Université P. et M. Curie (Paris VI), Michel Waldschmidt
Deuxième semestre 2007/2008

Master de sciences et technologies 1ère année - Mention : Mathématiques et applications
Spécialité : Mathématiques Fondamentales MO11 : Théorie des nombres (12 ECTS)

`Seul document autorisé : le polycopié`

Contrôle du 29 Février 2008
Durée : 3 heures
Barême approximatif : sur 20

(5/20) **Exercice 1.**

a) Soit θ un nombre réel dans l'intervalle $0 < \theta < 3$. Montrer que les deux propritétés suivantes sont équivalentes.

(i) Il existe une constante $c_1 > 0$ telle que, pour tout nombre rationnel p/q, on ait

$$\left| \sqrt[3]{2} - \frac{p}{q} \right| \geq \frac{c_1}{q^\theta}.$$

(ii) Il existe une constante $c_2 > 0$ telle que, pour tout couple (x, y) d'entiers $\neq (0, 0)$, on ait

$$|x^3 - 2y^3| \geq c_2 |y|^{3-\theta}.$$

b) Montrer qu'il existe une constante $c_3 > 0$ telle que, pour une infinité de couple (x, y) d'entiers, on ait

$$|x^3 - 2y^3| \leq c_3 |y|.$$

(3/20) **Exercice 2.** Soit Δ un nombre réel positif. Donner un exemple d'un polynôme homogène $f(X, Y) = aX^2 + bXY + cY^2$ de degré 2 dont le discriminant $b^2 - 4ac$ est Δ et tel que

$$\min\bigl\{|f(x, y)| \;;\; (x, y) \in \mathbf{Z} \times \mathbf{Z},\ (x, y) \neq (0, 0)\bigr\} = \sqrt{\Delta/8}.$$

(6/20) **Exercice 3.** On désigne par K le corps $\mathbf{Q}(\sqrt{2}, \sqrt{7}, i)$.

a) Quel est le degré de K sur $\mathbf{Q}$? Donner une base de K comme espace vectoriel sur $\mathbf{Q}$.

b) Montrer que K est une extension galoisienne de $\mathbf{Q}$, décrire son groupe de Galois et donner la liste des sous-corps. Pour chacun des sous-corps k décrire le groupe de Galois de K sur k et donner un élément primitif de k sur $\mathbf{Q}$.

`Rappel` : un élément *primitif* d'une extension finie E/F est un élément x de F tel que $F = E(x)$.

c) Soit $f(X) = X^4 + 2X^2 - 7 \in \mathbf{Q}[X]$. Quel est le corps de décomposition de f sur $\mathbf{Q}$? Quel est le corps de décomposition de f sur K ?

(6/20) **Exercice 4.**

Un entier positif D sans facteur carré est dit *congruent* s'il existe un triangle rectangle de cotés rationnels dont l'aire est égale à D ; autrement dit si et seulement s'il existe des nombres rationnels positifs $a, b, c \in \mathbf{Q}$ avec $a^2 + b^2 = c^2$ et $D = ab/2$.

a) Montrez que les solutions (a, b, c) de l'équation $a^2 + b^2 = c^2$ en nombres rationnels strictement positifs sont de la forme

$$c\left(\frac{1-t^2}{1+t^2}, \frac{2t}{1+t^2}, 1\right) \quad \text{avec } t \in \mathbf{Q},\ 0 < t < 1.$$

b) En considérant $x = -t$ et $y = (1 + t^2)/c$, déduisez de la question a) que D est congruent si et seulement si l'équation $Dy^2 = x^3 - x$ a une solution (x, y) dans $\mathbf{Q}^2$ avec $-1 < x < 0$.

c) Dessinez approximativement la courbe $C_D(\mathbf{R})$ d'équation $Dy^2 = x^3 - x$. En utilisant le fait qu'une droite qui intersecte $C_D(\mathbf{R})$ en deux points rationnels, l'intersecte en un troisième point rationnel, montrez que D est congruent si et seulement si l'équation $Dy^2 = x^3 - x$ a une solution dans $\mathbf{Q}^2$ avec $y \neq 0$.

d) Soit $(x, y) \in C_1(\mathbf{Q})$ avec $x > 1$. On a donc $y^2 = x^3 - x$.

(i) Montrez que x est un carré de $\mathbf{Q}$.

(ii) Montrez que $x + 1$ et $x - 1$ sont

- soit tous deux des carrés, i.e. $x \pm 1 = u_\pm^2$
- soit tous deux des doubles de carrés, i.e. $x \pm 1 = 2u_\pm^2$

avec u_+ et u_- dans $\mathbf{Q}$.

(iii) Soit $X(\mathbf{Q}) = \{(t, u, v) \in \mathbf{Q}^3 :\ t^2 - u^2 = 1,\ v^2 - t^2 = 1\}$; montrez que l'application

$$(t, u, v) \mapsto f(t, u, v) = \Big((t + u)(t + v), (t + u)(t + v)(u + v)\Big)$$

induit une bijection de $X(\mathbf{Q})$ sur $C_1(\mathbf{Q}) \setminus \{(-1, 0), (0, 0), (1, 0)\}$.

Indication : en notant $f(t, u, v) = (x, y)$ on pourra vérifier

$$x - 1 = (t + u)(u + v) \quad \text{et} \quad x + 1 = (t + v)(u + v),$$

puis considérer l'application

$$\begin{array}{ccc} C_1(\mathbf{Q}) \setminus \{(-1,0),(0,0),(1,0)\} & \longrightarrow & X(\mathbf{Q}) \\ (x, y) & \longmapsto & g(x, y) = \left(\dfrac{x^2+1}{2y}, \dfrac{x^2-2x-1}{2y}, \dfrac{x^2+2x-1}{2y}\right) \end{array}$$

et vérifier $f \circ g(x, y) = (x, y)$ pour $(x, y) \in C_1(\mathbf{Q}) \setminus \{(-1, 0), (0, 0), (1, 0)\}$.

e) On admet le fait que 1 n'est pas un nombre congruent. En posant $x = a^2/b^2$ et $y = ac^2/b^3$, montrer qu'il n'y a pas d'entiers non nuls a, b, c tels que $a^4 - b^4 = c^4$, i.e. que l'équation de Fermat pour $n = 4$ n'a pas de solutions entières.