Corrigé de l'examen partiel du 4 mars 2009 (2h)
Courbes elliptiques (F. Brunault, MA2 Lyon)

Exercice 1

(1) Posons $P = \sum_{j=0}^{k} a_j X^j$ avec $a_k \neq 0$. La fonction $a_k(\wp')^k$ possède un pôle d'ordre $3k$ en 0, et l'ordre d'annulation en 0 de $\sum_{j=0}^{k-1} a_j(\wp')^j$ est $\geq -3k+3$. On en déduit $\mathrm{ord}_0 P(\wp') = -3k$.

(2) D'après le (1), la fonction $\wp'$ est transcendante sur $\mathbf{C}$ et toute fonction elliptique $f \in \mathbf{C}(\wp')$ non nulle vérifie $\mathrm{ord}_0(f) \in 3\mathbf{Z}$. Comme $\wp$ a un pôle double en 0, on en déduit $\wp \notin \mathbf{C}(\wp')$. Par ailleurs $\mathbf{C}(\Lambda) = \mathbf{C}(\wp, \wp')$ et on sait par l'équation différentielle que $\wp$ est algébrique de degré ≤ 3 sur $\mathbf{C}(\wp')$. Le résultat en découle.

Exercice 2

(1) On a $C = V(F)$ avec $F = Y^2 - X^4 - 1 \in \mathbf{C}[X,Y]$. Montrons d'abord que F est irréductible dans $\mathbf{C}[X,Y]$. Si ce n'est pas le cas alors $F = F_1 F_2$ avec F_1, F_2 non constants. Comme F est unitaire en Y, le coefficient dominant de F_i en Y est inversible dans $\mathbf{C}[X]$, donc constant ; on peut donc supposer les F_i unitaires en Y. Posant $F_i = Y + G_i(X)$, il vient $G_2 = -G_1$ et $X^4+1 = -G_2 G_1 = G_1^2$, ce qui est absurde car X^4+1 est à racines simples. Ainsi, on peut tester la lissité de C en étudiant les dérivées partielles de F.

Si C possède un point singulier (x,y) alors $\partial F/\partial X(x,y) = -4x^3 = 0$ et $\partial F/\partial Y(x,y) = 2y = 0$ donc $x = y = 0$, ce qui est absurde car $(0,0) \notin C$.

La complétion projective $\overline{C}$ de C est donnée par $Y^2Z^2 = X^4 + Z^4$. Pour $Z = 0$ on a $X^4 = 0$ donc l'unique point à l'infini de C est $Q = (0:1:0)$. Dans la carte $Y = 1$, l'équation de $\overline{C}$ s'écrit $z^2 = x^4 + z^4$ et le point $Q = (0,0)$ est singulier. Donc $\overline{C}$ n'est pas lisse.

(2) Soit $\mathfrak{m}$ l'idéal maximal de $\mathbf{C}[C]$ en $P = (0,1)$. On sait que $\mathfrak{m}/\mathfrak{m}^2$ est un $\mathbf{C}$-espace vectoriel de dimension 1, engendré par les classes de x et $y-1$. Comme $(y+1)(y-1) = x^4 \in \mathfrak{m}^2$ et que $y+1 \notin \mathfrak{m}$, il vient en réduisant modulo $\mathfrak{m}^2$ que la classe de $y-1$ est nulle, donc $x \notin \mathfrak{m}^2$ est une uniformisante en P.

(3) Dans $\mathbf{C}(C)$, on a $y - 1 = \frac{x^4}{y+1}$ avec $\mathrm{ord}_P(x) = 4$ et $\mathrm{ord}_P(y+1) = 0$, d'où $\mathrm{ord}_P(y-1) = 4$.

Problème

(1) La complétion projective de E_0 est $E = V(Y^2Z + YZ^2 - X^3)$.

