Queen's University

Math & Stats Newsletter

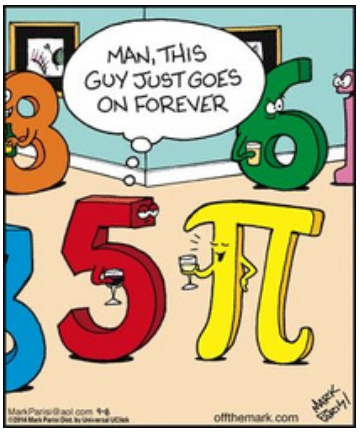
JANUARY

Quote of the Month

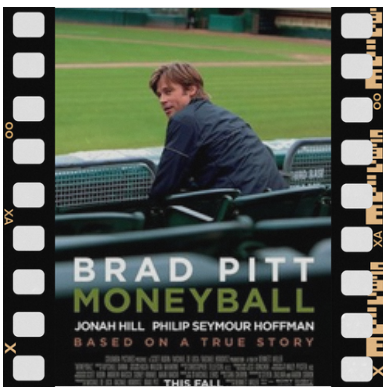
" The essence of mathematics lies in its freedom."

-Georg Cantor

Math Meme of the Month



Math Movie Reccomendation



MONEYBALL

Moneyball tells the story of how Billy Beane, the general manager of a professional baseball team, implemented mathematical analysis to construct a team. The movie gives viewers a glimpse of the role applied mathematics plays behind the scenes in professional sports

What's Coming Up?

- Trivia Night #2 - January 28th
  - Jeffery Hall rm. 234

- Candy Grams - Sold on February 10th

Student Spotlight: Olivia Saur

Olivia is a representative of the Math and Stats DSC in her 3rd year from Toronto. She is majoring in Mathematics, and her favourite course she has taken at Queen's is STAT 361. Olivia originally planned on majoring in Life Science, and decided to switch her Major after taking MATH 121 in first year. Upon graduation, she is planning on continuing her education in applied Statistics. She also has a strong background and interest in chemistry as well as health data.

Olivia is also a member of Students for Wishes, which supports the Make a WIsh Foundation in Toronto. She is part of the logistics team, and works to ensure events and initiatives run smoothly.

In addition to the DSC and Students for Wishes, Olivia is also ASUS course coordinator for MATH 121. Her position involves developing a review booklet and leading a session for first year calculus students. This initiative helps students prepare for their December and April exams.

Some fun facts about Olivia include that her favourite study spot at Queen's is Common Ground Coffeehouse in the ARC. When she isn't working or volunteering her

time, she enjoys baking with her housemates. Lastly, If she could travel anywhere in the world she would choose to go to Greece. We are so grateful to have Olivia as part of the DSC and thank her for taking the time to chat with us!

Professor Spotlight: Dr. Chunfang Devon Lin

Professor Lin completed her early education in China, and received her bachelors degree in Finance from the University of Science and Technology of China. She went on to complete her thesis based Masters in Statistics at Simon Fraser University. During that time she spent a semester working as a Data Analyst for the Canadian Institute for Health Information. Ultimately she decided to return to academia to immerse herself in its challenging environment, earning her PhD at SFU. Prof. Lin was also inspired by her supervisor at SFU, who saw her potential and encouraged her to pursue research. Her current research is in modelling, design and analysis of computer experiments among other things.

A piece of advice that Prof. Lin would give students is to work hard to explore your interests Her favourite courses to teach are STAT 269 and 471. Since STAT 269 is many students' first exposure to Statistics, Prof. Lin starts each lecture of the course by introducing a career or concept in Statistics as inspiration. In addition to setting up a theoretical basis for subsequent courses, students gain a better understanding of the field of Statistics and its relevance. In contrast to 269, STAT 471 is a more applied course focused on sampling and experimental design.

Prof. Lin accredits her success and motivation to the support of her academic family. She uses this term to refer to her close colleagues in her

field as well as within the department. She explained how being around hardworking people inspires her to work hard herself.

Professor Lin's dedication to her students and her field continues to inspire both her academic community and the next generation of statisticians.

Industry Spotlight: Cryptanalyst

What is Cryptoanalysis?

