

Licence de Mathématiques
UE2226M ; Algèbre approfondie

Durée : 3 h 00
Polycopiés de cours autorisés
Calculatrices autorisées

Le sujet comporte deux pages ; les deux exercices sont indépendants.

Exercice 1

Fermat a découvert le résultat suivant :

Proposition 1. Soit p un nombre premier arbitraire. Il existe deux entiers naturels x et y tels que

$$p = x^2 + 3y^2$$

si et seulement si $p \equiv 1 \pmod{3}$ ou $p = 3$.

On se propose de démontrer ce résultat. Pour cela, on introduit les anneaux $A = \mathbb{Z}[i\sqrt{3}]$ et $B = \mathbb{Z}[j]$, où $i^2 = -1$ et $j = \frac{-1+i\sqrt{3}}{2}$. Etant donné un élément $\alpha = x + iy\sqrt{3}$ de A ou de B , on note $\bar{\alpha} = x - iy\sqrt{3}$ son conjugué et $N(\alpha) = \alpha\bar{\alpha}$ sa norme.

(1) Préliminaires :

- Montrer que $B = \{\frac{m+in\sqrt{3}}{2} \mid m \text{ et } n \text{ sont des entiers relatifs de même parité}\}$.
- Déterminer les ensembles A^\times et B^\times .
- Montrer que tout élément β de B s'écrit $\beta = u\alpha$, où $\alpha \in A$ et $u \in B^\times$.
- Montrer que l'anneau A n'est pas factoriel (on pourra exhiber deux décompositions de l'entier 4 en produit d'irréductibles).
- Démontrer que l'anneau B est euclidien.
- Soit p un nombre premier impair différent de 3. Notant $\left(\frac{\bullet}{p}\right)$ le symbole de Legendre, montrer que $\left(\frac{-3}{p}\right) = +1$ si et seulement si $p \equiv 1 \pmod{3}$. On utilisera la loi de réciprocité quadratique.

(2) Démonstration de l'énoncé de Fermat :

- Traiter les cas $p = 2$ et $p = 3$.
On suppose désormais que p est un nombre premier impair différent de 3.
- Démontrer l'alternative suivante : soit p reste irréductible dans B , soit il s'écrit $p = \beta\bar{\beta}$, pour β un élément irréductible de B .
- Montrer que si $\left(\frac{-3}{p}\right) = +1$ (autrement dit, si -3 est un carré modulo p) alors p n'est pas premier dans B .
- En déduire que p s'écrit sous la forme $p = \alpha\bar{\alpha}$, où $\alpha \in A$.

Tournez la page, S.V.P.

- (e) On suppose maintenant qu'il existe deux entiers naturels x et y tels que $p = x^2 + 3y^2$. Montrer que $\left(\frac{-3}{p}\right) = +1$.
- (f) Démontrer la proposition de Fermat.

Exercice 2

Soit d un entier relatif supposé sans facteur de puissance quatrième (i.e. si p divise d alors p^4 ne divise pas d) et E_d la courbe elliptique définie sur \mathbb{Q} par l'équation de Weierstrass $y^2 = x^3 + dx$. On se propose de déterminer la partie de torsion $E_d(\mathbb{Q})_{tors}$ du groupe de Mordell-Weil $E_d(\mathbb{Q})$ de E_d .

- (1) (a) Soit p un nombre premier impair ne divisant pas d et \overline{E}_d la réduction de E_d modulo p . Montrer que $\#\overline{E}_d(\mathbb{F}_p) = p + 1$ si $p \equiv 3 \pmod{4}$.
- (b) En déduire que $\#E_d(\mathbb{Q})_{tors}$ divise 4 (on utilisera le théorème de la progression arithmétique de Dirichlet).
- (c) Conclure que $E_d(\mathbb{Q})_{tors}$ est isomorphe à l'un des trois groupes suivants : $\mathbb{Z}/2\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ ou $\mathbb{Z}/4\mathbb{Z}$.
- (2) (a) Démontrer que $E_d(\mathbb{Q})_{tors} \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ si et seulement si $-d$ est un carré.
- (b) On rappelle la formule suivante de duplication d'un point $P = (x, y)$ sur une courbe elliptique C d'équation $y^2 = x^3 + ax + b$: si P n'est pas d'ordre deux, alors l'abscisse de $2P$ est

$$x_{2P} = \frac{x^4 - 2ax^2 - 8bx + a^2}{(2y)^2}.$$

Montrer que l'équation $2P = (0, 0)$ admet une solution si et seulement si $P = (x, y)$ vérifie $x^2 = d$ et $y^2 = 2x^3$, donc si et seulement si $x = 2$ et $d = 4$ (on rappelle que d est supposé sans facteur de puissance quatrième). En déduire que $E_d(\mathbb{Q})_{tors} \simeq \mathbb{Z}/4\mathbb{Z}$ si et seulement si $d = 4$.

- (c) Conclure que

$$E_d(\mathbb{Q})_{tors} \simeq \begin{cases} \mathbb{Z}/4\mathbb{Z} & \text{si } d = 4 ; \\ \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} & \text{si } -d \text{ est un carré ;} \\ \mathbb{Z}/2\mathbb{Z} & \text{sinon.} \end{cases}$$