STUDENT SEMINAR

SOURABHASHIS DAS

MATHEMATICS & COMPUTER SCIENCE
UNIVERSITY OF LETHBRIDGE

Title: Group Structure on Elliptic Curves

Abstract:

Elliptic Curve Cryptography (ECC) is a modern approach used for public key encryption by utilizing the mathematics behind elliptic curves. ECC is used for encrypting important information by various agencies including the National Security Agency (NSA) and the cryptocurrency Bitcoin. ECC can be used on most of today's operating systems and browser including Apple OS X, Google Android, Microsoft Windows, Apple Safari and Google Chrome. Elliptic curves are especially important in number theory and have been used to solve various Diophantine equations, for example, they were used in the proof of Fermat's Last Theorem by Andrew Wiles. In this talk, we will focus on understanding the group structure defined by all the points with real coordinates on an elliptic curve in a geometrical way, i.e, by using the points of intersection of lines and curves. The basic concepts required to understand this topic, such as group and elliptic curve, will be discussed in brief. The only prerequisite for this talk is your interest in learning something new and exciting while eating a donut.

This talk will be accessible to all undergrads.

WHEN
FRIDAY, JAN 17
12:00—12:50

WHERE
D634

WHO
ANYONE WHO'S INTERESTED

REFRESHMENTS
DONUTS

Pacific Institute for the Mathematical Sciences

MATHEMATICS AND COMPUTER SCIENCE

http://www.uleth.ca/artsci/math-computer-science