Cryptoanalysis is the science of breaking cryptographic codes and uncovering weaknesses in encryption systems. It's a cornerstone of cybersecurity, ensuring data protection in a world where digital threats are constantly evolving.

Why It's Important:

Cryptoanalysts play a crucial role in protecting sensitive information, such as financial transactions, government communications, and personal data. Without cryptoanalysis, encryption methods could become outdated or vulnerable, putting entire industries at risk.

Day-to-Day Responsibilities

- **Analyzing Cryptographic Protocols**: Examining encryption algorithms for weaknesses or vulnerabilities.
- **Developing Testing Tools:** Writing software to simulate attacks on encryption systems.
- **Researching New Threats:** Keeping up-to-date with emerging technologies, such as quantum computing, that could disrupt current cryptographic methods.
- **Reporting Findings:** Documenting vulnerabilities and proposing countermeasures to secure systems.
- **Collaborating with Teams:** Working with cybersecurity experts, mathematicians, and software developers to ensure end-to-end security.

Skills Required for a Cryptoanalyst

Mathematical Foundations:

- Strong knowledge of number theory, including prime numbers and modular arithmetic.
- Familiarity with discrete mathematics, combinatorics, and linear algebra.
- Understanding of probability and statistics to analyze random key generation methods.

Computer Science Knowledge:

- Proficiency in programming languages such as Python, Java, or C++.
- Deep understanding of algorithms, especially those used for encryption and decryption (e.g., RSA, AES).
- Knowledge of data structures and complexity theory.

Problem-Solving and Analytical Thinking:

- Cryptoanalysis often involves identifying subtle flaws or patterns in cryptographic protocols—skills honed through puzzles, logic games, and competitive programming.

Soft Skills:

- Attention to detail is critical since small errors in analysis can lead to major consequences.
- Collaboration with other cybersecurity professionals to ensure encryption methods are secure.

Industry Applications

Government Agencies:

- **Communications Security Establishment (CSE):** Canada's national cryptologic agency responsible for protecting government communications and conducting signals intelligence.
- **Canadian Security Intelligence Service (CSIS):** Plays a role in safeguarding national security and may employ cryptoanalysts to support intelligence operations.
- **Department of National Defence (DND):** Uses cryptoanalysis for secure communications and cybersecurity in military operations.

Private Sector:

Tech companies like Google and Microsoft, financial institutions, and cybersecurity firms depend on cryptoanalysts to protect data from hackers and fraud.

Academia and Research:

Universities and research labs hire cryptoanalysts to develop new cryptographic protocols or improve existing ones.

Emerging Technologies:

- Blockchain and cryptocurrency systems (e.g., Bitcoin) rely on secure cryptographic methods, with cryptoanalysts identifying weaknesses or optimizing systems.
- Quantum computing threatens existing encryption methods, creating demand for post-quantum cryptography research.

How to Get Started

Educational Pathway:

Most cryptoanalysts have a degree in mathematics, computer science, or cybersecurity. Advanced degrees (e.g., an MSc or Ph.D.) can open doors to higher-level research or government positions.

Course topics to consider:

Mathematics: Abstract algebra, number theory, cryptography, and discrete mathematics.

Computer Science: Algorithms, data structures, cybersecurity fundamentals, and machine learning (for pattern recognition in cryptanalysis).

Self-Study Resources:

Online courses on platforms like Coursera or edX (e.g., Stanford's Cryptography course).

Books such as The Code Book by Simon Singh or Cryptography and Network Security by William Stallings.

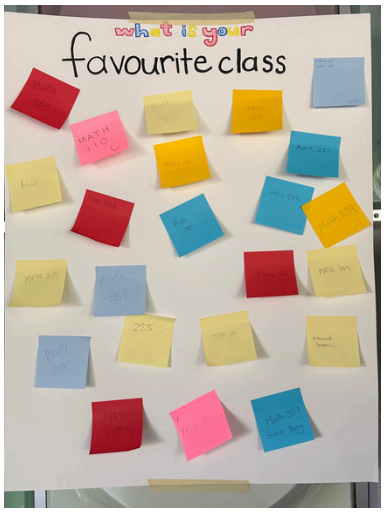
Free cryptography challenges and puzzles, like those on cryptopals.com.

