Exercise 1 Show that the invariant $\gamma(L)$ of a lattice L is scaling-invariant and rotation invariant. That is:

i) $\gamma(c \cdot L) = \gamma(L)$ for any $c \in \mathbb{R}^\times$.

ii) $\gamma(\mathbf{R} \cdot L) = \gamma(L)$ for any $\mathbf{R} \in \mathcal{O}_n(\mathbb{R})$, the group of orthonormal transformations.

Exercise 2 How does the Lagrange reduction algorithm behave if the input is not a basis, that is if $\mathbf{b}_1, \mathbf{b}_2$ are co-linear? Does it terminates, and if so, what is its output? Discuss the two cases:

i) If $\mathbf{b}_1 = \alpha \mathbf{b}_2$ for $\alpha \in \mathbb{Q}$

ii) If $\mathbf{b}_1 = \alpha \mathbf{b}_2$ for $\alpha \in \mathbb{R} \setminus \mathbb{Q}$.

(Hint: You should recognize an algorithm invented about 2 millennia before Lagrange!)

Exercise 3 In this exercise we consider applying Lagrange Reduction over the Gaussian integers, that is the ring $\mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}\}$ where $i \in \mathbb{C}$ is an imaginary unit: $i^2 + 1 = 0$. The Euclidean inner product is replace by the Hermitian inner product : $\langle x, y \rangle = \sum x_j \bar{y}_j$. The rounding of a complex number $a + bi \in \mathbb{C}$ is given as $\lfloor a + bi \rceil := \lfloor a \rceil + \lfloor b \rceil i \in \mathbb{Z}[i]$.

i) Prove that for all $c \in \mathbb{C}$, $|c - \lfloor c \rceil| \leq \sqrt{2}/2 < 1$.

ii) Given the basis $\mathbf{B} \in \mathbb{C}^{2\times 2}$ of a Gaussian lattice $G = \mathbf{B} \cdot \mathbb{Z}[i]^2$, prove that Lagrange algorithm terminates and that it output a shortest non-zero vector of G (you can ignore the issue of representing irrational complex numbers, and assume that each arithmetic operation over $\mathbb{C}$ takes time 1).

iii) (Hard). And what about the same over the Eisenstein integers: $\mathbb{Z}[j] = \{a + bj : a, b \in \mathbb{Z}\}$ where $j \in \mathbb{C}$ is a solution of $j^2 + j + 1 = 0$? How would you even define rounding from $\mathbb{C}$ to $\mathbb{Z}[j]$?