

# Références

- SVP: [https://en.wikipedia.org/wiki/Lattice\\_problem](https://en.wikipedia.org/wiki/Lattice_problem)
- Dual Lattice: [https://en.wikipedia.org/wiki/Dual\\_lattice](https://en.wikipedia.org/wiki/Dual_lattice)
- How to calculate the shortest vectors in a lattice: <https://www.ams.org/journals/mcom/1975-29-131/S0025-5718-1975-0379386-6/S0025-5718-1975-0379386-6.pdf>
- LLL: [https://en.wikipedia.org/wiki/Lenstra–Lenstra–Lovász\\_lattice\\_basis\\_reduction\\_algorithm](https://en.wikipedia.org/wiki/Lenstra–Lenstra–Lovász_lattice_basis_reduction_algorithm)
- GSO: [https://en.wikipedia.org/wiki/Gram–Schmidt\\_process](https://en.wikipedia.org/wiki/Gram–Schmidt_process)
- Lattices in CS: [https://cims.nyu.edu/~regev/teaching/lattices\\_fall\\_2004/ln/introduction.pdf](https://cims.nyu.edu/~regev/teaching/lattices_fall_2004/ln/introduction.pdf)
- Generating hard SVP instances: <https://people.csail.mit.edu/vinodv/CS294/ajtai99.pdf>

