain $i$. Le birapport est invariant sous l'action naturelle de $\mathrm{PGL}_2(k)$.

**Exercice 3.** On considère les couples formés d'une courbe elliptique E sur $k$ et d'une bijection $\sigma\colon \{0, \ldots, 3\} \to \mathrm{E}[2]$, $i \mapsto \sigma_i$ avec $\sigma_0 = 0$. Étant fixé $f \in \mathrm{H}^0(2[0])$ non constant, on pose

$$\lambda(\mathrm{E}, \sigma) := (f(\sigma_0), \ldots, f(\sigma_3)).$$

Montrer les faits suivants :

(1) $\lambda(\mathrm{E}, \sigma)$ ne dépend pas de $f$.

(2) Pour un automorphisme $\alpha \in \mathrm{Aut}(\mathrm{E})$ de E on pose $\alpha * \lambda(\mathrm{E}, \sigma) := \lambda(\mathrm{E}, \alpha \circ \sigma)$. L'orbite de $\lambda = \lambda(\mathrm{E}, \sigma)$ sous l'action de $\mathrm{Aut}(\mathrm{E})$ est :

$$\begin{cases} \{\lambda\} & \text{si } j \neq 0, 1728, \\ \{\lambda, \frac{\lambda-1}{\lambda}, -\frac{1}{\lambda-1}\} & \text{si } j = 0, \\ \{\lambda, \frac{1}{\lambda}\} & \text{si } j = 1728. \end{cases}$$

**Exercice 4.** On se place sur une clôture algébrique $\bar{\mathbb{F}}_p$ de $\mathbb{F}_p$ pour $p \geqslant 5$. Le but de cet exercice est de calculer la cardinalité de l'ensemble

$$\mathscr{E}^{\mathrm{ss}} = \{\text{courbes elliptiques super-singulières sur } \bar{\mathbb{F}}_p\}/\cong .$$

Pour ce faire on pose $m = (p-1)/2$ et on considère le polynôme de Hasse

$$\mathrm{H}_p(\lambda) = \sum_{i=0}^{m} \binom{m}{i}^2 \lambda^i.$$

Pour l'instant on accepte l'identité

$$(*) \qquad 4\lambda(1-\lambda)\mathrm{H}_p'' + 4(1-2\lambda)\mathrm{H}_p' - \mathrm{H}_p \equiv 0 \pmod{p}.$$

(1) Montrer que $\mathrm{H}_p(0) = 1$ et $\mathrm{H}_p(1) = \binom{p-1}{m} \equiv (-1)^m \pmod{p}$.

(2) En utilisant $(*)$ montrer que $\mathrm{H}_p$ n'a pas de zéros multiples.

(3) Détérminer le diviseur de ramification du morphisme

$$j\colon \mathbb{P}^1 \longrightarrow \mathbb{P}^1, \qquad j(\lambda) = 256\frac{(\lambda^2-\lambda+1)^3}{\lambda^2(1-\lambda)^2}.$$

(4) Pour $j = 0, 1728$ on pose $\varepsilon_p(j) = 1$ si la courbe elliptique d'invariant $j$ est supersingulière et $\varepsilon_p(j) = 0$ sinon. Déduire de (3) l'identité

$$|\mathscr{E}^{\mathrm{ss}}| = \frac{p-1}{12} + \frac{2}{3}\varepsilon_p(0) + \frac{1}{2}\varepsilon_p(1728).$$

(5) Conclure que

$$|\mathscr{E}^{\mathrm{ss}}| = \left[\frac{p-1}{12}\right] + \begin{cases} 0 & \text{si } p \equiv 1 \pmod{12}, \\ 1 & \text{si } p \equiv 5 \pmod{12}, \\ 1 & \text{si } p \equiv 7 \pmod{12}, \\ 2 & \text{si } p \equiv 11 \pmod{12}. \end{cases}$$

(6) Montrer $(*)$.