Code & Resources

- Mon projet (🦀): https://github.com/filedesless/classes/tree/main/INF889B/svp
  - SVP exact par énumération + coupures
  - Orthogonalization de base Gram-Schmidt & réduction de base LLL
- nalgebra (🦀): https://nalgebra.org/
  - Librairie d'algèbre linéaire
- SAGEMATH (🐍): https://www.sagemath.org/
  - Framework de math
  - Prototype, visualisation, génération de donnée de test et benchmark
- fplll (c++): https://github.com/fplll/fplll
  - Algorithmes sur les réseaux (dont LLL) utilisé par sage

Références

- SVP: https://en.wikipedia.org/wiki/Lattice_problem
- 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
- GSO: https://en.wikipedia.org/wiki/Gram–Schmidt_process
- Lattices in CS: 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