Lattices are usually represented by a basis, i.e., a set of linearly independent vectors \( b_1, \ldots, b_k \) that generate the lattice. In this assignment we consider alternative representations, and algorithms to convert between them.

1 Working with a triangular basis

In the problem 2 you will show (among other things) that every full rank integer lattice has a lower triangular basis. Triangular bases are very convenient to work with, as shown in this first problem.

Give a polynomial time algorithm that on input a full rank lower triangular basis \( B \in \mathbb{Z}^{n \times n} \) and a vector \( t \in \mathbb{Z}^n \), returns a lower triangular basis \( B' \) for the lattice generated by all integer linear combinations of \( B \) and \( t \).

(Hint: first give an algorithm that on input \((B, t)\), returns a new pair \((B', t')\) such that the first coordinate of \( t \) is zero. Use the determinant of the lattice to make sure all numbers involved do not get too big.)

2 Linear dependencies

Consider a set of (linearly dependent) integer vectors \( b_1, \ldots, b_k \in \mathbb{Z}^n \) (for \( k > n \)), and assume for simplicity that they span the entire space \( \mathbb{R}^n \). Show that the set of their integer linear combinations

\[
L(b_1, \ldots, b_k) = \{ \sum_i b_i x_i : \forall i. x_i \in \mathbb{Z} \}
\]

is a lattice, by giving a polynomial time algorithm that on input \( b_1, \ldots, b_k \), returns a basis for the lattice they generate. (Hint: Find a sublattice of the form \( d \cdot \mathbb{Z}^n \), and then add the \( b_i \) vectors to it, one at a time, using the result proved in problem 1.)

3 Systems of equations

Consider a system of \( k \) equations in \( n \) variables

\[
(i = 1, \ldots, k) \sum_{j=1}^{n} a_{i,j} x_j = 0 \pmod{m_i}
\]

where all \( a_{i,j} \) and \( m_i \) are integers. Show that the set of integer solutions to the system is a lattice, by giving a polynomial time algorithm that on input the coefficients \( a_{i,j} \) and moduli \( m_i \), returns a lattice basis. (Hint: consider the dual of the lattice generated by the (linearly dependent) vectors \( \frac{1}{m_i}(a_{i,1}, \ldots, a_{i,n})^T \) and \((0, \ldots, 0, 1, 0, \ldots, 0)^T\).)