2010–2011

UNIVERSITÉ DE RENNES 1

Théorie des nombres

Interrogation 1 (6 octobre 2010)

Documents et calculatrice sont autorisés. Les téléphones portables sont interdits.

Durée : 45mn

Sauf mention explicite du contraire, toutes les réponses doivent être accompagnées d'une démontration.

Exercice 1

Le but de cet exercice est de retrouver le théorème des deux carrés en utilisant les propriétés de l'anneau des entiers de Gauss.

1. Quel est l'anneau des entiers de $\mathbb{Q}(i)$? Est-il euclidien ? principal ? factoriel ? (Il n'est pas demandé de fournir une preuve détaillée).
2. Dans la suite, p désignera un nombre premier impair. Montrer que si $p \equiv 3 \pmod 4$ alors p n'est pas somme de deux carrés (d'entiers naturels).
3. Montrer que p est somme de deux carrés si et seulement s'il est la norme d'un élément $a + ib$ de $\mathbb{Z}[i]$.
4. Montrer que dans ce cas $(a + ib)|p$ dans $\mathbb{Z}[i]$, et que $a + ib$ est irréductible dans $\mathbb{Z}[i]$.
5. En déduire que p est somme de deux carrés si et seulement s'il est réductible dans $\mathbb{Z}[i]$.
6. Si p est irréductible dans $\mathbb{Z}[i]$, montrer que l'idéal (p) est premier. Que peut-on en déduire au sujet de l'anneau quotient $\mathbb{Z}[i]/(p)$?
7. Montrer que $\mathbb{Z}[i]/(p) \simeq \mathbb{F}_p[X]/(X^2 + 1)$.
8. Montrer que $\mathbb{F}_p[X]/(X^2 + 1)$ est intègre si et seulement si -1 n'est pas un carré dans $\mathbb{F}_p$.
9. *(Question bonus)* Montrer que -1 est un carré dans $\mathbb{F}_p$ si seulement si $p \equiv 1 \pmod 4$. Conclure.