**Examen final du 22 avril 2009 (3 heures)**
Courbes elliptiques (F. Brunault, MA2 Lyon)

*Seules les notes manuscrites du cours sont autorisées.*

**Exercice**

Soit $\Lambda$ un réseau de $\mathbf{C}$. On note $\wp$ la fonction de Weierstraß. Soit $f$ une fonction elliptique, holomorphe sur $\mathbf{C} - \Lambda$ et telle que $\operatorname{ord}_0(f) \geq -2$. Démontrer qu'il existe $a, b \in \mathbf{C}$ tels que $f = a\wp + b$. En déduire la dimension du $\mathbf{C}$-espace vectoriel $\{f \in \mathbf{C}(\Lambda)^*; \operatorname{div}(f) \geq -2[0]\} \cup \{0\}$.

**Problème**

On considère la courbe affine plane, définie sur $\mathbf{Q}$, d'équation

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

**I.** 1. Donner l'équation de sa complétion projective $E$.

2. Vérifier que $E$ est une courbe elliptique définie sur $\mathbf{Q}$.
3. Démontrer que $x$ est une uniformisante au point $P_0 = (0, 0)$.
4. Que vaut $\operatorname{ord}_{P_0} y$ ?
5. Déterminer le diviseur de la fonction rationnelle $g = y + x^2$.
6. Interpréter géométriquement la partie positive de $\operatorname{div}(g)$.
7. Démontrer que $P_0$ est d'ordre 5 dans $E(\mathbf{Q})$.
8. En calculant le discriminant de l'équation, démontrer que celle-ci est minimale en tout nombre premier.
9. Pour quels nombres premiers $p$, la réduction $\widetilde{E}$ de $E$ modulo $p$ est-elle une courbe elliptique sur $\mathbf{F}_p$ ?
10. Démontrer que $\widetilde{P_0} \in \widetilde{E}(\mathbf{F}_p)$ est un point lisse de $\widetilde{E}$.
11. Établir que si $E$ a bonne réduction en $p$, alors 5 divise $|\widetilde{E}(\mathbf{F}_p)|$.
12. Démontrer que $E(\mathbf{Q})_{\text{torsion}}$ est engendré par $P_0$.

Soit $L(E, s) = \sum_{n=1}^{\infty} a_n n^{-s}$ la fonction $L$ associée à $E$. On rappelle, pour tout $p$ premier, la formule $a_p = p + 1 - |\widetilde{E}(\mathbf{F}_p)|$.

**II.** 1. On suppose ici que $E$ a bonne réduction en $p$. Posons $1 - a_p X + pX^2 = (1 - \alpha X)(1 - \beta X)$ avec $\alpha, \beta \in \mathbf{C}$. Démontrer que $\alpha \neq \beta$, puis établir $a_{p^k} = (\alpha^{k+1} - \beta^{k+1})/(\alpha - \beta)$ pour tout $k \geq 0$ (on pourra décomposer en éléments simples).

2. En déduire $|a_{p^k}| \leq (k+1)p^{k/2}$ pour tout $p$ premier et $k \geq 0$.
3. Démontrer, pour tout $n \geq 1$, la majoration $|a_n| \leq d(n)\sqrt{n}$, où $d(n)$ est le nombre de diviseurs positifs de $n$.
4. En déduire $|a_n| \leq 2n$ pour tout $n \geq 1$.
5. Démontrer que la série $L(E, s)$ converge si $s \in \mathbf{C}, \Re(s) > 2$.
6. Démontrer que la série $f_E(z) = \sum_{n=1}^{\infty} a_n e^{2i\pi nz}$ converge et définit une fonction holomorphe sur le demi-plan $\{z \in \mathbf{C}, \Im(z) > 0\}$.
7. Pour tout $s \in \mathbf{C}$, $\Re(s) > 2$, démontrer la relation
$$(2\pi)^{-s}\Gamma(s)L(E, s) = \int_0^{\infty} f_E(iy)y^{s-1}\mathrm{d}y.$$
8. On admet l'équation fonctionnelle $f_E(-\frac{1}{11z}) = -11z^2 f_E(z)$. Démontrer que $L(E, s)$ se prolonge en une fonction entière sur $\mathbf{C}$.
9. Démontrer que $L(E, 1) = 2\sum_{n=1}^{\infty} \frac{a_n}{n} e^{-2\pi n/\sqrt{11}}$.
10. En déduire $L(E, 1) \neq 0$ (on pourra utiliser la question II.4.).
11. Que peut-on (pré)dire sur le groupe $E(\mathbf{Q})$ ?
12. Que prédit la conjecture de Birch et Swinnerton-Dyer sur le groupe de Tate-Shafarevich $Ш(E)$ ? *Indication* : si $\alpha$ est l'unique racine réelle du polynôme $x^3 - x^2 + \frac{1}{4}$, on a $\int_{\alpha}^{+\infty} \frac{\mathrm{d}x}{\sqrt{x^3 - x^2 + \frac{1}{4}}} = 6,346\ldots$