(2) Montrons d'abord que $F = Y^2 + Y - X^3$ est irréductible dans $\overline{\mathbf{F}_p}[X, Y]$. Si ce n'est pas le cas, on a $F = F_1F_2$ et par la même méthode que l'exercice 2 on a $F_i = Y + G_i(X)$. Cela entraîne $G_1 + G_2 = 1$ et $G_1G_2 = -X^3$, et la considération des degrés donne une contradiction.

Si E_0 possède un point singulier (x, y) alors $3x^2 = 2y+1 = 0$. Si $p \neq 3$ alors $x = 0$ d'où $y \in \{0, -1\}$, ce qui est impossible. Si $p = 3$, le point $(-1, 1)$ est singulier. Ainsi E est une courbe elliptique ssi $p \neq 3$.

(3) Dénombrons $E(\mathbf{F}_p)$ en essayant toutes les valeurs de y. Pour $p = 2$, on trouve les points $(0, 0)$ et $(0, 1)$, donc $\operatorname{card} E(\mathbf{F}_2) = 3$ (avec le point à l'infini). Pour $p = 3$, on trouve $(0, 0)$, $(-1, 1)$ et $(0, -1)$ d'où $\operatorname{card} E(\mathbf{F}_3) = 4$. Enfin pour $p = 5$, on trouve $(0, 0)$, $(-2, 1)$, $(0, -1)$, $(1, 2)$ et $(-2, -2)$ d'où $\operatorname{card} E(\mathbf{F}_5) = 6$.

(4) On suppose $p \neq 3$. Soit $P = (x, y) \in E$. Les formules explicites du cours donnent $-P = (x, -y-1)$. Si $2y+1 = 0$ alors $2P = O = (0 : 1 : 0)$. Sinon on pose $\lambda = 3x^2/(2y + 1)$ et $\nu = -(x^3 + y)/(2y + 1)$. En utilisant $(2y + 1)^2 = 4(y^2 + y) + 1 = 4x^3 + 1$, il vient finalement

$$2P = \begin{cases} (\frac{x^4-2x}{4x^3+1}, -\lambda(\lambda^2 - 2x) - \nu - 1) & \text{si } 2y + 1 \neq 0; \\ O & \text{sinon.} \end{cases}$$

(5) On a $3P = O$ si et seulement si $2P = -P$ ce qui équivaut encore à $x(2P) = x(P)$, puisque $2P \neq P$ (on a supposé $P = (x, y) \neq O$). Ainsi $3P = 0$ si et seulement si $4x^3 + 1 \neq 0$ et $(x^4 - 2x)/(4x^3 + 1) = x$. La dernière équation s'écrit $x(x^3 - 2) = x(4x^3 + 1)$, c'est-à-dire $x = 0$ ou $x^3 = -1$ (on a $p \neq 3$), et ces solutions vérifient bien $4x^3 + 1 \neq 0$. Finalement $3P = O$ équivaut à $x = 0$ ou $x^3 = -1$.

(6) Comme $\mathbf{F}_p^*$ est cyclique d'ordre $p - 1$, non divisible par 3, l'application $x \mapsto x^3$ définit une bijection de $\mathbf{F}_p^*$, donc de $\mathbf{F}_p$. Pour chaque $y \in \mathbf{F}_p$, il y a donc exactement un $x \in \mathbf{F}_p$ vérifiant $y^2 + y = x^3$. Ainsi $\operatorname{card} E(\mathbf{F}_p) = p + 1$.

(7a) Comme 3 divise le cardinal du groupe cyclique $\mathbf{F}_p^*$, il existe $j \in \mathbf{F}_p^*$ d'ordre 3. L'application $(x, y) \mapsto (jx, y)$ est bien définie car $(jx)^3 = j^3x^3 = x^3$. Elle est visiblement rationnelle, donc régulière. Comme $u^3 = 1$, u est un automorphisme de E. Remarquons que $u(P+Q) = u(P)+u(Q)$

pour tous $P, Q \in E$; cela résulte par exemple du fait que u est une application affine, donc préserve l'alignement.

