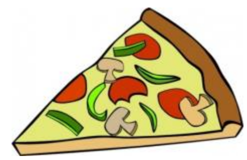
Department of Mathematics

April 24, 2023

UNDERGRADUATE MATH SEMINAR

The next math seminar will be



DATE: **THURSDAY, April 27**

Time & **12:30 –** Refreshments in **Bailey 204**

Location: **12:50 – 1:45** Seminar in **Bailey 207**

Professor John Cullinan

In this seminar, **Professor John Cullinan** from the Department of Mathematics at **Bard College** will present the following talk:

Title: Towards a Universal Gibbs Constant

Abstract: The Gibbs Phenomenon occurs when one tries to approximate a jump-discontinuous function by a Fourier series. Near the jump, the Fourier series will overshoot and undershoot the value of the function by roughly 9% of the value of the jump, regardless of which function you start with. We call this percentage, which has the exact value

$$\frac{1}{\pi}\int_0^{\pi}\frac{\sin t}{t}\,dt$$

the *Gibbs constant*. In this talk we will give an overview of the Gibbs phenomenon and then show that the identical Gibbs constant occurs when approximating jump-discontinuous functions using classical families of orthogonal polynomials, which brings up the notion of a "universal" Gibbs constant. No prior knowledge of Fourier analysis will be assumed, and we will de-emphasize technical proofs in favor of illustrative examples. This is joint work with Antu Santanu (Bard `23).

Pieces from Thesis – by Daniel Tyebkhan

My thesis, advised by Professor Jeffrey Hatley, explored elliptic curves and their application to integer factorization over the course of the fall and winter terms. Generally, elliptic curves are curves of the form $y^2 = x^3 + ax + b$ with some constraints. A group can be constructed by pairing the points on an elliptic curve with a binary operation and introducing a special “point at infinity” to act as the identity element. This operation yields some interesting results, especially when considering an elliptic curve over a field (or even a ring) other than the real numbers. These properties make elliptic curves an especially efficient medium to perform the necessary computations for cryptographic processes that keep data secure on the internet today. They are also key components of Andrew Wiles’ proof of Fermat’s Last Theorem and form the basis of an efficient factorization algorithm by Lenstra which was the primary focus of my final paper.

The process was both fun and challenging. When I began this project, I was not even aware of the applications of elliptic curves to factoring numbers, only that I would tackle some topic under the umbrella of elliptic curves. With Jeff’s guidance, I first taught myself the basic theory from a textbook, then explored a variety of applications before settling on integer factorization. Factorization is a particularly interesting problem due to its large asymptotic complexity and importance to cryptography. I worked through the details of the algorithm and programmed my own implementation. After I felt I understood everything, I began writing and quickly found that I did not understand everything, leading to a cycle of writing, learning, and writing before ending up with my final finished paper.

I offer three pieces of advice to incoming thesis students: First, set aside dedicated blocks of time for reading, and later, writing. It is easy to fall behind when your deadlines are mainly self-imposed. Second, take time to attempt proofs and exercises on your own, even if they are given in the book or paper you are reading. This will give you a much better indication of whether you fully or partially understand a concept than simply reading a proof and nodding along. Finally, explore non-trivial facts stated by the sources you are learning from. Some of the most interesting and memorable parts of my thesis involved going outside the book given by my advisor and searching -- both on my own and with help -- for answers to why a statement was true beyond taking the author’s words at face value.