UPS – Centre d'Orsay
Mathématiques

Arithmétique – Maîtrise
Année 2003–2004

FEUILLE D'EXERCICES n° 5

Exercice 1 – Soit $p \equiv 1 \pmod 4$, $k \in \mathbb{Z}$ tel que $k^2 \equiv -1 \pmod p$ et $\Lambda \subset \mathbb{Z}^2$ l'ensemble des points (x, y) tels que $x \equiv ky \pmod p$.

a) Montrer que $\Lambda = \{(px + ky, y), x, y \in \mathbb{Z}\}$. Quel est le volume de Λ ? Montrer que Λ contient un point (x, y) tel que $0 < x^2 + y^2 < 2p$.

b) En déduire que $p = x^2 + y^2$.

c) Redémontrer ce résultat (p est somme de deux carrés)
i) en utilisant la principalité de $\mathbb{Z}[i]$.
ii) en considérant $J(\chi, \chi)$ pour un caractère χ d'ordre 4 de $\mathbb{F}_p^*$.

Exercice 2 – Soit $K = \mathbb{Q}(\sqrt{D})$ le corps quadratique imaginaire de discriminant $D < 0$.

a) Montrer que tout idéal de $\mathcal{O}_K$ s'écrit $I = \delta\big(a\mathbb{Z} + \frac{b+\sqrt{D}}{2}\mathbb{Z}\big)$ où $a, b, \delta \in \mathbb{Z}$, $a > 0$, $b^2 \equiv D \pmod{4a}$, et qu'on peut supposer $|b| \leqslant a$. Réciproquement un tel $\mathbb{Z}$-module est un idéal, $NI = a\delta^2$ et $I \cap \mathbb{Z} = \delta a\mathbb{Z}$.

b) Avec les notations de la question précédente, on note $c := \frac{b^2-D}{4a}$.
i) Montrer que $\big(c, \frac{-b+\sqrt{D}}{2}\big)$ est dans la même classe d'idéaux que I.
ii) En déduire que toute classe d'idéaux contient un idéal $J = a\mathbb{Z} + \frac{b+\sqrt{D}}{2}\mathbb{Z}$ avec $|b| \leqslant a \leqslant c := \frac{b^2-D}{4a} \in \mathbb{Z}$, et que l'on peut supposer $b \geqslant 0$ si l'une des inégalités est une égalité. Un idéal possédant une telle base est dit *réduit*.
iii) Montrer que $NJ = a \leqslant \sqrt{|D|/3}$. Comparer avec ce que donnerait le théorème de Minkowski (cf. le dernier exercice).

c) Montrer que $N(aX + \frac{b+\sqrt{D}}{2}Y) = a(aX^2 + bXY + cY^2)$, pour $X, Y \in \mathbb{Q}$.
i) en déduire que $a^2 = \min Nx$ quand x parcourt $J \setminus \{0\}$ [*pour tout X, Y entiers non tout deux nuls, on a $X^2 - |XY| + Y^2 \geqslant 1$*].
ii) Montrer qu'il y a un unique idéal réduit dans chaque classe d'idéaux [*montrer que $ac = \min N(x)$, quand x parcourt $J \setminus \mathbb{Z}$*]. En déduire

Théorème 1. *Soit K un corps quadratique imaginaire de discriminant $D < 0$. Les classes d'idéaux de K sont en bijection avec les triplets (a, b, c) satisfaisant $b^2 - 4ac = D$, $|b| \leqslant a \leqslant c$ et $b \geqslant 0$ si $|b| = a$ ou $a = c$.*

Remarque : D étant fixé, ces triplets sont faciles à énumérer grace à $|b| \leqslant a \leqslant \sqrt{|D|/3}$, $b \equiv D \pmod 2$, et au test $c := \frac{b^2-D}{4a} \in \mathbb{Z}$.

d) Calculer $h\big(\mathbb{Q}(\sqrt{-d})\big)$ pour $d = 3, 4, 7, 8, 11, 12, 15, 16, 19, 20, 43, 48, 163$.

e) Donner la structure du groupe de classes d'idéaux de $\mathcal{O}_K$ pour $K = \mathbb{Q}(\sqrt{-21})$ et $K = \mathbb{Q}(\sqrt{-23})$.

