Friday, April 7

2:00-2:15

Misleading Pathological Mistakes Jessie Carr, Illinois College

Faculty Advisor: Pat Kiihne (Old Main 302)

An incorrect algorithm is one that will not provide correct solutions for all cases. As people build their mathematical knowledge, they often investigate the truthfulness of an algorithm and deem it to be true based on only a few examples. Often this reason behind mathematical mistakes is ignored. People could learn the error pattern because they formulated the wrong idea based upon following one seemingly correct example based on an incorrect algorithm. When do pathological mistakes yield a seemingly correct answer? Several examples ranging from arithmetic to algebra to calculus are explored, several surprises are uncovered, and better yet, several "wrong" algorithms are shown to work…that is, given ideal conditions. Ideas to be explored during this presentation deal with incorrect algorithms with fractions, distribution during multiplication, and the misapplication of exponent rules.

Sending Messages through an Ion Channel Delin Wang, Benedictine University

Faculty Advisor: Manmohan Kaur (Old Main 521)

An ion channel is a pathway in a cell membrane that controls the passage of certain ions from one location to another. A cryptographic method was developed based an ion channel model. English alphabets were written in the form of ions that have positive or negative charges on them. The knowledge of the Metropolis Algorithm was required in the process of encryption or decryption.

2:20-2:35

The Prime Number Theorem Jennifer Muskovin, Benedictine University

Faculty Advisor: Timothy Comar (Old Main 302)

The prime number theorem describes the asymptotic distribution of the prime numbers. We will discuss a proof of this theorem that utilizes the Riemann zeta function.

The Continuous Birthday Problem Josh Barks,Olivet Nazarene University

Faculty Advisor: Dale Hathaway (Old Main 521)

I will be examining a solution to a generalization of the birthday problem which entails determining the probability that at least two people in a group of size n were born within a time interval of length t units, on a continuous scale (0 to 365). This problem was first proposed in 1977 and to our knowledge has not been solved. By taking a limit of a previously derived formula we were able to develop a solution.

2:40-2:55

On Base Percentage: What is it Good for? Pablo Marquez, Benedictine University

Faculty Advisor: Jeremy Nadolski (Old Main 302)

This presentation is a continuation and improvement of last year's talk entitled "On Base Percentage & Multiple Linear Regression." Unlike last year's model, we have investigated possible outliers and rid the model of these in order to better improve prediction accuracy. Also, in the development of the model, we set aside 25% of our observations as a validation sample to ensure a properly fit model to the data. Finally to validate our model, we applied the non-parametric test, Kolmogrov-Smirnov statistic. We will also propose future research in Biology and to apply other techniques to detect outliers.

RSA Attack Janet Scardino & Daniel Faber, Benedictine University

Faculty Advisor: Manmohan Kaur (Old Main 521)

RSA is a cryptosystem used worldwide to key vital information such as credit numbers secret. In this talk we will discuss how the security of an RSA cryptosystem can be compromised by embedding a backdoor in the key generation scheme. In particular, we will discuss the paper by Crepeau and Slakmon in detail.

3:15-3:30

Symmetries of Differential Equations Andrew Greene, Bradley University

Faculty Advisor: Michael Lang (Goldspohn 22)

A common technique for solving differential equations involves changing variables. This technique exploits symmetries of the differential equation. In this talk I define Lie point symmetries and explain how to find them and use them to solve a first-order ordinary differential equation.

Existence of Regular Stick Numbers of Knots Kenneth Miller, Benedictine University

Faculty Advisor: Timothy Comar (Old Main 302)

We will discuss a technique for constructing a polygonal (stick) embedding of a knot in space such that each stick has the same length and the angles between adjacent sticks are the same. We will focus on the case when the angle is arccos(-1/3).

