UNIVERSITÉ DE RENNES 1

Théorie des nombres

Examen — 1re session

Durée : 2h
Les notes de cours et de TD sont autorisées.

Exercice 1

1. Est-ce que 62 est un carré modulo 101 ?
2. Est-ce que 65 est un carré modulo 101 ?
3. Est-ce que 31 est un carré modulo 91 ?

Exercice 2

Trouver les solutions $(x, y) \in \mathbb{Z}^2$ de l'équation diophantienne $x^2 - 89y^2 = -1$.

Exercice 3

On cherche à résoudre l'équation diophantienne $x^2 + 3 = 2^n$, d'inconnues $x \in \mathbb{Z}$ et $n \in \mathbb{N}$. On rappelle que l'anneau des entiers de $\mathbb{Q}(\sqrt{-3})$ est euclidien. Soit (x, n) une solution de l'équation.

1. Montrer que x est impair. Montrer que x^2+3 est divisible par 4. On suppose désormais x positif.
2. Supposons n pair. En factorisant $2^n - x^2$, montrer que $2^{\frac{n}{2}+1} = 4$, $x = 1$ et $n = 2$.
3. On suppose désormais n impair. Vérifier que l'on doit avoir $n > 3$.
4. Montrer que 2 est irréductible dans l'anneau des entiers de $\mathbb{Q}(\sqrt{-3})$.
5. Factoriser $\frac{x^2+3}{4}$ dans l'anneau des entiers de $\mathbb{Q}(\sqrt{-3})$. Conclure.

Exercice 4

Soit $K = \mathbb{Q}(\sqrt{-m})$ un corps quadratique imaginaire, avec $m > 0$ un entier sans facteur carré. Soit $\mathcal{O}_K$ l'anneau des entiers de K, et I un idéal non nul de $\mathcal{O}_K$.

1. Soit $\sigma\colon K \to \mathbb{C}$ un plongement de K dans $\mathbb{C}$. Montrer que $\sigma(I)$ est un réseau de $\mathbb{C}$.
2. Montrer que $\mathcal{O}_K/I$ est fini.
3. On pose $N(I) \overset{\text{déf}}{=} \operatorname{Card}(\mathcal{O}_K/I)$. Si l'idéal I est principal, engendré par $x \in \mathcal{O}_K$, montrer que $N(I) = N_{K/\mathbb{Q}}(x)$.

4. Montrer que si J est un idéal de $\mathcal{O}_K$ qui contient I, alors $N(I) = N(J)\,\mathrm{Card}(J/I)$.
5. Montrer que le volume du réseau $\sigma(I)$ est $\begin{cases} \frac{1}{2}\sqrt{m}\,N(I) & \text{si } -m \equiv 1 \pmod 4 \\ \sqrt{m}\,N(I) & \text{sinon.} \end{cases}$
6. Montrer qu'il existe un $x \in I \setminus \{0\}$ tel que

$$N_{K/\mathbb{Q}}(x) \leqslant \begin{cases} \frac{2}{\pi} m\,N(I) & \text{si } -m \equiv 1 \pmod 4 \\ \frac{4}{\pi} m\,N(I) & \text{sinon.} \end{cases}$$

7. En déduire que si $m = 1$ ou $m = 3$ alors $\mathcal{O}_K$ est principal, sans passer par le fait qu'il est euclidien.