

Applications of Exponential Sums: An Overview

Dr. Luo Jinquan

Research Fellow,

Division of Mathematical Sciences,
School of Physical and Mathematical Sciences,
Nanyang Technological University,
Singapore



Date : 13 March 2009 (Friday)

Time : 4.30 pm – 5.30 pm

Venue: SPMS-Executive Classroom 1, MAS-03-06
School of Physical and Mathematical Sciences

Exponential sums over finite fields are fundamental and important objects in number theory and arithmetic geometry for studying the number of solutions to the equations over finite fields. For several decades, a series of profound results on the estimation of the absolute values to the exponential sums have been found by the methods in number theory and arithmetic geometry. In practice, exponential sums have important applications in coding and cryptography. For example, in CDMA communication system we need to find sequences which have low auto and cross correlation values. It is equivalent to find a series of exponential sums which have small absolute values. In coding theory, exponential sums are used for estimating the minimum distances of linear codes. Moreover, the weight distribution of the cyclic codes can be obtained if the associated exponential sums are evaluated explicitly. In this talk, we will provide some examples to show how the exponential sums are employed in studying the properties of cyclic codes, constant composition codes, sequences, authentication codes and curves.

Host: Coding and Cryptography Research Group, Division of Mathematical Sciences,
School of Physical and Mathematical Sciences

SCHOOL OF PHYSICAL AND MATHEMATICAL SCIENCES

NANYANG TECHNOLOGICAL UNIVERSITY

SPMS-MAS-03-01, 21 NANYANG LINK, SINGAPORE 637371

FAX: +65 6515 8213 TEL: +65 6513 7423