Breaking Data Encryption Standard Through DNA Computation Ivana Stefanovska, Benedictine University

Faculty Advisor: Manmohan Kaur (Old Main 521)

Nearly thirty years ago the United States government allowed the National Bureau of Standards (NBS) to publish Data Encryption Standard (DES) in hopes of protecting valuable and sensitive, yet unclassified data in the Federal and other data banks. Although it was set to be replaced by alternative methods within five years, DES was accepted and implemented in banks throughout the world until 1998, when the DES's 56-bit key was cracked. In this presentation we will discuss how the human code for life, DNA, was used in easily and efficiently establishing a key. Running the DES circuit on a fixed 64 bit string of DNA was the initial step in the attack on DES. Today, the future of molecular computation can lead to the cracking of other encryption methods, including AES.

3:35-3:50

A Proof of the Hardy-Ramanujan-Rademacher Expansion for p(n) Eugene Eyeson, Benedictine University

FacultyAdvisor: Timothy Comar (Goldspohn 22)

First, we shall define the unrestricted partition function p(n) and illustrate by elementary means how to determine the value of p(n) for some positive integer n. Then we shall state the theorem, giving an outline of the program for proving this result. There are two very essential ideas of this proof, namely (1) the behavior of the eta function under transformations of the modular group (2) Cauchy's integral theorem, relating p(n) to its generating function, and (3) Farey fractions.

The arccos(-1/3)-regular Stick Number of Knots Debbie Witczak, Benedictine University

Faculty Advisor: Timothy Comar (Old Main 302)

We will discuss the lower bounds for the stick number of certain knots with specific geometric conditions. In particular, we consider stick knots where each stick has length one and the angles between each sticks are arccos(-1/3).

Musical Symmetries from the Baroque, Classical, and Romantic Periods Christine Martin, Benedictine University

Faculty Advisor: Lisa Townsley (Old Main 521)

The presentation will survey uses of mathematical symmetry in musical compositions of the Baroque, Classical, and Romantic Periods. Specific symmetries that will be discussed include inversions, retrogrades, and frieze patterns.

3:55-4:10

Understanding Calculus Theorems Using Hyperreals Leon Coleman, Chicago State University

Faculty Advisor: Rohan Attele *(Old Main 302)*

I introduce the hyperreal number system. With it, along with its logic, I will prove several theorems in calculus and real analysis. One will see that the classical limit concept is not needed for this nonstandard concept.

Steganographs Found in DNA Encrypting 3-dimensional Protein Structure Shakil Hafiz, Benedictine University

Faculty Advisor: Manmohan Kaur (Old Main 521)

The accepted theory of interpreting the process of converting DNA to amino acids, and subsequently proteins, has been that of a linear substitution cipher. Each codon (set of three nucleotides) translates into a single amino acid. However, this does not account for the specific three-dimensional folding of the amino acids once they are translated. Two amino-acid chains which are exactly alike can form proteins with different tertiary structures depending on initial conditions. A new theory hypothesizes that the genetic code may be more than just a substitution cipher with one-to-one correspondence. It could be a steganograph, with hidden, enciphered information regarding not only the sequence of amino acids, but also their tertiary structure. This project aims to explore the possibility of such steganographs by looking at isometries of DNA, mRNA, and tRNA.

Saturday, April 8

9:40-9:55

Lie Groups and Several Examples Mingjie Yang, Benedictine University

Faculty Advisor: Timothy Comar (Old Main 302)

A Lie Group is a group that is also a differentiable manifold. We will provide a brief introduction to Lie Groups and differential manifolds, and discuss several examples of Lie Groups.

Undeniable Signatures: Knowing How to Keep a Secret Aimee-Jasmine C. Paran, Benedictine University

Faculty Advisor: Manmohan Kaur (Old Main 521)

Digital signatures authenticate digital information, which is implemented through public-key cryptography. Undeniable signatures are a form of digital signatures. This discussion will present the two complementary algorithms for a digital signature: one for signing, and the other for verification. Particularly, undeniable signatures are more private than the basic digital signature. This type of encryption scheme prevents any recipient to show the signature without cooperation from the original signer. For undeniable signatures, the signer issues a certain number, depending on the signer's public key and the message signed. They have two distinctive features: an interactive verification process and a cryptographic protocol. As a result, undeniable signatures remain secure due to the fact that the signer can limit who can verify the signature and forgery can be proven.

