**Examen partiel du 4 mars 2009 (2h)**

Courbes elliptiques (F. Brunault, MA2 Lyon)

*Seules les notes manuscrites du cours sont autorisées.*

**Exercice 1**

Soit $\Lambda$ un réseau de $\mathbf{C}$. On note $\mathbf{C}(\Lambda)$ le corps des fonctions elliptiques pour $\Lambda$, et $\wp \in \mathbf{C}(\Lambda)$ la fonction de Weierstraß.

(1) Soit $P \in \mathbf{C}[X]$ un polynôme de degré $k \in \mathbf{N}$. Montrer que $P(\wp')$ admet un pôle d'ordre $3k$ en 0.

(2) Montrer que l'extension $\mathbf{C}(\wp') \subset \mathbf{C}(\Lambda)$ est de degré 3 et qu'une base en est donnée par $(1, \wp, \wp^2)$.

**Exercice 2**

On considère la courbe affine plane $C : y^2 = x^4 + 1$, définie sur $\mathbf{C}$.

(1) Montrer que $C$ est lisse. Qu'en est-il de sa complétion projective ?

(2) Montrer que $x$ est une uniformisante en $P = (0, 1) \in C$.

(3) Déterminer l'ordre d'annulation en $P$ de la fonction $y - 1$.

**Problème**

Soit $p$ un nombre premier. On considère la courbe affine plane $E_0$ d'équation $y^2 + y = x^3$, définie sur $\mathbf{F}_p$.

(1) Quelle est la complétion projective $E$ de $E_0$ ?

(2) Pour quels $p$ la courbe $E$ est-elle une courbe elliptique ?

(3) Calculer le cardinal de $E(\mathbf{F}_p)$ pour $p = 2, 3, 5$.

(4) On suppose que $E$ est une courbe elliptique. Soit $P = (x, y) \in E - \{O\}$. Exprimer $-P$ et $2P$ en fonction de $x$ et $y$ (on donnera $x(2P)$ en termes de $x$ seulement).

(5) En déduire que $3P = O$ si et seulement si $x = 0$ ou $x^3 = -1$.

(6) On suppose $p \equiv 2 \pmod 3$. En remarquant que $x \mapsto x^3$ est une bijection de $\mathbf{F}_p$, montrer que le cardinal de $E(\mathbf{F}_p)$ est $p + 1$.

(7) On suppose $p \equiv 1 \pmod 3$.

(a) Montrer que $\mathbf{F}_p^*$ possède un élément $j$ d'ordre 3 et que $u : (x, y) \mapsto (jx, y)$ définit un automorphisme de $E$.

(b) Montrer que $u$ commute avec l'endomorphisme de Frobenius $\phi$ de $E$.

(c) Quels sont les points fixes de $u$ ?

(d) En déduire que le cardinal de $E(\mathbf{F}_p)$ est divisible par 3.

(e) Montrer que $u^2 + u + 1 = 0$ dans $\mathrm{End}(E)$ (on note $1 = [1]$ l'identité de $E$).

(f) Déterminer les points d'ordre 3 de $E$.

(g) En déduire que le cardinal de $E(\mathbf{F}_p)$ est divisible par 9.

(h) Montrer que $E(\mathbf{F}_p)$ n'est pas cyclique.

(8) Déterminer la structure des groupes $E(\mathbf{F}_7)$ et $E(\mathbf{F}_{11})$.

---