Topics: Lattice reduction and applications.

12.1. Find a Lagrange–Gauss reduced basis for the lattice L given by

$$\left\{\begin{bmatrix}-5\\-4\end{bmatrix}, \begin{bmatrix}2\\3\end{bmatrix}\right\}$$

and use it to solve SVP in L. If you have a calculator handy, keep track of the Hadamard ratio as you apply the algorithm.

12.2. Let $L \subset \mathbf{R}^2$ be the lattice with basis matrix

$$M = \begin{bmatrix} 2 & 1 \\ -1 & 1 \end{bmatrix}.$$

Let $L^\vee \subset \mathbf{R}^2$ be the lattice with basis matrix $M^\vee = (M^\mathsf{T})^{-1}$.

(a) Show that

$$L^\vee = \{y \in \mathbf{R}^2 : \ \langle x, y\rangle \in \mathbf{Z} \text{ for all } x \in L\}.$$

We call $L^\vee$ the *dual lattice to L*.

(b) Let B be the $\mathbf{Z}$-basis of L consisting of the columns of M, and $B^\vee$ the $\mathbf{Z}$-basis of $L^\vee$ consisting of the columns of $M^\vee$. Compare the Hadamard ratios $\mathcal{H}(B)$ and $\mathcal{H}(B^\vee)$.

12.3. Given $n \in \mathbf{Z}_{\geqslant 1}$, a real number x is said to be *algebraic of degree n* if there exist integers $a_0, \dots, a_n$ with $a_n \neq 0$ such that

$$a_0 + a_1 x + \cdots + a_n x^n = 0.$$

(a) Describe a lattice-based procedure for investigating whether a given real number is algebraic of degree n.

(b) You are given a real number α such that

$$\alpha \approx -1.764, \quad \alpha^2 \approx 3.112, \quad \alpha^3 \approx -5.489, \quad \alpha^4 \approx 9.683.$$

You form the matrix

$$M = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 1000 & -1764 & 3112 & -5489 & 9683 \end{bmatrix}$$

and find out that the LLL reduction of the lattice with basis matrix M has basis matrix

$$\begin{bmatrix} 1 & -4 & 5 & -2 & 2 \\ -1 & -3 & -4 & 6 & -2 \\ -4 & 0 & 1 & 0 & 3 \\ 0 & 2 & 1 & 3 & 8 \\ 1 & 1 & -1 & 3 & 3 \\ -1 & -3 & -4 & -2 & 1 \end{bmatrix}$$

What do you guess about the number α? How could you build more confidence in your guess?

12.4. Let (w_1, w_2) be an ordered $\mathbf{Z}$-basis of a lattice $L \subset \mathbf{R}^2$. Prove that (w_1, w_2) is Lagrange–Gauss reduced if and only if

$$\|w_1\| \leqslant \|w_2\| \qquad \text{and} \qquad |\langle w_1, w_2 \rangle| \leqslant \frac{1}{2}\|w_1\|^2.$$

12.5. Let (w_1, w_2) be a $\mathbf{Z}$-basis of a lattice $L \subset \mathbf{R}^2$.

(a) Prove that if (w_1, w_2) is Lagrange–Gauss reduced then it is LLL-reduced.

(b) Give an example to show that the converse is not true in general.

12.6. We explore the Closest Vector Problem (CVP) in full rank 2. Let $L \subset \mathbf{R}^2$ be a full lattice and let $\mathcal{F}$ be the fundamental domain with respect to a $\mathbf{Z}$-basis of L.

(a) Convince yourself that it suffices to know how to solve the CVP for $v \in \mathcal{F}$.

(b) Let $L = \mathbf{Z}^2 \subset \mathbf{R}^2$ be the square lattice with the standard basis $\{e_1, e_2\}$. For a vector $v \in \mathcal{F}$, show that the closest vector to v is the closest corner of the closure of $\mathcal{F}$.

(c) Give an example showing that the statement in (a) does not hold for all $\mathbf{Z}$-bases of $\mathbf{Z}^2$.