

# INMAA Fall Meeting

Manchester College

October 27, 2007

## Abstracts

### **An elementary history of Fermat's Last Theorem**

**John Swallow**

Davidson College

Fermat's Last "Theorem" occupies a singular place in the history of mathematics, having informed and inspired mathematicians over three centuries. Surprisingly diverse branches of mathematics have sprung from the search for a proof of its simple conjecture: For  $n > 2$ ,  $x^n + y^n = z^n$  has no solutions in positive integers.

This talk chronicles the history of the theorem, stopping short of Wiles' proof and placing emphasis on the significant ideas and methods of proof which the problem engendered. The talk should be accessible to everyone who is familiar with the unique factorization of integers into primes and who would enjoy charting the history of arithmetic amidst innovations in algebra, geometry, and computers.

### **Circular irrationalities: From Galois to Kummer and back again**

**John Swallow**

Davidson College

The truth value of the statement "Harry and Isabel are siblings, and Joe and Karl are siblings" is very probably not invariant under every permutation of the names. Surprisingly, the study of roots such as  $2^{(1/2)}$  and  $3^{(1/5)}$  proceeds similarly: in place of sentences, consider equations relating the roots and ask which of them hold true under certain permutations of the roots. We introduce this study of  $n$ th roots and then tell the story of how some basic questions, solved with real contributions by undergraduates, pointed the way to some significant new results in field theory. This work is joint with Davidson undergraduates Frank Chemotti '05 and Andy Schultz '02, as well as D. Benson, N. Lemire, and J. Mináč.

### **The dynamical motion of the zeros of the partial sums of $e^z$**

**Amos Carpenter**

Butler University

In a paper in 1924 Szegő claimed that, for all  $n$  sufficiently large, the discrepancy function for the zeros of the partial sums of  $e^z$  is bounded, but no estimates for the bound were given. In contrast, we show that this boundedness fails to be true. An Interactive Supplement, which directly shows the dynamical motion of the zeros of the partial sums of  $e^z$ , will be presented.

### **Parabolas in Space**

## **Adam Coffman**

IPFW

I will present parametric equations for parabolic curves in three-dimensional space and then generalize to surfaces in space containing many parabolas, using computer graphics to illustrate a classification theorem of Peters and Reif for quadratically parametrized surfaces.

## **More Functions on the Mosaic of $n$**

### **Jared Erickson**

Valparaiso University

The mosaic of the integer  $n$  is the array of prime numbers resulting from iterating the Fundamental Theorem of Arithmetic on  $n$  and on any resulting composite exponents. In this presentation we generalize the functions  $\Omega(n)$  and  $\lambda(n)$  to the mosaic of  $n$ . We also introduce a new function,  $\psi_{\{j,i\}}(n)$ , a partial summation of the primes in the mosaic. We examine properties of these functions.

## **Modeling actuator Hysteresis with a directed graph.**

### **W. Steve Galinaitis**

Rose-Hulman Institute of Technology

A directed graph is used to model rate independent hysteresis for an actuator with a bounded input  $u(t)$  that attains only  $n$  distinct levels  $u_{min} = u_1 < u_2, \dots, u_{n-1} < u_n = u_{max}$  between a minimum input  $u_{min}$  and maximum input  $u_{max}$ . It is proven that this discrete model fulfills the basic properties of rate independent hysteresis model. It is then shown that a control input  $u^*$  exists that minimizes the positioning error induced by hysteresis, and a method for determination of this minimizing control is provided. The veracity of this approach is demonstrated through simulation, and experimentally by controlling a piezoelectric stack actuator in real time.

## **The Pohlig-Hellman exponentiation cipher as a bridge between classical and modern cryptography**

### **Joshua Holden**

Rose-Hulman Institute of Technology

The Pohlig-Hellman exponentiation cipher is a symmetric-key cipher that uses some of the same mathematical operations as the better-known RSA and Diffie-Hellman public-key cryptosystems. First published in 1978, the Pohlig-Hellman cipher was never of practical importance due to its slow speed compared to ciphers such as DES and AES. The theoretical importance of the Pohlig-Hellman cipher comes from the fact that it relies on the Discrete Logarithm Problem for its resistance against known-plaintext attacks, as does RSA and several other modern cryptosystems. For this reason, the Pohlig-Hellman system can play a very important role pedagogically, since it also shares many features in common with classical ciphers such as shift ciphers and Hill ciphers. Thus, it allows the instructor to introduce the important concepts of the discrete logarithm and known-plaintext attacks separately from the more conceptually difficult idea of public-key cryptography.

## **Solving Problems Using Projective Geometry**

**John Massman**

Rose-Hulman Institute of Technology

Some problems posed in Euclidean space can be readily analyzed in projective space which lets us solve the problem in Euclidean space. We introduce projective space and homogeneous coordinates, equations in projective space and Bézout's theorem. We show how to move equations from Euclidean space to projective space and apply Bézout's theorem to the equations in projective space. The result allows us to solve the original problem in Euclidean space. This is illustrated with examples in  $\mathbb{R}^2$  and  $\mathbb{R}^3$ .

## **The Tower of Hanoi and The Tower Of Valpo**

**Chris Wagner**

Valparaiso University

In the classic Towers of Hanoi problem, the stack of  $n$  disks must always be decreasing in size starting at the bottom. The Tower of Stanford problem (AMM IIV #4 April 2004 pp 364-365) relaxes this requirement so that in any stack only the largest disk of a given stack must be at the bottom. We are investigating a generalization of the Tower of Stanford problem: the  $k$  largest disks of any stack must be in decreasing order from the bottom. Thus,  $k=1$  is the Tower of Stanford problem and  $k=n$  is the Tower of Hanoi. This talk describes our progress to date, including a conjecture for the optimal moves for  $k=2$ .