(7b) Le Frobenius est donné par $\phi(x, y) = (x^p, y^p)$. On a $u \circ \phi(x, y) = (jx^p, y^p)$ et $\phi \circ u(x, y) = (j^p x^p, y^p) = (jx^p, y^p)$ puisque $p \equiv 1 \pmod 3$. Donc ϕ et u commutent.

(7c) On a $u(O) = O$ et si $u(x, y) = (x, y)$ alors $x = 0$ ce qui entraîne $y \in \{0, -1\}$. Les points fixes de u sont donc $\{O, (0, 0), (0, -1)\}$.

(7d) Comme u laisse stable $E(\mathbf{F}_p)$ et u est d'ordre 3, les orbites de u sont de cardinal 1 ou 3. Comme u a 3 points fixes, le cardinal de $E(\mathbf{F}_p)$ est divisible par 3.

(7e) Soit $P = (x_0, y_0) \in E$. La droite $D : y = y_0$ coupe E aux points $(x_0, y_0), (jx_0, y_0)$ et $(j^2 x_0, y_0)$. Ainsi $D \cap E = \{P, u(P), u^2(P)\}$ et $P + u(P) + u^2(P) = O$. Ceci étant valable pour tout P, il vient $u^2 + u + 1 = 0$.

(7f) On utilise le (5). Si $P \in E$ est d'ordre 3 alors $P = (x, y)$ vérifie $x = 0$, cas déjà étudié, ou $x^3 = -1$ c'est-à-dire $x \in \{-1, -j, -j^2\}$. On a alors $y^2 + y + 1 = 0$ donc $y \in \{j, j^2\}$. Les 8 points d'ordre 3 sont donc

$$\{(0, 0), (0, -1), (-1, j), (-1, j^2), (-j, j), (-j, j^2), (-j^2, j), (-j^2, j^2)\}.$$

(7g) L'ensemble $T = \{P \in E; 3P = O\}$ est un sous-groupe de E. On a vu à la question précédente que T est de cardinal 9 et on constate que $T \subset E(\mathbf{F}_p)$. Par le théorème de Lagrange, le cardinal de $E(\mathbf{F}_p)$ est divisible par 9.

(7h) Par le théorème de structure des groupes abéliens finis, on a $T \cong \mathbf{Z}/9\mathbf{Z}$ ou $T \cong \mathbf{Z}/3\mathbf{Z} \times \mathbf{Z}/3\mathbf{Z}$ mais le premier cas est exclu car les éléments de T ont pour ordre 1 et 3. Le groupe abélien fini $E(\mathbf{F}_p)$ admet ainsi un sous-groupe isomorphe à $\mathbf{Z}/3\mathbf{Z} \times \mathbf{Z}/3\mathbf{Z}$, il ne peut donc être cyclique.

(8) Par (7g), on sait que 9 divise $\operatorname{card} E(\mathbf{F}_7)$. À chaque valeur de $x \in \mathbf{F}_7$ correspondent au plus deux points de $E(\mathbf{F}_7)$, d'où l'estimation $\operatorname{card} E(\mathbf{F}_7) \leq 2 \cdot 7 + 1 < 18$. On a donc $E(\mathbf{F}_7) = T \cong \mathbf{Z}/3\mathbf{Z} \times \mathbf{Z}/3\mathbf{Z}$.

Par (6), on sait que $\operatorname{card} E(\mathbf{F}_{11}) = 12$. Par le théorème de structure, il vient $E(\mathbf{F}_{11}) \cong \mathbf{Z}/12\mathbf{Z}$ ou $E(\mathbf{F}_{11}) \cong \mathbf{Z}/6\mathbf{Z} \times \mathbf{Z}/2\mathbf{Z}$. Pour trancher, il suffit de déterminer les points d'ordre 2 de $E(\mathbf{F}_{11})$ (il y en a 1 dans le premier cas et 3 dans le second). Or si $P = (x, y)$ est d'ordre 2 alors $2y + 1 = 0$ donc $y = 5$ puis $x = 2$. On a donc $E(\mathbf{F}_{11}) \cong \mathbf{Z}/12\mathbf{Z}$.
