Quantum algorithms for number theoretic problems

Sean Hallgren, Penn State

Exponential speedups by quantum algorithms have been found mostly for number theoretic problems, such as computing the unit group and class group in constant degree number fields. I will discuss what is known about the main problems in number fields and function fields. I will also discuss where limitations of the quantum techniques appear in a natural generalization of the approach to graph isomorphism.