Experimental Mathematics Lab Projects

Lattice Reduction

Lattice reduction is a powerful tool to find short vectors in lattices. Mostly known in this area is the so-called LLL algorithm of Lenstra, Lenstra and Lovasz. Roughly speaking, given a basis of a lattice, the LLL algorithm outputs a 'reduced' basis for the same lattice, with the difference that this 'reduced' basis has plenty of advantages and many applications in number theory and in cryptography.

A first goal of this project would be to understand 'reduced' bases from an algorithmic point of view, and test various examples. In a second time, one could use the LLL algorithm as a black-box (there are many good implementations of the algorithm in various languages) to study some of its applications such as

- approximating numbers by fractions with 'small' numerator and denominator. More precisely, given integers $x, N \geq 2$, finding 'small' integers a, b such that $x \equiv a/b \pmod{N}$ can be efficiently solved using lattice reduction of a lattice of rank 2. A related application is simultaneous Diophantine approximation.
- finding small integer roots of univariate polynomials modulo a given integer, that is, given a monic integer polynomial $F(t) = t^n + a_{n-1}t^{n-1} + \ldots + a_1 t + a_0$ and an integer root x_0 modulo some integer N, i.e. such that $F(x_0) \equiv 0 \pmod{N}$ and $|x_0| \leq N^{1/n}$ (i.e. x_0 is a 'small' root). Via lattice reduction (LLL) one can find such a root by finding a polynomial that has the same zeroes as the target polynomial but has smaller coefficients. This is known as Coppersmith's technique, after Don Coppersmith.
- many other applications

References.

- https://en.wikipedia.org/wiki/Lenstra?Lenstra?Lovasz_lattice_basis_reduction_algorithm