Références

- [Dieter, 1975] How to Calculate Shortest Vectors in a Lattice

- [vEB, 1981] ? Another NP-Complete problem and the complexity of computing the shortest vectors in a lattice

- [Lenstra, 1982] Factoring polynomials with rational coefficients

- [Ajtai, 1998] The shortest vector problem in L2 is NP-hard for randomized reductions

- [Regev, 2005] On lattices, learning with errors, random linear codes, and cryptography