



2008 - 2009



**MATHEMATICS COLLOQUIUM SERIES**  
**UNIVERSITY OF CENTRAL FLORIDA**

---

**Professor Xiang-dong Hou**  
**Department of Mathematics**  
**University of South Florida**

Will speak on

**"Reversed Dickson Polynomials Over Finite Fields"**

**Abstract:**

Let  $n \geq 0$  be an integer. Waring's formula gives an explicit polynomial  $D_n(x, y)$  with integer coefficients such that  $x_1^n + x_2^n = D_n(x_1 + x_2, x_1 x_2)$ . Fix an element  $a$  in a finite field  $F_q$ . The polynomial  $D_n(x, a)$  is called a Dickson polynomial. Dickson polynomials have been well studied. In particular, it is known which Dickson polynomials are permutations of  $F_q$ .

Reversed Dickson polynomials (RDP) are  $D_n(a, x)$ , obtained from Dickson polynomials  $D_n(x, a)$  by reversing the roles of the indeterminate  $x$  and the parameter  $a$ . Little was known about RDPs previously. The primary question that we are interested in is which RDPs are permutations of  $F_q$ . We find several families of permutational RDPs and have a conjecture about the answer to the above question when  $q$  is a prime. We also discover a connection between permutational RDPs and almost perfect nonlinear (APN) functions. The latter have important applications in cryptography.

This is a joint work with Mullen (Penn State), Sellers (Penn State) and Yucas (S. Illinois).

Date: Thursday, April 2, 2009

Time: 11:30 AM

Place: MAP 318

Everyone is cordially requested to attend.