Internships and Networking:

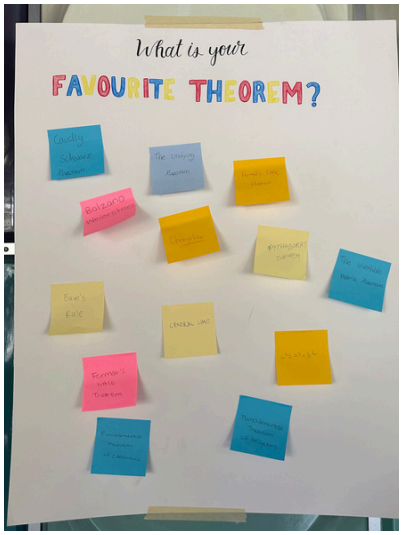
Seek internships at cybersecurity firms, financial institutions, or government agencies.

Participate in cybersecurity competitions, such as Capture The Flag (CTF) challenges, which often involve cryptographic problem-solving.

FALL EVENTS RECAP

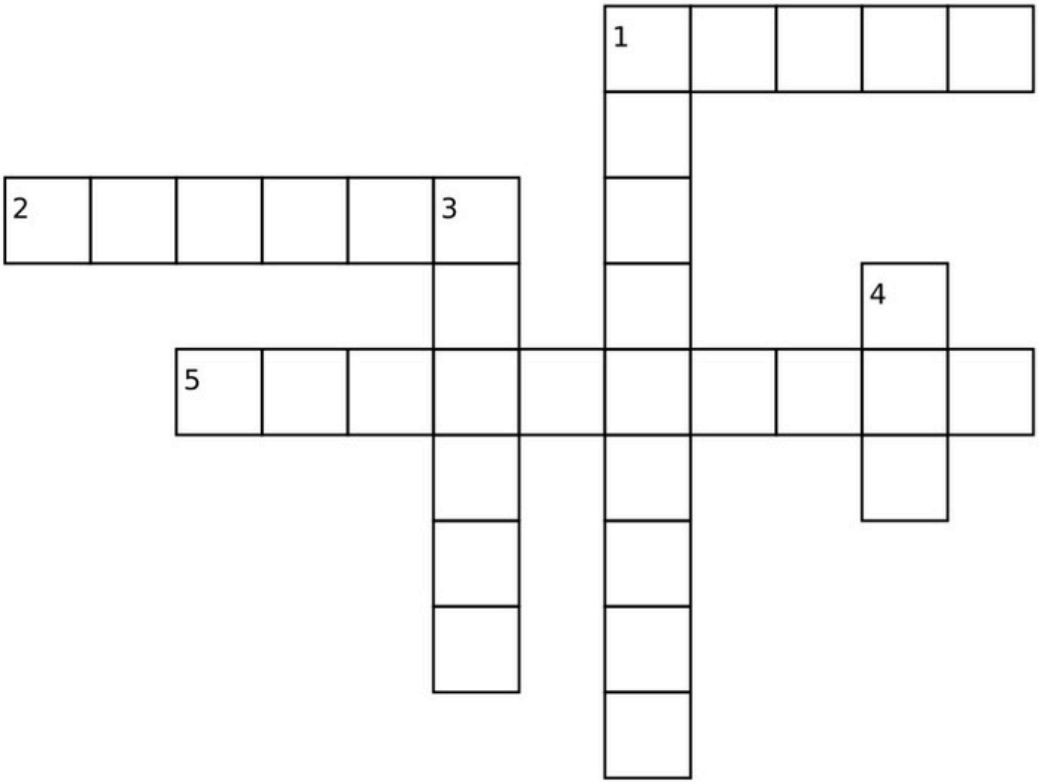


Pizza Lunch



Escape Jeffery

Puzzle of the Month



Down:

1. Sequence where each number is the sum of the two previous numbers
3. The Father of Geometry
4. Smallest perfect number

Across:

1. True of False: 51 is a prime number
2. Angle greater than 90 degrees
5. when two circles share a centre