Lethbridge Number Theory and Combinatorics Seminar

Monday — October 2, 2017
Room: C630
Time: 12:00 to 12:50 p.m.

Andrew Fiori

The average number of quadratic Frobenius pseudoprimes

Abstract: Primality testing has a number of important applications. In particular in cryptographic applications the complexity of existing deterministic algorithms causes increasing latency as the size of numbers we must test grow and the number of tests we must run before finding a prime grows aswell. These observations lead one to consider potentially non-deterministic algorithms which are faster, and consequently leads one to consider the false positives these algorithms yield, which we call pseudoprimes.

In this talk I will discuss my recent work with Andrew Shallue where we study Quadratic Frobenius Pseudoprimes. I shall describe our results on an asymptotic lower bounds on the number of false positives. These results represent a generalization of those Erdos-Pomerance concerning similar problems for (Fermat) pseudoprimes.

EVERYONE IS WELCOME!

Visit the seminar web page at
http://www.cs.uleth.ca/∼nathanng/ntcoseminar/

Pacific Institute *for the* Mathematical Sciences