Corrigé de l'examen final du 22 avril 2009
Courbes elliptiques (F. Brunault, MA2 Lyon)

Exercice

Par hypothèse, il existe $a \in \mathbf{C}$ tel que $f(z) = \frac{a}{z^2} + O_{z \to 0}(\frac{1}{z})$. La fonction elliptique $g = f - a\wp$ est holomorphe sur $\mathbf{C} - \Lambda$ et a au plus un pôle simple en 0. Comme la somme des résidus de g doit être nulle, on en déduit que g est holomorphe sur $\mathbf{C}/\Lambda$, donc constante. De plus, la fonction $\wp$ étant non constante, la dimension cherchée vaut 2.

Problème

I. 1. On a $E = V(Y^2Z + YZ^2 - X^3 + X^2Z)$.

2. Si $(x_0, y_0) \in E$ vérifie $2y_0 + 1 = 3x_0^2 - 2x_0 = 0$ alors $y_0 = -\frac{1}{2}$ et $x_0 \in \{0, \frac{2}{3}\}$ ce qui conduit à une impossibilité.

3. L'idéal maximal $\mathfrak{m}$ de $\overline{\mathbf{Q}}[E - \{O\}]$ associé à P_0 est engendré par x et y. D'après l'équation, on a $y \in \mathfrak{m}^2$. Comme P_0 est lisse, la fonction $x \in \mathfrak{m} - \mathfrak{m}^2$ est une uniformisante en P_0.

4. On a $y = x^2 \cdot \frac{x-1}{y+1}$ d'où l'on déduit $\operatorname{ord}_{P_0} y = 2$.

5. La fonction $g = y + x^2$ est régulière sur $E - \{O\}$. Comme $\operatorname{ord}_O y = -3$ et $\operatorname{ord}_O x^2 = -4$, il vient $\operatorname{ord}_O g = -4$. Reste à déterminer les zéros de g et leurs multiplicités. Si g s'annule en $P = (x_0, y_0) \in E$ alors $y_0 = -x_0^2$ et en reportant on a $x_0^3 = x_0^4$ d'où $P \in \{P_0, P_1\}$ avec $P_1 = (1, -1)$. Comme $g = x^3 - y^2$ avec $\operatorname{ord}_{P_0} x^3 = 3$ et $\operatorname{ord}_{P_0} y^2 = 4$, on a $\operatorname{ord}_{P_0} g = 3$. Comme le degré du diviseur de g est nul, il vient $\operatorname{div}(g) = 3[P_0] + [P_1] - 4[O]$.

6. La parabole d'équation $y = -x^2$ coupe la courbe elliptique aux points P_0 et P_1 avec multiplicité 3 et 1 respectivement.

7. La tangente à E en P_0 est la droite $y = 0$. En reportant dans l'équation, il vient $x \in \{0, 1\}$ d'où $-2P_0 = (1, 0)$. Par ailleurs, le diviseur de g étant principal, on a $3P_0 = -P_1 = (1, 0) = -2P_0$, donc P_0 est d'ordre 5. Explicitement $2P_0 = (1, -1)$, $3P_0 = (1, 0)$ et $4P_0 = (0, -1)$.

8. On trouve successivement $b_2 = -4$, $b_4 = 0$, $b_6 = 1$, $b_8 = -1$ et $\Delta = -11$. Ainsi E a bonne réduction en p premier $\neq 11$. Comme $v_{11}(\Delta) = 1 < 12$, l'équation est aussi minimale en $p = 11$.

9. Par la question précédente, la courbe $\widetilde{E}$ (définie sur $\mathbf{F}_p$) est donnée par la même équation que E. C'est une courbe elliptique si et seulement si $\Delta \not\equiv 0 \pmod{p}$ c'est-à-dire $p \neq 11$.

10. On a $P_0 = (0 : 0 : 1)$ donc $\widetilde{P_0} = (0 : 0 : 1)$, qui est un point lisse de $\widetilde{E}$ en considérant la dérivée partielle par rapport à Y.

11. Si E a bonne réduction en p, on a un morphisme (surjectif) de groupes $\pi : E(\mathbf{Q}_p) \to \widetilde{E}(\mathbf{F}_p)$. Comme $\pi(P_0) = \widetilde{P_0} \neq O$, le point $\widetilde{P_0}$ est d'ordre 5 dans $\widetilde{E}(\mathbf{F}_p)$. On conclut par le théorème de Lagrange.

