Department of Mathematics

May 4, 2020

Fall Term Preregistration: Petitioning Begins Saturday, May 9

It is time to start planning your fall term course schedule, as the petitioning process starts on Saturday, May 9 and runs through Tuesday, May 12.

For the fall, the following math courses are petition courses:

- All calculus courses numbered 115 and below, that is, Math 100, 110, 113, 115 and 115H
- Math 197 – Discrete Math for Computer Science
- Math 199 – Introduction to Logic and Set Theory
- Statistics 104 – Introduction to Statistics

The Courses: This fall, the Math Department will be offering several interesting courses beyond the calculus sequences that are suitable for math majors and minors.

- **Math 199** is the department's "bridge course," intended to help students make the transition from computationally oriented courses to more theoretical proof-writing courses. This is a **required** course for all math majors and minors that is *usually* taken after Math 115.
- **Math 219 – Discrete Mathematics**. In this course, topics studied may include graph theory, partially ordered sets, the Four-Color Theorem, and more. As a 200-level course, Math 219 is appropriate for students coming from Math 199, as well as more advanced students.
- **Math 336 – Real Variable Theory.** is a core course that is **required** for math majors. In this course, you will learn some of the theoretical underpinnings of the calculus of functions whose domain lies within the set of *real* numbers.
- **Math 432 – Abstract Algebra 2.** This course is an *extension of the fields* of math studied in Math 332 (that was a hidden math pun), building around a study of Galois Theory. This course should be attractive to students considering pursuing honors in the major and/or considering graduate study in math.

Helpful reminder: contact your academic advisor to discuss your fall term plans.

For a complete listing of fall course offerings: https://www.union.edu/registrar/2020-2021-course-and-exam-schedules

The newly developed website https://www.union.edu/advising-registration contains an overview of advising and registration. It also contains a helpful Step-By-Step Guide and an FAQ page.

Pieces from Theses

This week's contribution is from **Bhuwan** (**Ashvin) Gokhool**, a double Math and Computer Science major. He wrote a joint thesis, advised by **Professor Jue Wang** in the Math department and **Professor Matthew Anderson** in the Computer Science department.

Writing a thesis is, without doubt, a complex process and in my personal experience, that process always seemed arduous until it was over. However, in retrospect, it was one of the most gratifying pieces of independent work I was able to carry out at Union. I can vividly remember this time last year, during my Junior Spring term, when alongside my fellow classmates of Capstone Project, I was going over numerous academic research in disciplines where Computer Science and Mathematics overlapped. I knew that the upcoming two terms would not be a walk in the park, so I

(continued on next page)

had to choose a theme that I would love to be immersed in and that is how I landed into the world of Cryptography, the art of writing or solving codes.

My research specifically explored Key Exchange protocols that were based on passwords and how practical they would be. Before going any further, it seems necessary to provide some background. Assume Alice and Bob, from distinct locations, want to communicate with each other along a shared network, like the Internet, but they wish to do so confidentially. One method is for Alice to scramble her message (encryption), send it to Bob, and once received Bob would be able to reorder and recover the original message (decryption). For this to happen, we need a publicly known encryption algorithm and a secret key known only to them. This gives rise to the Key Exchange Problem: "How do they decide on a shared secret key while communicating in an unauthenticated network?"

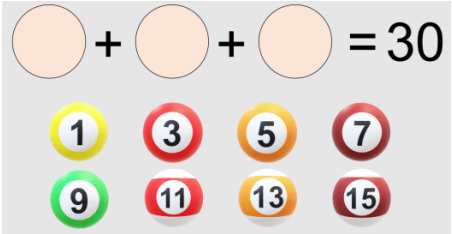
The protocols I studied tried to answer this problem by assuming that Alice and Bob already share a small human-memorizable password and try to build a large random key (typically 1024-2048 bits) using it. Note that if they use the password to communicate, it could be easily broken by brute-force search. The two protocols I studied were the Simple Password Authenticated Key Exchange (SPAKE) and the Password Authenticated Key Exchange by Juggling (JPAKE). Having no prior background in Cryptography, I had to spend the majority of the first term learning the material that would enable me to understand the papers.

By the second term, I had a good grasp of the material and started the implementation process. My goal was to see how long these protocols would take when applied to a simple text messaging application. Using the Python programming language, aided by its Crypto Library for generating cryptographically secure random numbers, large random primes and their primitive roots, and directly translating the Number Theory concepts to code, I was truly engaged in both the CS and Math worlds.

Going into the thesis project, I had absolutely no knowledge of Cryptography, but by the end of it, I can proudly say that I learned a lot. My advisors were genuinely motivating and often steered me in the right direction. I am grateful that Union pushes students to explore things on their own in this way. One piece of advice to anyone attempting a senior thesis would be to take your time in deciding on a topic and choose something that you are really interested in.

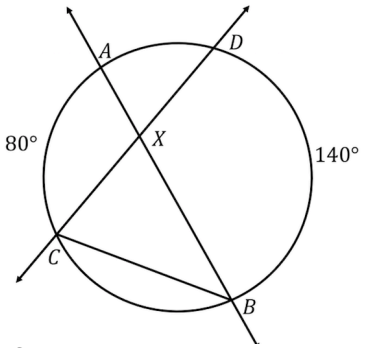
Problem of the Newsletter – May 4, 2020

Here is another puzzle floating around Facebook: place three balls in the circles so the numbers sum to 30. You may use a ball more than once, but you must use exactly three balls!



Submit your solution to **Professor Paul Friedman** (friedmap@union.edu) by noon on Friday, May 8.

Solution to Last Week's Problem



From the figure above, the angles at B and C are 40° and 70°, respectively. Thus angle BXD is 110°.