Exercise 3.1 (The basis reduction algorithm). (32+3 points)

In this exercise we will do several experiments with the lattice basis reduction algorithm. For that (and also for later programming tasks) we need a running implementation.

(i) Implement the basis reduction algorithm in a programming language of your choice. Hand in the source code. Hint: Try to work bottom up. Implement the vector arithmetic first, afterwards scalar products and the \( \mu_{i,j} \). Build from that the GSO, which in turn is used by the size-reduction and the exchange-step. Once you have all this, start writing the basis reduction algorithm. It is helpful to employ a computer algebra system for that task!

If you did not succeed in making the algorithm run, use your brain or a built in function of a computer algebra system like Maple or MuPAD. Let’s now try our nice example from the last sheet:

(ii) Test the algorithm! Compute \( a, b \in \mathbb{Z} \) with \( a^2 + b^2 = 1034353 \) using your basis reduction algorithm.

(iii) For which parameters \( \delta \) do you obtain a solution? Note that in the Maple and MuPAD implementations the parameter \( \delta \) is fixed and cannot be changed.

Let us now consider the lattice \( L = \mathcal{L}(B) \) spanned by the basis \( B = \begin{bmatrix} 2 & 1 & 5 & 8 \\ 7 & 2 & 5 & 5 \\ 2 & 3 & 1 & 1 \\ 5 & 8 & 9 & 9 \end{bmatrix} \).

(iv) Minkowski’s theorem states that for any lattice we have \( \lambda(L) \leq \sqrt{n} \det(L)^{1/n} \). What is the value of this bound in our example?

(v) What is the length of the shortest vector in the output of the basis reduction algorithm?

(vi) What is the value of the integer \( D = \prod_{i=1}^{4} \det(\mathcal{L}(b_1, \ldots, b_i))^2 \) for the input basis?

(vii) What is the number of iterations predicted by the running time analysis from the lecture?

(viii) What is the value of \( D \) upon finding a reduced basis?

(ix) Give an upper bound on the number of iterations based on the initial and final value of \( D \).

(x) What is the number of iterations actually executed?