12. Les groupes $\widetilde{E}(\mathbf{F}_2)$ et $\widetilde{E}(\mathbf{F}_3)$ sont d'ordre $\leq 2 \cdot 3 + 1 < 10$ et par la question précédente, ils sont donc isomorphes à $\mathbf{Z}/5\mathbf{Z}$. Montrons que l'application canonique $\pi_2 : E(\mathbf{Q})_{\text{torsion}} \to \widetilde{E}(\mathbf{F}_2)$ est injective. Soit $P \in E(\mathbf{Q})_{\text{torsion}}$ tel que $\pi_2(P) = 0$. Si P est d'ordre $2^\alpha m$ avec m impair, alors $2^\alpha P$ est d'ordre m et le corollaire 4.18 du cours entraîne $2^\alpha P = O$. En considérant la réduction π_3 modulo 3, il vient $2^\alpha \pi_3(P) = 0$ donc $\pi_3(P) = 0$ (on est dans $\mathbf{Z}/5\mathbf{Z}$) et comme l'ordre de P n'est pas divisible par 3 (c'est une puissance de 2), une nouvelle utilisation du corollaire 4.18 entraîne $P = O$. *Remarque* : on pouvait aussi vérifier à la main que $E(\mathbf{Q})[2] = 0$.

II. 1. Si $\alpha = \beta$ alors $\alpha = \pm\sqrt{p}$ et $a_p = 2\alpha = \pm 2\sqrt{p}$, ce qui est absurde puisque $a_p \in \mathbf{Z}$. En décomposant en éléments simples, on trouve

$$\begin{aligned} \frac{1}{1 - a_p X + pX^2} &= \frac{\alpha}{\alpha - \beta} \cdot \frac{1}{1 - \alpha X} - \frac{\beta}{\alpha - \beta} \cdot \frac{1}{1 - \beta X} \\ &= \frac{1}{\alpha - \beta} \Big(\sum_{k \geq 0} \alpha^{k+1} X^k - \sum_{k \geq 0} \beta^{k+1} X^k \Big). \end{aligned}$$

En identifiant dans $1/(1 - a_p X + pX^2) = \sum_{k \geq 0} a_{p^k} X^k$, on obtient le résultat.

2. Supposons $p \neq 11$. D'après les bornes de Hasse $|a_p| \leq 2\sqrt{p}$, donc α et β sont conjugués complexes ce qui entraîne $|\alpha| = |\beta| = \sqrt{p}$. Comme $a_{p^k} = \sum_{j=0}^{k} \alpha^j \beta^{k-j}$, il vient $|a_{p^k}| \leq (k+1)p^{k/2}$. Si $p = 11$ alors $a_{p^k} = a_p^k$ pour tout $k \geq 0$, et comme $|a_p| \leq 1$, le résultat est immédiat.

3. D'après ce qui précède, la majoration $|a_n| \leq d(n)\sqrt{n}$ est vraie si n est une puissance d'un nombre premier. On conclut par multiplicativité (si m et n sont premiers entre eux, alors $a_{mn} = a_m a_n$ et $d(mn) = d(m)d(n)$).
4. Si d divise n alors n/d aussi, et au moins l'un des deux est $\leq \sqrt{n}$, ce qui entraîne la majoration $d(n) < 2\sqrt{n}$, d'où $|a_n| \leq 2n$.
5. Si $\Re(s) > 2$ alors $\sum_{n\geq 1} n^{1-\Re(s)}$ converge, donc $L(E,s)$ converge absolument.
6. Posons $\mathcal{H} = \{z \in \mathbf{C}; \Im(z) > 0\}$. Soit $y_0 > 0$. Si $\Im(z) \geq y_0$ alors $|a_n e^{2i\pi nz}| \leq 2ne^{-2\pi n y_0}$. La série $\sum_{n\geq 1} ne^{-2\pi n y_0}$ étant convergente, la série de fonctions holomorphes $\sum_{n\geq 1} a_n e^{2i\pi nz}$ converge uniformément sur tout compact de $\mathcal{H}$. Elle y définit donc une fonction holomorphe.
7. Soit $s \in \mathbf{C}$, $\Re(s) > 2$. La série de fonctions $\sum_{n\geq 1} a_n e^{-2\pi n y} y^{s-1}$ converge simplement vers $f_E(iy)y^{s-1}$, et on a la majoration

$$\begin{aligned}\int_0^{+\infty} \left|a_n e^{-2\pi n y} y^{s-1}\right| \mathrm{d}y &\leq 2n \int_0^{+\infty} e^{-2\pi n y} y^{\Re(s)-1} \mathrm{d}y \\ &\leq \frac{2n\Gamma(\Re(s))}{(2\pi n)^{\Re(s)}}\end{aligned}$$