Exercice 3 – Soit p un nombre premier.

a) Montrer que si $K = \mathbb{Q}(\sqrt{D})$ est de discriminant D alors $p\mathcal{O}_K$ s'écrit sous la forme $\wp$, $\wp^2$ ou $\wp\overline{\wp}$ suivant la valeur du caractère de Legendre $\left(\frac{\Delta}{p}\right)$. Etudier le cas $p = 2$.

b) Montrer que l'équation $x^2 + 3y^2 = p$ admet une solution en nombres entiers si et seulement si $p \not\equiv 2 \pmod 3$.

Exercice 4 – Soit $n > 0$. Montrer les égalités suivantes :

$$\frac{1}{4}\#\{(x,y) \in \mathbb{Z}^2,\ x^2 + y^2 = n\} = \sum_{\substack{d|n \\ d\equiv 1 \pmod 4}} 1 - \sum_{\substack{d|n \\ d\equiv 3 \pmod 4}} 1.$$

$$\frac{1}{6}\#\{(x,y) \in \mathbb{Z}^2,\ x^2 + xy + y^2 = n\} = \sum_{\substack{d|n \\ d\equiv 1 \pmod 3}} 1 - \sum_{\substack{d|n \\ d\equiv 2 \pmod 3}} 1.$$

On suppose maintenant n impair

$$\frac{1}{2}\#\{(x,y) \in \mathbb{Z}^2,\ x^2 + 7y^2 = n\} = \sum_{\substack{d|n \\ d\equiv 1,2,4 \pmod 7}} 1 - \sum_{\substack{d|n \\ d\equiv 3,5,6 \pmod 7}} 1.$$

[*on pourra montrer que* $\mathbb{Z}[i]$, $\mathbb{Z}[j]$ *et* $\mathbb{Z}[\frac{1+\sqrt{-7}}{2}]$ *sont principaux, et considérer les idéaux de norme* n]

Exercice 5 – Dans cet exercice, on utilisera le résultat suivant :

Théorème 2 (Minkowski)**.** *Soit* K *un corps de nombre,* $n = [K : \mathbb{Q}]$ *son degré,* D_K *son discriminant. On note encore* r_1 *le nombre de plongements de* K *dans* $\mathbb{R}$ *et* $2r_2$ *le nombre de plongements de* K *dans* $\mathbb{C}$ *non réels* ($r_1 + 2r_2 = n$)*. Alors toute classe d'ideaux de* $\mathcal{O}_K$ *possède un représentant entier* $I \subset O_K$ *tel que*

$$N(I) \leqslant \left(\frac{4}{\pi}\right)^{r_2} \frac{n!}{n^n}\sqrt{|D_K|}.$$

Soit $K = \mathbb{Q}(\alpha)$, $\alpha^3 = 7$.

a) Montrer que $\mathcal{O}_K = \mathbb{Z}[\alpha]$ et calculer D_K.

b)i) Etudier la décomposition de $3\mathcal{O}_K$ et de $7\mathcal{O}_K$.

ii) Soit $p \neq 3, 7$ un nombre premier. Montrer que $p\mathcal{O}_K$ est premier ssi $7 \notin (\mathbb{F}_p^*)^3$.

iii) Si $p \equiv -1 \pmod 3$. Montrer que $p\mathcal{O}_K = \wp\wp'$ et calculer $e_{\wp/p}$, $f_{\wp/p}$.

iv) Si $p \equiv 1 \pmod 3$. Montrer que si $7 \in (\mathbb{F}_p^*)^3$ on a $p\mathcal{O}_K = \wp_1\wp_2\wp_3$.

c) Montrer que

$$N_{K/\mathbb{Q}}(a + b\alpha + c\alpha^2) = a^3 + 7b^3 + 49c^3 - 21abc$$

puis calculer le nombre de classes h_K et donner le groupe des classes [*montrer que les idéaux premiers au dessus de* $2, 3, 5$ *ne sont pas principaux*]