Department of Mathematics February 8, 2008

UNDERGRADUATE MATHEMATICS SEMINAR

The next meeting of the seminar will be this coming **Monday, February 11th,** with refreshments beginning at **4:00** in the Math Common Room, **Bailey 204**, and the lecture following at **4:15** in **Bailey 207**.

In this seminar, Union College's own **Professor Kim Plofker** will be presenting the talk below.

TITLE: Iterative Numerical Methods and their Astronomical Applications in Medieval Sanskrit Poetry (Yes, Really!)

ABSTRACT: The scientific culture of India from about 600-1500 CE blended astronomy, astrology, architecture, and poetry with some surprisingly modern-looking mathematics to address some fascinating problems whose motivation we still don't fully understand. We will look at the cultural and textual context of one of these problems, and the mathematical strategies that were applied to it. This is an interdisciplinary talk, most of which will be accessible to non-mathematicians.

Pieces from Theses: A View from **Valerie Gomes** ('08)

Who would have thought that a braid, something so seemingly common and simple, could aid in the security of sending and receiving messages? I researched this idea last fall with the help of Professor Brenda Johnson. Prior to picking a thesis topic, I thought about which math classes I had taken that were the most interesting, and decided on Knot Theory and Mathematical Cryptology. With these classes in mind, I looked over the list of thesis topics that various math professors had chosen to research, and saw that Professor Johnson had some ideas relating to knot theory.

Although Professor Johnson had presented a specific area of knot theory, she gave me the option of finding another knot theory-related topic to research—the perfect opportunity to incorporate my interest in cryptology. I was not sure if there was any connection between the two fields, but it turned out that braid theory, a branch of knot theory, was on the verge of making a big splash in cryptology.

I began learning about braids, since they were not covered in the class I had taken on knot theory, and found that braids have many properties useful in cryptology. Braids are essentially just what you would think they would be, if you are picturing a braid in one's hair, but they can have as many strands and crossings as desired. A braid's strands are connected by a bar on the top and a bar on the bottom, and knots and links are formed when the top and bottom strands are connected to each other's

We can make the picture of a braid useful by assigning letters, in particular, σ's, to the braid's crossings. There are positive and negative crossings depending on overstrands and understrands within the braids, which are signified by σ_i and σ_i^{-1}, respectively, and the subscript "i" denotes which two strands are creating the crossing. The collection of σ_i's is called a "word" for the braid, and there are equivalence relations that allow for multiple words for the same braid. Words are very useful in cryptology.

Permutation braids take a strand in the top i^{th} position to the bottom b_i^{th} position using straight lines and only positive crossings. They actually create a braid group, the n-braid group (where n is the number of strands in the braid), with properties including the existence of an identity, inverses, and associative multiplication. Left and right braids are subgroups of the n-braid group. Left braids are made up of the left strands and right braids are made up of the right strands. One of the standard forms for braids, the left-canonical form, is necessary for incorporating braids in cryptographic schemes.

(Continued on page 2)

The Diffie-Hellman key exchange is one of the most basic and important cryptographic systems, and is the basis for braid-based encryption schemes. This system relies on the difficulty of finding "x" and "y" from the single value "g^{xy}". A similar idea is used in the Anshel-Anshel-Goldfeld key exchange, which utilizes braids and conjugates i.e. axa^{-1}, where a and x are braids. Along with several key exchanges, a braid-based encryption scheme also exists.

Since the use of braids in cryptology is still a new idea, braid-based encryption schemes and key exchanges are fairly vulnerable to attacks, so further research is required before they can be used. My thesis had more of the feel of a textbook because I provided an introduction to braids and their many properties, which included definitions, theorems, and lots of examples. I then tied them (no pun intended) into cryptology. It was difficult at first to get in the mode of writing like a textbook and presenting technical information in a conversational manner, but by the end, it came pretty naturally.

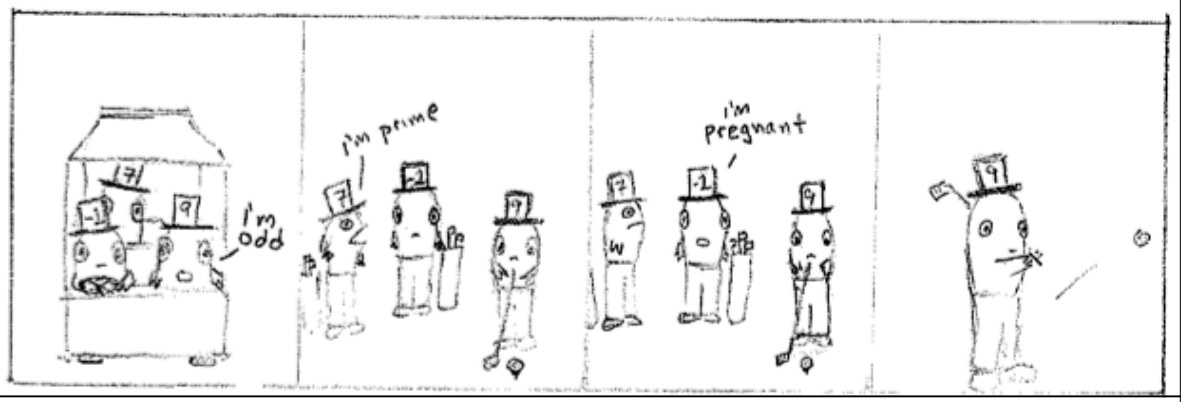
My advice for underclass math majors is to make your thesis your own; math does allow for creativity!

Resources for Students

- Are You Actuarially Thinking? Union graduate Eric Hornick ('86) of Oliver Wyman Actuarial Consulting, Inc., and President of Casualty Actuaries of Greater New York (CAGNY) wrote to the Math Department to announce that information about the CAGNY Scholarship for the 2008/2009 academic year is now available on the CAS website: http://www.casact.org/affiliates/cagny/. The application deadline is April 15, 2008. **Last year, there was a winner from Union College!** (For information about the actuarial profession, check out http://www.BeAnActuary.org.)
- Preparing for an Actuarial Exam? Professor Elias Saab of the University of Missouri at Columbia has created website http://www.saab.org/actuarial.html on which students can practice interactive online actuarial problems for Exam P, Exam FM, and Exam MLC, the first few exams from the Society of Actuaries (http://www.soa.org).

Fishy Math

by
Shawn Bartok &
Richie Bonventre



Problem of the Newsletter: February 8, 2008

Congratulations to **Schuyler Smith**, for submitting a correct solution to last week's problem. You can view last week's question with a winning solution on the first floor bulletin board in Bailey Hall.

Here is this week's problem: Plot all points in the xy-plane that satisfy $x^2 + (y+2)^2 = 4(\sqrt{x^2+y^2}+1)$. As a hint for this problem going *polar* might warm your *heart*! The answer submission deadline is noon on February 14th – hmmm, that was a hint, too!

Email (friedmap@union.edu) or deliver your solution to Professor Friedman in Bailey 107D, or put it in his mailbox in the Math Department's office on the second floor of Bailey Hall.