qui est le terme général d'une série convergente. Grâce au théorème de convergence dominée, l'intégrale $\int_0^{+\infty} f_E(iy)y^{s-1}\mathrm{d}y$ converge et vaut $\sum_{n=1}^{\infty} \int_0^{+\infty} a_n e^{-2\pi n y} y^{s-1} \mathrm{d}y$, ce qui, par le même calcul que plus haut, donne $(2\pi)^{-s}\Gamma(s)L(E,s)$.
8. La fonction $(2\pi)^{-s}\Gamma(s)$ est méromorphe et ne s'annule pas sur $\mathbf{C}$. Il suffit donc de montrer que le membre de droite se prolonge. Posons $y_0 = 1/\sqrt{11}$. Le changement de variables $y' = 1/(11y)$ échange les intervalles $]0, y_0]$ et $[y_0, +\infty[$, ce qui permet d'écrire

$$\begin{aligned}\int_0^{+\infty} f_E(iy)y^{s-1}\mathrm{d}y &= \int_0^{y_0} f_E(iy)y^{s-1}\mathrm{d}y + \int_{y_0}^{+\infty} f_E(iy)y^{s-1}\mathrm{d}y \\ &= \int_{y_0}^{+\infty} \Big(f_E(iy)y^{s-1} + f_E\big(\frac{i}{11y}\big)\frac{(11y)^{1-s}}{11y^2}\Big)\mathrm{d}y.\end{aligned}$$

Par l'équation fonctionnelle, on a $f_E\big(\frac{i}{11y}\big) = 11y^2 f_E(iy)$ pour tout $y > 0$, ce qui conduit à la formule

$$(1) \qquad \int_0^{+\infty} f_E(iy)y^{s-1}\mathrm{d}y = \int_{y_0}^{+\infty} f_E(iy)\big(y^{s-1} + (11y)^{1-s}\big)\mathrm{d}y.$$

Pour $y \geq y_0$ et $s \in \mathbf{C}$, posons $F(y,s) = f_E(iy)\big(y^{s-1} + (11y)^{1-s}\big)$. La fonction $s \mapsto F(y,s)$ est holomorphe sur $\mathbf{C}$. Il reste à majorer $F(y,s)$ uniformément pour $s \in K$ compact de $\mathbf{C}$. Il existe $C > 0$ telle que $|f_E(iy)| \leq Ce^{-2\pi y}$ pour tout $y \geq y_0$ (on peut prendre $C = 2\sum_{n=0}^{\infty}(n+1)e^{-2\pi n y_0}$). Soient a, b tels que $a \leq \Re(s) \leq b$ pour tout $s \in K$. Alors $|y^{s-1}| = y^{\Re(s)-1} = y_0^{\Re(s)-1}(\frac{y}{y_0})^{\Re(s)-1} \leq y_0^{a-b}y^{b-1}$ d'où $|F(y,s)| \leq C(y_0^{a-b} + 11^{b-1})y^{b-1}e^{-2\pi y}$ pour tout $y \geq y_0$ et $s \in K$. Cette dernière fonction étant intégrable sur $[y_0, +\infty[$, le résultat suit.

9. En évaluant (1) en $s = 1$, il vient $(2\pi)^{-1}L(E,1) = 2\int_{1/\sqrt{11}}^{+\infty} f_E(iy)\mathrm{d}y$ d'où $L(E,1) = 4\pi \sum_{n=1}^{\infty} a_n \int_{1/\sqrt{11}}^{+\infty} e^{-2\pi n y}\mathrm{d}y = 2\sum_{n=1}^{\infty} \frac{a_n}{n} e^{-2\pi n/\sqrt{11}}$.
10. Posons $\lambda = e^{-2\pi/\sqrt{11}}$. Comme $a_1 = 1$ et avec la question II.4., il vient $|L(E,1) - 2\lambda| \leq \frac{4\lambda^2}{1-\lambda}$. Pour démontrer que $L(E,1) \neq 0$, il suffit d'établir $\frac{4\lambda^2}{1-\lambda} < 2\lambda$ c'est-à-dire $\lambda < \frac{1}{3}$. On a par exemple $\frac{2\pi}{\sqrt{11}} \geq \frac{6}{4}$ donc $e^{2\pi/\sqrt{11}} \geq e^{3/2} \geq 1 + \frac{3}{2} + \frac{9}{8} > 3$.
11. La première partie de la conjecture de Birch et Swinnerton-Dyer prédit que $E(\mathbf{Q})$ est fini. En utilisant I.12., on peut donc prédire que $E(\mathbf{Q})$ est d'ordre 5, engendré par P_0.
12. La seconde partie de la conjecture prédit la formule

$$L(E,1) \overset{?}{=} \frac{|\text{Ш}(E)| \cdot \prod_p c_p}{|E(\mathbf{Q})_{\text{torsion}}|^2} \cdot \Big|\int_{E(\mathbf{R})} \omega_E\Big|.$$

