1046-68-1571 **Gilles Villard*** (Gilles.Villard@ens-lyon.fr), Laboratoire LIP, 46 Allee d'Italie, F69364 Lyon Cedex07, France. *Numerical analysis tools for LLL lattice basis reduction.* Preliminary report.

LLL-reduction of lattice bases is an important algorithm [Lenstra, Lenstra, Lovàsz 1982] in computer science and mathematics making worthwile efficiency improvements.

A key ingredient of currently fastest reduction algorithms is using floating point approximations of rational numbers involved in the underlying Gram-Schmidt orthogonalisation (for integer bases). We especially refer to Schnorr's algorithms, and to the L2 Algorithm of Nguyen and Stehlé.

Revisiting and improving classical tools from the field of numerical analysis, such as QR perturbation analyses, we strengthen Schnorr's and the L2 approach, design a LLL-reduceness certificate, and propose a new algorithm for improving the quality of LLL-reduced bases. We describe these developments, and show in particular how floating point computations may be introduced at various levels in the overall reduction process.

This research is done in collaboration with I. Morel (U. Lyon, U. Sydney), and D. Stehlé (CNRS, Macquarie U., U. Sydney). (Received September 16, 2008)