Lethbridge Number Theory and Combinatorics Seminar

Monday — September 16, 2013
Room: E575
Time: 12:00 to 12:50 p.m.

Farzad Aryan
(University of Lethbridge)

On distribution of squares modulo a composite number q

Abstract: A natural number s is said to be a square modulo a composite number q if it is a square modulo each of the prime numbers dividing q. Let p be a prime number, then

$$\mathbf{Prob}(s \text{ is a square mod } p) = \frac{p+1}{2p} \approx \frac{1}{2}.$$

Roughly speaking, the probability of a number to be a square modulo q is $1/2^{\omega(q)}$, where $\omega(q)$ is the number of prime divisors of q.

Fix h and let $\mathcal{X} : \{1, 2, \cdots, q\} \to \mathbb{N}$ be a random variable, given by

$$\mathcal{X}(i) = \#\{s \in [i, i+h] : s \text{ is a square modulo } q\}.$$

For the mean, we have $\mathbf{E}(\mathcal{X}) \approx h/2^{\omega(q)}$, and, in this talk, we show the following bound for the variance:

$$\mathbf{Var}(\mathcal{X}) \leq \mathbf{E}(\mathcal{X}) \approx \frac{h}{2^{\omega(q)}}.$$

EVERYONE IS WELCOME!

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

Pacific Institute *for the* Mathematical Sciences