Université de Rennes 1
UFR mathématiques
Master 1

Examen terminal de Théorie des nombres
(Jean-Pierre Escofier)
17 décembre 2008

Barême envisagé : 6 points pour l'exercice I ; 14 points pour l'exercice II.
Documents de cours et de TD autorisés. Calculatrices non autorisées.
Il sera tenu compte de la qualité de la présentation et de la rédaction.

I- On pose $\alpha = \sqrt{41}$; on note K le corps $\mathbb{Q}[\alpha]$ et A l'anneau des entiers algébriques de K.

1) Décrire les éléments de A.
2) Déterminer le développement de α en fraction continue.
3) En déduire une solution en nombres entiers de l'équation

$$x^2 - 41y^2 = -1.$$

4) Trouver, à partir de la solution trouvée dans la question précédente, une solution en nombres entiers de l'équation

$$x^2 - 41y^2 = 1.$$

5) Décrire l'ensemble $A^\times$ des unités de A.

Tournez la page pour l'exercice II.

II-

1) Calculer les symboles de Legendre $\left(\frac{6}{p}\right)$ pour $p = 29, 31, 43, 47, 73$.

2) Soit p un nombre premier, $p \geqslant 6$. Quelles sont les seules valeurs que peut prendre $p \bmod 24$?

3) On note E l'ensemble des nombres premiers tels que $\left(\frac{-6}{p}\right) = 1$ et F l'ensemble des nombres premiers tels que $\left(\frac{-6}{p}\right) = -1$. Déterminer E et F à l'aide de congruences modulo 24.

4) Montrer que si $p \in E$, alors p est représenté proprement par une forme quadratique réduite

$$q(x, y) = ax^2 + 2bxy + cy^2$$

de discriminant 6.

5) Déterminer, à l'aide de la description donnée en cours, les formes quadratiques définies positives réduites de discriminant 6.
On les notera q_1 et q_2.

6) Montrer que E se décompose en deux sous-ensembles :
- l'ensemble des p tels que p soit représenté proprement par q_1 ;
- l'ensemble des p tels que p soit représenté proprement par q_2.

7) On peut, bien sûr, trouver directement par essais successifs une solution en nombres entiers de $x^2 + 6y^2 = 73$; on demande de montrer comment le théorème de Minkowski permet de retrouver cette solution.

Corrigé

I- On pose $\alpha = \sqrt{41}$; on note K le corps $\mathbb{Q}[\alpha]$ et A l'anneau des entiers algébriques de K.

1) Comme $41 = 1 \bmod 4$, les éléments de A sont de la forme $u+v(1+\alpha)/2$ avec u, v entiers ; on peut aussi les décrire comme les éléments de la forme $(u + v\alpha)/2$ avec u, v entiers de même parité.

2) $\alpha = 6 + \alpha - 6 = 6 + \dfrac{1}{(\alpha+6)/5} = 6 + \dfrac{1}{2 + (\alpha-4)/5}$
$= 6 + \dfrac{1}{2 + \dfrac{1}{(\alpha+4)/5}} = 6 + \dfrac{1}{2 + \dfrac{1}{2 + (\alpha-6)/5}}$
$= 6 + \dfrac{1}{2 + \dfrac{1}{2 + \dfrac{1}{(\alpha+6)}}}$.
Comme le terme suivant est 12, on a $\alpha = [6, \overline{2, 2, 12}]$.

3) La première fraction est $6 + \dfrac{1}{2 + \dfrac{1}{2}} = 32/5$; comme la période est impaire, on obtient la solution $x = 32, y = 5$ de l'équation $x^2 - 41y^2 = -1$. Vérification : $32^2 - 41 \times 25 = 1024 - 1025 = -1$.

4) Le carré de $32+5\alpha$ est $2049+320\alpha$; il donne la solution $x = 2049, y = 320$ de l'équation $x^2 - 41y^2 = 1$. Vérification : $2049^2 - 41 \times 102400 = 1024 - 1025 = 4198401 - 4198400 = 1$.

