

# Student Workshop Presentation in Pure Mathematics

## *Lattice Basis Reduction and its Applications*

Murray R. Bremner, University of Saskatchewan

Abstract: A *lattice* of dimension  $n$  is the set of all *integer* linear combinations of a basis of  $\mathbb{R}^n$ . For  $n \geq 2$ , every  $n$ -dimensional lattice has many different bases; the problem of lattice basis reduction is to find a basis consisting of relatively short vectors. The LLL algorithm for lattice basis reduction was published in 1982 in a famous paper by Lenstra, Lenstra and Lovász which presented the first polynomial-time algorithm for factoring polynomials with rational coefficients. In part one of this talk, I will review the basic theory of lattices, explain the LLL algorithm, and give computer examples. In part two, I will describe the applications of LLL to cryptography, number theory, and algebra.