COLLOQUIUM

Richard McIntosh
University of Regina

On the Fermat, Lucas and Baillie-PSW Probabilistic Primality Tests

Mathematics and Statistics

Friday, January 27, 2017, 3:30 - 4:30 PM, RI 209

"The problem of distinguishing prime numbers from composite numbers and of resolving the latter into their prime factors is known to be one of the most important and useful in arithmetic."

C. F. GAUSS

Abstract: In number theory, a *probable prime* is an integer that satisfies a specific condition that is satisfied by prime numbers, but which is not satisfied by most composite numbers. Composite probable primes are called *pseudoprimes*. The Fermat probable prime test is based on Fermat's Little Theorem. Compared to the primes the Fermat pseudoprimes are very rare. Because the number of multiplications and modular reductions in this test is proportional to $\log n$, where n is the number being tested, this test and its variations can be applied to numbers with millions of digits. The Lucas probable prime test is based on Lucas (or generalized Fibonacci) sequences and the Baillie-PSW probable prime test, named after Baillie, Pomerance, Selfridge, and Wagstaff, is a combination of a strong Fermat probable prime test and a strong Lucas probable prime test. It is estimated that there is no composite number with less than about 10,000 digits that can fool this test. Many computer algebra systems and software packages, including MAPLE, Mathematica, PARI/GP, SageMath and Maxima, use some version of the Baillie-PSW primality test. In this talk a brief description of these tests and the underlying theory will be given.

University of Regina