5) Les unités de $\mathbb{Z}[\alpha]$ forment un groupe isomorphe à $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}$ que les questions précédentes permettent de déterminer ; à $(a, b) \in \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}$ correspond l'élément $(-1)^a(32 + 5\alpha)^b)$.
Les unités de A forment aussi un groupe $A^\times$ isomorphe à $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}$. Montrons qu'il est identique au groupe précédent.
Une unité de A est un élément de la forme $(u+v\alpha)/2$, avec u, v entiers de même parité, de norme ± 1. On a donc $u^2 - 41v^2 = \pm 4$.
Si u et v sont pairs, on a $u = 2u'$, $v = 2v'$ avec $u', v' \in \mathbb{Z}$ et on se ramène à $u'^2 - 41v'^2 = \pm 1$. D'après les questions précédentes, les solutions sont $\pm(32 + 5\alpha)^b)$, avec $b \in \mathbb{Z}$.
Si u et v sont impairs, on a $u = 2u' + 1$, $v = 2v' + 1$ avec $u', v' \in \mathbb{Z}$, d'où $u'^2 + u' - 41(v'^2 + v') = 10 \pm 1$. Comme $k^2 + k$ est pair pour tout k entier, le premier membre est pair et on ne peut avoir de solution.

II-

1) On peut d'abord vérifier que les nombres 29, 31, 43, 47, 73 sont premiers. On effectue alors les calculs en utilisant la loi de réciprocité.
$\left(\frac{6}{29}\right) = \left(\frac{2}{29}\right)\left(\frac{3}{29}\right) = (-1) \times (-1)^{(2\times 28)/4}\left(\frac{2}{3}\right) = 1$; on a $6 = 8^2 \bmod 29$.
$\left(\frac{6}{31}\right) = \left(\frac{2}{31}\right)\left(\frac{3}{31}\right) = 1 \times (-1)^{(2\times 30)/4}\left(\frac{1}{3}\right) = -1$.
$\left(\frac{6}{43}\right) = \left(\frac{2}{43}\right)\left(\frac{3}{43}\right) = (-1) \times (-1)^{(2\times 42)/4}\left(\frac{1}{3}\right) = 1$; on a $6 = 7^2 \bmod 43$.
$\left(\frac{6}{47}\right) = \left(\frac{2}{47}\right)\left(\frac{3}{47}\right) = 1 \times (-1)^{(2\times 46)/4}\left(\frac{2}{3}\right) = 1$; on a $6 = 10^2 \bmod 47$.
$\left(\frac{6}{73}\right) = \left(\frac{2}{73}\right)\left(\frac{3}{73}\right) = 1 \times (-1)^{(2\times 72)/4}\left(\frac{1}{3}\right) = 1$; on a $6 = 15^2 \bmod 73$.

2) Un nombre premier, $p \geqslant 6$, n'est pas un multiple de 2, 3 ; on en déduit que $p \bmod 24 = 1, 5, 7, 11, 13, 17, 19, 23$; donnons un exemple des deux premières possibilités : 73 et 29 ; les six suivantes sont données par les restes eux-mêmes.

3) On a : $\left(\frac{-6}{p}\right) = (-1)^{(p-1)/2}\left(\frac{2}{p}\right)\left(\frac{3}{p}\right) = (-1)^{(p^2-1)/8} \times (-1)^{(p-1)/2}\left(\frac{p}{3}\right)$.
D'où $\left(\frac{-6}{p}\right) = \left(\frac{2}{p}\right)\left(\frac{p}{3}\right)$. On construit le tableau suivant à partir des congruences modulo 8 et modulo 3.

$p \bmod 24$	1	5	7	11	13	17	19	23
$\left(\frac{2}{p}\right)$	1	-1	1	-1	-1	1	-1	1
$\left(\frac{p}{3}\right)$	1	-1	1	-1	1	-1	1	-1
$\left(\frac{6}{p}\right)$	1	1	1	1	-1	-1	-1	1

On a donc $E = \{1, 5, 7, 11\}$ et $F = \{13, 17, 19, 23\}$ (modulo 24).

4) Si $p \in E$, alors p est diviseur propre de la forme quadratique positive $x^2 + 6y^2$ puisqu'il existe x_0 tel que $x_0^2 = -6 + kp$, soit $x_0^2 + 6 = kp$ avec $\text{pgcd}(x_0, 1) = 1$; on a nécessairement $k > 0$. Il est donc représenté proprement par une forme quadratique réduite positive de discriminant 6. Une variante est de dire que p est représenté proprement par la forme $kx^2 + 2x_0xy + py^2$ dont le discriminant est $kp - x_0^2 = 6$.

5) Si $ax^2 + 2bxy + cy^2$ est une forme quadratique réduite de discriminant 6, on a $0 < a \leqslant 2\sqrt{6/3}$, $|b| \leqslant \sqrt{6/3}$, d'où $a = 1, 2$ et $b = 0, 1$; on est conduit aux formes $q_1(x, y) = x^2 + 6y^2$ et $q_2(x, y) = 2x^2 + 3y^2$.

