Université Paul Sabatier
Licence L3 ESR 2017–2018
Arithmétique

TD 6 : Géométrie des nombres

Exercice 1. Construire dans le plan :

1) un convexe d'aire infinie mais ne contenant aucun point de $\mathbb{Z}^2$;
2) une partie symétrique par rapport à l'origine et d'aire infinie mais ne contenant aucun point de $\mathbb{Z}^2$.

Exercice 2. On rappelle les deux points du théorème de Minkowski :

Soit $C \subset \mathbb{R}^n$ un convexe symétrique par rapport à 0.

1) Si $\mathrm{vol}(C) > 2^n$, alors C contient au moins un élément non nul de $\mathbb{Z}^n$.
2) Si $\mathrm{vol}(C) = 2^n$ et si C est compact, on a la même conclusion.

— Montrer que $1 \Rightarrow 2$.
— (Facultatif) Montrer que $2 \Rightarrow 1$.

Exercice 3. Soit un entier $r \geq 1$.

1) Démontrer le « principe des tiroirs pour les mesures » :
   Soient $(X, \mathcal{A}, \mu)$ un espace mesuré et (X_j) une suite de parties mesurables de X.
   Si $\sum_j \mu(X_j) > r\,\mu(\cup_j X_j)$, alors il existe un point de X appartenant à au moins $r+1$ de ces parties.
2) En déduire le théorème de Blichfeldt :
   Soit R une partie Lebesgue-mesurable de $\mathbb{R}^n$.
   — Si $\mathrm{vol}(R) > r$, alors R contient $r+1$ points distincts dont les différences sont à coordonnées entières.
   — (Facultatif) Si $\mathrm{vol}(R) = r$ et si R est compact, on a la même conclusion.

Exercice 4. Soit un nombre premier

$$p \equiv 1 \bmod 4.$$

Il existe donc un entier a tel que $-1 \equiv a^2 \bmod p$.

En considérant le réseau $\Gamma := \{(ps + at, t) \mid s, t \in \mathbb{Z}\} \subset \mathbb{R}^2$ et le disque ouvert C de centre 0 et de rayon $\sqrt{2p}$, redémontrer [1] le théorème des deux carrés « de Fermat » [2] :

$$p \text{ est somme de deux carrés.}$$

Exercice 5.

1) Soit un nombre premier $p > 2$. Il existe donc [3] des entiers r, s tels que $r^2 + s^2 \equiv -1 \bmod p$.

   En considérant le réseau $\Gamma := A\left(\mathbb{Z}^4\right)$ pour $A = \begin{pmatrix} p & 0 & r & s \\ 0 & p & s & -r \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$ et la boule ouverte $C \subset \mathbb{R}^4$ de centre 0 et de rayon [4] $R = \sqrt{2p}$, démontrer que

$$p \text{ est somme de quatre carrés.}$$

2) En utilisant l'identité des quatre carrés d'Euler [5], selon laquelle le produit de deux sommes de quatre carrés est une somme de quatre carrés, en déduire le théorème des quatre carrés de Lagrange :

$$\text{tout entier positif est somme de quatre carrés.}$$

Exercice 6. (Facultatif) Soient $x, y \in \mathbb{R}$ et $n \in \mathbb{N}^*$. Montrer qu'il existe :

1) $a, b, c \in \mathbb{Z}$ tels que $0 < c \leq n$ et $(x - a/c)^2 + (y - b/c)^2 \leq \frac{4}{\pi n c^2}$;
2) $a, b, c \in \mathbb{Z}$ tels que $|a|, |b| \leq n$, $(a, b) \neq (0, 0)$ et $|ax + by + c| < 1/n^2$.

Exercice 7. (Facultatif) Soient $m > 1$ et a deux entiers. Montrer que pour tout réel $X \in \,]1, m[$, il existe deux entiers x et y tels que $ax \equiv y \pmod{m}$, $1 \leq x < X$ et $|y| \leq m/X$.

---

1. Cf. TD 5, exercice 5.
2. Énoncé par Albert Girard dès 1625, puis par Fermat, et démontré en 1749 par Euler.
3. Cf. TD 4, exercice 1.
4. On rappelle que le volume de la boule unité en dimension n est égal à $\frac{\pi^{n/2}}{\Gamma(\frac{n}{2}+1)}$ et que $\Gamma(n+1) = n!$.
5. Analogue pour 4 carrés de celle de Diophante pour 2 carrés, vue dans le TD 5, exercice 6.