ALGORITHMS ON LATTICES

EXERCISE 1

IMPORTANT: Your solutions will only be evaluated once you have solved Problem 8.

Problem 1. [5 pts] Show that $\{(a+b\sqrt{2}, a-b\sqrt{2}) \in \mathbb{R}^2 \mid a, b \in \mathbb{Z}\}$ is a lattice.

Problem 2. [6 pts]

(a) Given an $m \times n$ integer matrix A show that

$$\mathrm{Ker}(A) = \{(x_1, \ldots, x_m) \in \mathbb{Z}^m \mid (x_1, \ldots, x_m)A = (0, \ldots, 0)\}$$

is a lattice of rank $m - \mathrm{rank}(A)$.

(b) Given an $m \times n$ integer matrix A and a positive integer n show that

$$\{(x_1, \ldots, x_m) \in \mathbb{Z}^m \mid (x_1, \ldots, x_m)A = (0, \ldots, 0) \pmod{n}\}$$

is a lattice of rank m.

Problem 3. [6 pts] Let $a, b \in \mathbb{N}$. Show that there exits a solution $x, y, z \in \mathbb{Z}$ to the equation $ax + by = z$ satisfying $x^2 + z^2 \leq b\sqrt{2}$.

Problem 4. [4 pts] Let b_1, b_2 be a basis of $L \subseteq \mathbb{R}^2$. Suppose that b_1', b_2' is the output basis when Gauss-reduction algorithm applied to b_1, b_2. We will call such a basis b_1', b_2' **shortest basis**.

(a) Show that $\| b_1' \| \leq \| b_2' \| \leq \| b_2' + kb_1' \|$ for all $k \in \mathbb{Z}$.

(b) Show that b_1', b_2' is shortest basis if and only if $\| b_1' \| \leq \| b_2' \| \leq \| b_2' \pm b_1' \|$.

Problem 5.[8 pts] Let b_1', b_2' be shortest basis of $L \subseteq \mathbb{R}^2$.

(a) Define $Q(x, y) = \| xb_1' + yb_2' \|^2$. Show that $Q(x, y) = ax^2 + 2bxy + cy^2$ with $a, c \geq 0$ and $a \leq c$.

(b) Prove that $Q(1, -1) \geq Q(0, 1)$.

(c) Show that $2b \leq a$. Hence show that $a \leq \sqrt{\frac{4}{3}(ac - b^2)}$.

(d) Show that $\det(L)^2 = | b^2 - ac |$.

Problem 6. [3 pts] Prove that the following three bases of $\mathbb{R}^2$ all generate the same two-dimensional lattice:

$$\text{basis 1: } b_1 = (0, 2)\ \ b_2 = (5, 1)$$
$$\text{basis 2: } b_1 = (85, -31)\ \ b_2 = (-60, 22)$$
$$\text{basis 3: } b_1 = (-230, 84)\ \ b_2 = (545, -199).$$

Problem 7. [3 pts] Apply the Gauss-reduction algorithm to the following pairs of vectors:

$$b_1 = (-1, -38, 86), b_2 = (0, -27, 61)$$
$$b_1 = (40, -82, -74, -5), b_2 = (29, -58, -45, -12).$$

Problem 8. [15 pts] Let A be a $m \times n$ integer matrix. Recall that if $B = \mathrm{HNF}(A)$ then there is a $m \times m$ unimodular matrix U such that $B = UA$.

Modify the given `HNFORMS` algorithm code so that it also produces the unimodular matrix U as part of the output.

(**Note:** If you don't like the provided `HNFORMS` code, then you can implement your own version by following the algorithm discussed in the exercise session.).