Primality testing, then and now

Carl Pomerance, Dartmouth College

The task is simply stated. Given a large integer, decide if it is prime or composite. Gauss wrote of this algorithmic problem (and the twin task of factoring composites) in 1801: ``the dignity of science itself seems to require that every possible possible means be explored for the solution of a problem so elegant and so celebrated."" Though progress with factoring composites has been steady and substantial, I think Gauss would be especially pleased with the enormous progress with primality testing, both in practice and in theory. In fact, one of the latest developments strangely and aptly employs a construct Gauss used to deal with ruler and compass constructions of regular polygons! This talk will present a survey of some of the principal ideas used in the prime recognition problem starting with the 19th century work of Lucas, to the 21st century work of Agrawal, Kayal, and Saxena, and beyond.