10:00-10:15

Crash Course in Lie Algebras Robert Maynard, Benedictine University

Faculty Advisors: Timothy Comar & Lisa Townsley (Old Main 302)

This paper will cover the concepts and foundations of Lie Algebras. Topics will include Lie groups, weight functions, Ado's and Iwasawa's Theorems (not proven), and representations. I will also show that Lie groups under exponential maps yield lie algebras.

Monte Carlo Estimation of the Price of an Option Derek Serrano, Augustana College

Faculty Advisor: Thomas Bengtson (Old Main 521)

We show how Monte Carlo methods can be used to estimate the price of a financial option. We also make some observations about the value of such an option as a function of the exercise price.

10:20-10:35

How do you factor n! Robert Andry, Bradley University

Faculty Advisor: Alberto L. Delgado (Old Main 302)

Let p be a prime and n a positive integer. Define $e(n)$ to be the exponent on the prime p in the factorization of $n!$. I study the behavior of $e(n)$; in particular, I show that $n/(p-1) - \log_p(n+1) \le e(n) \le (n-1)/(p-1)$ which quickly implies that $\lim_{n\to\infty} e(n)/n = 1/(p-1)$.

A Term in Australia Andrew Brasile, Augustana College

Faculty Advisor: Thomas Bengtson (Old Main 521)

Last fall I spent a term abroad at The University of Wollongong in Australia. I'll share how the term was set up, what studying math there was like, and a bit about some extra-curricular activities.

10:50-11:05

Coloring Rational Knots Ryan Ephgrave, Bradley University

Faculty Advisor: Michael Lang (Old Main 302)

It can be difficult to determine whether or not two knot projections come from the same knot. Invariants are often helpful in this determination. One such invariant is colorability. We will describe how to calculate this invariant easily for the class of rational knots.

Reconstructing Phylogenies Courtney Cook, Augustana College

Faculty Advisor: Thomas Bengtson (Old Main 521)

The problem of reconstructing phylogenetic relationships from DNA sequence information is difficult. We illustrate why by considering some simple examples.

11:10-11:25

Knotted Ribbons (Not Ribbon Knots) Jason Wood, Bradley University

Faculty Advisor: Michael Lang (Old Main 302)

A knot is "amphicheiral" when it can be deformed into its mirror image. We will discuss how amphicheirality translates between a knotted ribbon and the knotted string at its core.

Genealogy Graphs Christina Gillen, Augustana College

Faculty Advisor: Thomas Bengtson (Old Main 521)

We consider the situation where a number of couples each have two children, a boy and a girl, and where after several generations each of the descendants is equally related to each of the original ancestors. We show that there are constraints on the pattern of marriages within each generation.

11:30-11:45

Computer Simulation of Enigma: Is Enigma Still Secure? Russel Zagorski, Benedictine University

Faculty Advisor: Manmohan Kaur (Old Main 302)

The enigma uses different mechanisms to encipher and decipher a message. At first, the enigma was simpler, but as time went on, more mechanisms were added to the enigma's design to provide a more secure method of encryption. In this talk, I will look into how the enigma works and how each addition of mechanisms affected the enigma. I will also demonstrate a computer program representation of enigma, which I have created in part.

On the Center of a Graph Sara Muhs, Augustana College

Faculty Advisor: Thomas Bengtson (Old Main 521)

We show how any graph can be extended so that the original graph is the center of the extension. We also consider the problem of adding an edge to a graph to minimize the sum of the eccentricities of the vertices of the graph.