RÉSEAUX EUCLIDIENS EN CRYPTOGRAPHIE
2023 – TD 2

ALEXANDRE WALLET, QUYEN NGUYEN

Exercice 1. (Réseaux et non-réseaux)

(1) L'ensemble $\mathbb{Z} + \sqrt{2}\mathbb{Z}$ est-il un réseau de $\mathbb{R}$?

(2) Soit V la droite de $\mathbb{R}^2$ engendrée par $(1, \sqrt{2})$. Quel est le rang de $\mathbb{Z}^2 \cap V$? Si π désigne la projection orthogonale sur V, l'ensemble $\pi(\mathbb{Z}^2)$ est-il un réseau de $\mathbb{R}^2$?

(3) Montrer que les sous-groupes de $\mathbb{R}$ sont soit denses, soit des $\alpha\mathbb{Z}$ pour $\alpha \in \mathbb{R}$.

Exercice 2. On veut démontrer constructivement le résultat suivant :

Pour tout réseau $\mathcal{L}$ de rang 2, il existe une base (b_1, b_2) telle que b_1 est un plus court vecteur de $\mathcal{L}$ et $|\langle b_1, b_2\rangle| \leq \frac{1}{2}\|b_1\|^2$.

On considère l'algorithme suivant, attribué à Gauss et à Lagrange.

---

input : Une base (b_1, b_2) d'un réseau $\mathcal{L}$, avec $\|b_1\| \leq \|b_2\|$
output: Une base (b, b') satisfaisant les hypothèses de l'énoncé.
repeat
  $x \leftarrow \lfloor \frac{\langle b_1, b_2\rangle}{\|b_1\|^2} \rceil$
  $t \leftarrow b_2 - x b_1$
  $b_2 \leftarrow b_1, b_1 \leftarrow t$
until $\|b_1\| \geq \|b_2\|$;
return (b_2, b_1)

On commence par la correction de l'algorithme.

(1) Montrer qu'à chaque itération, l'algorithme ne manipule que des bases de $\mathcal{L}$.

(2) Notons (b_1', b_2') une base obtenue après une itération de la boucle. Montrer que pour tout $z \in \mathbb{Z}$ on a $\|b_1' + z b_2'\| \geq \|b_1'\|$. En déduire que si (b, b') est la sortie de l'algorithme, on a $|\langle b, b'\rangle| \leq \|b\|^2/2$.

(3) Montrer que $\|b\| = \lambda_1(\mathcal{L})$. *Optionnel :* montrer aussi que $\|b'\| = \lambda_2(\mathcal{L})$.

Il reste à montrer que l'algorithme se termine. L'idée est de montrer que la quantité $(\|b_1\|b_2\|)^2$ est diminué d'un facteur constant à chaque passage dans la boucle.

(4) Montrer que si $x = 0$ alors la boucle est terminée.

(5) Montrer que $|x| = 1$ n'est possible qu'à la première ou à la dernière itération de l'algorithme (Indice : penser à la question (2)).

On suppose maintenant que (b_1, b_2) donne $|x| \geq 2$. Soit $\widetilde{b_2}$ la projection de b_2 sur $(\mathbb{R}b_1)^\perp$.

(6) Montrer que $\|b_2\|^2 \geq \|\widetilde{b_2}\|^2 + \frac{9}{4}\|b_1\|^2$ et que $\|t\|^2 \leq \|\widetilde{b_2}\|^2 + \frac{1}{4}\|b_1\|^2$. En déduire que $\|b_2\|^2 \geq 3\|t\|^2$, si l'on n'est pas à la dernière itération.

(7) Supposons que $(b_1, b_2) \in \mathbb{Z}^m$ est la base en entrée de l'algorithme. Conclure que l'algorithme itère un nombre au plus polynomial de fois en la taille de ses entrées.