6) On sait que p est représenté par q_1 ou q_2. Si p est représenté par q_1, on a $x \neq 0 \bmod 6$; Si p est représenté par q_2, on a $x \neq 0 \bmod 3$. En raisonnant modulo 3, on voit qu'on ne peut avoir $x^2 - 6y^2 = p = 2u^2 - 3v^2$ d'où $x^2 = 2u^2 \bmod 3$; puisque $x, u \neq 0 \bmod 3$, 2 serait un carré modulo 3, contradiction. Par conséquent, E et F sont disjoints.
Si $p = 1 \bmod 24$, on ne peut avoir $p = 2x^2 + 3y^2$ car on aurait $2x^2 = 1 \bmod 3$, 2 serait un carré modulo 3, contradiction. Donc $p = x^2 + 6y^2$; par exemple : $73 = 7^2 + 6 \times 2^2, 97 = 1^2 + 6 \times 4^2, 193 = 13^2 + 6 \times 2^2$.
Si $p = 5 \bmod 24$, on ne peut avoir $p = x^2 + 6y^2$ car on aurait $x^2 = 2 \bmod 3$, 2 serait un carré modulo 3, contradiction. Donc $p = 2x^2 + 3y^2$; par exemple : $29 = 2\times1^2+3\times3^2, 53 = 2\times5^2+3\times1^2, 101 = 2\times7^2+3\times1^2$.
Si $p = 7 \bmod 24$, on ne peut avoir $p = 2x^2 + 3y^2$ car on aurait $2x^2 = 1 \bmod 3$, 2 serait un carré modulo 3, contradiction. Donc $p = x^2 + 6y^2$; par exemple : $7 = 1^2 + 6 \times 1^2, 31 = 5^2 + 6 \times 1^2, 103 = 7^2 + 6 \times 3^2$.
Si $p = 11 \bmod 24$, on ne peut avoir $p = x^2 + 6y^2$ car on aurait $x^2 = 2 \bmod 3$, 2 serait un carré modulo 3, contradiction. Donc $p = 2x^2 + 3y^2$; par exemple : $11 = 2\times2^2+3\times1^2, 59 = 2\times4^2+3\times3^2, 83 = 2\times2^2+3\times5^2$.

7) On peut, bien sûr, trouver directement par essais successifs une solution en nombres entiers de $x^2 + 6y^2 = 73$. Pour utiliser le théorème de Minkowski, on part de $33^2 = -6 \bmod 73$. On construit le réseau des points $x = 33y \bmod 73$. Une base de ce réseau est formée de $(33, 1)$ et $(-40, 1)$. Le volume du réseau est 73. On prend des convexes ellipses d'équation $x^2 + 6y^2 = r^2$; leur surface est $\pi r^2/\sqrt{6}$; on prend r de façon que son aire soit $\geqslant 4 \times 73$, soit $r \geqslant 15,09$ environ. On trouve alors des points (x, y) tels que $x^2 + 6y^2 < 228$, d'où $x^2 + 6y^2 = 73k$ avec $k = 1, 2, 3$. Le point (7,2) y est.

Un tableau des points du réseau proches de 0 au sens de x^2+6y^2 petit donne :

$y=1$	-40	33
$y=2$	-7	66
$y=3$	-47	26
$y=4$	-14	59
$y=5$	-54	19
$y=6$	-21	52

Le seul point avec $y>0$ tel que $x^2+6y^2<228$ est le bon.
On peut chercher un argument valable pour tout p premier tel que $p=1 \bmod 24$. On note a tel que $a^2=-6 \bmod p$ et on choisit le réseau des $x=ay \bmod p$. Une base de ce réseau est formée par les vecteurs $(a,1)$ et $(a-p,1)$; son volume est p. On prend r de façon que $\pi r^2/\sqrt{6} \geqslant 4\times p$, soit $r \geqslant 2\sqrt{\sqrt{6}p/\pi}$; un point du réseau situé dans la zone ainsi définie vérifie $x^2+6y^2 \leqslant 4\sqrt{6}p/\pi \approx 3,11p$, d'où $x^2+6y^2=kp$ avec $k=1,2,3$. Si $k=3$, on a $x^2+6y^2=3p$, d'où $x=0 \bmod 3$, $x=3u$ donc $3u^2+2y^2=p$, ce qui est impossible. Si $k=2$, on a $x^2+6y^2=2p$, d'où $x=0 \bmod 2$, $x=2u$ donc $2u^2+3y^2=p$, ce qui est impossible. Finalement, $k=1$.
Une solution de $x^2+6y^2=73$ diffère de la précédente à une unité de $\mathbb{Z}[\imath\sqrt{6}]$ près. Les solutions de $x^2+6y^2=73$ sont donc $\pm(7,2)$.