Séminaire d'Algèbre, Topologie et Géométrie
Jeudi 2 février à 14h00
Salle I

Bas Edixhoven

(Leiden University)

Title : *Fast computation of the number of vectors of given length in a lattice.*

Abstract : The question is how one can compute the number of ways in which an integer m can be written as a sum of n squares of integers, fast. I will explain how recent progress in computation of 2-dimensional Galois representations make it possible to compute this number, for n even and m given with its factorisation in prime numbers, in time at most a power of n.log(m) (assuming the Riemann hypothesis for number fields). This is an application of a generalisation by Peter Bruin of joint work of the speaker with Jean-Marc Couveignes, Robin de Jong and Franz Merkl.

For details, see :
http ://www.math.univ-toulouse.fr/ couveig/book.htm
http ://www.math.u-psud.fr/ bruin/
http ://www.math.leidenuniv.nl/nl/theses/196/