Title: Number-theoretic methods in quantum computing

Abstract: An important problem in quantum computation is the so-called

approximate synthesis problem: to find a circuit, preferably as short

as possible, that approximates a given unitary operator up to given

epsilon. For nearly two decades, the standard solution to this problem

was the Solovay-Kitaev algorithm, which is based on geometric

ideas. This algorithm produces circuits of size O(log^c(1/epsilon)),

where c is approximately 3.97. It was a long-standing open problem

whether this exponent c could be reduced to 1.

In this talk, I will report on a new class of number-theoretic

algorithms that achieve circuit size O(log(1/epsilon)), thereby

answering the above question positively. In certain important cases,

such as the commonly used Clifford+T gate set, one can even find

algorithms that are optimal in an absolute sense: the algorithm finds

the shortest circuit whatsoever for the given problem instance. This

is joint work with Neil J. Ross.