Si $p \neq 11$ alors $E_0(\mathbf{Q}_p) = E(\mathbf{Q}_p)$ donc $c_p = 1$. D'après I.12., on a $|E(\mathbf{Q})_{\text{torsion}}| = 5$. L'équation de E peut se mettre sous la forme $(y + \frac{1}{2})^2 = x^3 - x^2 + \frac{1}{4}$. Ce dernier polynôme admettant une unique racine réelle α, le groupe $E(\mathbf{R})$ est connexe (faire un dessin) et $\omega_E = \frac{\mathrm{d}x}{2y+1} = \frac{1}{2}\frac{\pm\mathrm{d}x}{\sqrt{x^3-x^2+\frac{1}{4}}}$. Par le changement de variables $y \leftrightarrow -1-y$, l'intégrale sur $E(\mathbf{R})$ revient au double de l'intégrale sur $\{(x,y) \in E(\mathbf{R}); y \geq -\frac{1}{2}\}$, d'où $|\int_{E(\mathbf{R})} \omega_E| = \int_{\alpha}^{+\infty} \frac{\mathrm{d}x}{\sqrt{x^3-x^2+\frac{1}{4}}}$ et

$$|\text{Ш}(E)| \cdot c_{11} \overset{?}{=} \frac{25L(E,1)}{\Omega_E^+}.$$

Un calcul numérique donne alors $|Ш(E)| \cdot c_{11} \stackrel{?}{=} 1$ (la majoration du premier reste de la série $L(E,1)$ donne déjà que la valeur conjecturale de $|Ш(E)| \cdot c_{11}$ est < 2). En conclusion, on peut prédire que le groupe de Tate-Shafarevich de E est trivial.

Remarques

1. On peut démontrer que $c_{11} = 1$. En effet, cela revient à montrer que l'unique point singulier $(-3,5) \in \widetilde{E}(\mathbf{F}_{11})$ n'est pas dans l'image de $\pi_{11} : E(\mathbf{Q}_{11}) \to \widetilde{E}(\mathbf{F}_{11})$. Supposons par l'absurde que $(x,y) \in E(\mathbf{Q}_{11})$ vérifie $\pi_{11}(x:y:1) = (-3:5:1)$. Alors $x = -3+11t$ et $y = 5+11u$ avec $t,u \in \mathbf{Z}_{11}$, et en reportant dans l'équation, on trouve $66 = 121(11t^3 - 10t^2 + 3t - u^2 - u)$, une contradiction.
2. La finitude de $E(\mathbf{Q})$ a été démontrée par Billing et Mahler (On exceptional points on cubic curves, *J. London Math. Soc.* **15** (1940), pp. 32–43). On peut rendre explicite la 2-descente du théorème de Mordell, la tâche étant compliquée ici par le fait que les points de 2-torsion de E ne sont pas rationnels (ils engendrent un corps de nombres de degré 6). Il est à noter que E n'est autre que la *courbe modulaire* $X_1(11)$, qui paramètre les courbes elliptiques munies d'un point d'ordre 11. Le résultat $E(\mathbf{Q}) \cong \mathbf{Z}/5\mathbf{Z}$ se traduit alors par le fait (non évident) qu'aucune courbe elliptique sur $\mathbf{Q}$ ne peut posséder un point rationnel d'ordre 11.
3. Par la théorie des *symboles modulaires*, on peut démontrer que $L(E,1) = \Omega_E^+/25$. La conjecture de Birch et Swinnerton-Dyer pour E est donc équivalente à l'énoncé $|Ш(E)| = 1$. Comme $L(E,1) \neq 0$, le théorème de Kolyvagin donne la finitude de $|Ш(E)|$. Les travaux récents et très profonds de Kato, joints à ceux de Perrin-Riou et Schneider, donnent une autre démonstration (p-adique) de la finitude de $Ш(E)$ et montrent même que son ordre est une puissance de 2. Enfin, par la 2-descente, $Ш(E)$ n'a pas d'élément d'ordre 2, ce qui achève de démontrer la conjecture (complète) de Birch et Swinnerton-Dyer pour E. En utilisant les théorèmes de Kato et Kolyvagin et des calculs explicites, Stein a récemment vérifié la conjecture de Birch et Swinnerton-Dyer (à un nombre fini de facteurs premiers près) pour beaucoup de courbes elliptiques de rang ≤ 1 sur $\mathbf{Q}$.