Pacific Institute for the Mathematical Sciences

PIMS Distinguished Speakers Series

MICHAEL J. JACOBSON, Jr.

Professor and Associate Head, Department of Computer Science
Board Member at ISPIA (Institute for Security, Privacy and Information Assurance)
University of Calgary

Title: Computations in Quadratic Fields

Talk is accessible to undergrads. No prior knowledge of quadratic fields assumed.

Abstract:
Quadratic fields have been studied since the time of Gauss, and in modern times have been used in applications such as integer factorization and public-key cryptography. In this talk, we will give a brief overview of some applications and computational problems in this area. Our main focus will be on computing tables of the ideal class group of quadratic fields, which are used to provide valuable numerical evidence in support of a number of unproven heuristics and conjectures. We will discuss recent efforts to extend existing, unconditionally correct tables of both imaginary and real quadratic fields.

Bio:
PhD in Computer Science, Technische Universität Darmstadt, Germany (1999)
M.Sc. in Computer Science, University of Manitoba (1995)

Areas of research: cryptography (data security) and computational number theory.

Friday—October 26, 2018
12:00 to 12:50 pm
D-634
** S N A C K S **