Université des Sciences et Technologies de Lille
U.F.R. de Mathématiques

Licence Sciences et Technologies A - MIMP
M 36 "Arithmétique et introduction à la théorie des nombres"
DS du 11 janvier - 2011
Durée : 2 heures
SANS DOCUMENT NI CALCULATRICE

Avertissement : on insiste sur la nécessité de fournir des arguments complets, rédigés de façon claire et ordonnée, pour justifier les réponses. Le barème donné a seulement une valeur indicative.

Exercice 1

Soit $\mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}\}$ l'anneau des entiers de Gauss. Rappelons que si x est un élément de $\mathbb{Z}[i]$, sa norme $N(x) = x\bar{x}$ ou $\bar{x}$ est le conjugué complexe de x.

1. Montrer que pour tous $x, y \in \mathbb{Z}[i]$,
$$N(xy) = N(x)N(y). \tag{1}$$

2. Un triplet pythagoricien (a, b, c) est un triplet d'entiers positifs vérifiant la relation de Pythagore : $a^2 + b^2 = c^2$.
On considère les nombres $x = m + ni \in \mathbb{Z}[i]$ tels que : $0 < n < m$. En utilisant l'identité (1) avec $x = y$, montrer qu'il y a une infinité de triplets pythagoriciens.

3. Le but de cette question est de montrer que si p est un nombre premier (dans $\mathbb{Z}$) vérifiant : $p \equiv 1 \pmod 4$, alors p n'est pas irréductible dans $\mathbb{Z}[i]$. Rappelons d'abord le théorème de Wilson : Si q est un nombre premier, alors
$$(q-1)! \equiv -1 \pmod q.$$
   (a) Soit p un nombre premier (dans $\mathbb{Z}$) tel que $p \equiv 1 \pmod 4$. En écrivant
$$(p-1)! = (1.2\ldots\frac{p-1}{2})((p-\frac{p-1}{2})\ldots(p-2)(p-1))$$
   et en utilisant le théorème de Wilson, montrer qu'il existe $m \in \mathbb{Z}$ tel que $m^2 \equiv -1 \pmod p$.
   (b) Rappelons que si un élément irréductible x de $\mathbb{Z}[i]$ divise yz alors x divise y ou x divise z. Montrer que p ne divise ni $(m + i)$ ni $(m - i)$ dans $\mathbb{Z}[i]$.

(c) Conclure.

4. Décomposer 13 (resp. 17) en produit de facteurs irréductibles dans $\mathbb{Z}[i]$ et déduire l'ensemble des couples $(x, y) \in \mathbb{Z}$ vérifiant $x^2 + y^2 = 221 = 13.17$.

Exercice 2

1. Résoudre l'équation de Pell-Fermat :

$$x^2 - 3y^2 = 1; x \in \mathbb{Z}, y \in \mathbb{Z} \tag{2}$$

2. Résoudre l'équation

$$x^2 - 3y^2 = -1; x \in \mathbb{Z}, y \in \mathbb{Z}. \tag{3}$$

3. Le but de cette question est de trouver les entiers n tel que le nombre $t = \sqrt{1 + 12n^2}$ soit un entier.
   (a) Montrer si $t = \sqrt{1 + 12n^2}$ est un entier alors t est impair. Montrer que alors on est amené à trouver des entiers m et n tel que

$$3n^2 = m(m + 1).$$

   (b) Montrer que si p est un nombre premier qui divise n alors p^2 divise m ou bien p^2 divise $(m + 1)$.
   En déduire qu'il existe des entiers a, b tels que :
   $(m = 3b^2$ et $m + 1 = a^2)$ ou $(m = b^2$ et $m + 1 = 3a^2)$.
   (c) Montrer alors qu'on est amené à résoudre les équations (2) et (3).
   (d) Trouver les entiers n tels que $t = \sqrt{1 + 12n^2}$ soit un entier.
   (e) Expliciter deux valeurs de $t > 1$.

BARÈME INDICATIF :
Exercice 1 : 10 points (1+2+3+1+1+2)
Exercice 2 : 10 points (2+2+1+1+1+2+1).