

Licence de Mathématiques
UE2226M ; Algèbre approfondie

Durée : 2 h 00
Polycopiés de cours autorisés
Calculatrices inutiles

Le sujet comporte DEUX PAGES ; les trois exercices sont indépendants. Il est inutile d'avoir tout traité pour obtenir la note maximale. Ce qui fait doit être bien fait.

Barème indicatif : Exercice 1 : 12 points ; Exercice 2 : 6 points ; Exercice 3 : 12 points.

Exercice 1

Fermat a découvert le résultat suivant :

Proposition 1. *Si p est un nombre premier vérifiant $p \equiv 1$ ou $3 \pmod{8}$, alors il existe deux entiers naturels x et y tels que*

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

Réciproquement, si $p \equiv -1$ ou $-3 \pmod{8}$, alors cette équation n'admet pas de solution en entiers.

On se propose de démontrer ce résultat en travaillant dans l'anneau $A = \mathbb{Z}[i\sqrt{2}]$, où $i^2 = -1$. Etant donné $\alpha = x + iy\sqrt{2} \in A$, on note $\bar{\alpha} = x - iy\sqrt{2}$ son conjugué et $N(\alpha) = \alpha\bar{\alpha}$ la norme. On rappelle que A est Euclidien pour le stathme N et que $A^\times = \{\alpha, N(\alpha) = 1\} = \{\pm 1\}$. Enfin, le symbole de Legendre $\left(\frac{\cdot}{p}\right)$, pour p un premier impair, est multiplicatif et vérifie

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}, \quad \left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}.$$

Soit p un nombre premier impair.

- (1) Démontrer l'alternative suivante : soit p reste irréductible dans A , soit il s'écrit $p = \alpha\bar{\alpha}$, pour α un élément irréductible de A .
- (2) Montrer que si $\left(\frac{-2}{p}\right) = +1$ (autrement dit, si -2 est un carré modulo p) alors p n'est pas premier dans A .
- (3) On suppose qu'il existe deux entiers naturels x et y tels que $p = x^2 + 2y^2$. Montrer que $\left(\frac{-2}{p}\right) = +1$.
- (4) Démontrer la proposition de Fermat.

Exercice 2

Pour chaque conique projective C_i suivante, définie sur \mathbb{Q} , dire s'il existe un point rationnel, et, le cas échéant, paramétrer l'ensemble $C_i(\mathbb{Q})$.

- (1) $C_1 : X^2 - 2Y^2 + 3Z^2 = 0$;
- (2) $C_2 : X^2 - 4Y^2 + 3Z^2 = 0$.

Tournez la page, S.V.P.

Exercice 3

Soit d un entier relatif supposé sans facteur de puissance quatrième (i.e. $p \mid d \Rightarrow p^4 \nmid d$) 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 \bar{E}_d la réduction de E_d modulo p . Montrer que $\#\bar{E}_d(\mathbb{F}_p) = p + 1$ 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 $x = \pm 2$ 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

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