Special Topics in Mathematics:
Number Theory and Cryptography

Math 340/400

Spring 2019

Instructor

Dr. Seth Harris
Hall of Sciences 302
Email (preferred): sharris2@drew.edu
Phone: (973) 408-3401

Class Meetings

Monday, Wednesday, Friday, 1:15 PM – 2:20 PM
Hall of Sciences 308

Office Hours

Monday 2:30 PM – 3:30 PM
Tuesday 1:15 PM – 2:30 PM
Wednesday 10:30 AM – 11:30 AM
or by appointment

Prerequisite

Math 310 (Foundations of Higher Mathematics) or permission of the instructor.

Textbooks

We will be using two textbooks for this course:

Elementary Number Theory
Gareth Jones and Mary Jones

Introduction to Mathematical Cryptography, 2$^{\text{nd}}$ Edition
Jeffrey Hoffstein, Jill Pipher, and Joseph Silverman

Core Topics

NT Chapter 1: Euclidean algorithm
NT Chapter 2: Prime numbers
NT Chapter 3: Congruences
NT Chapter 4: More congruences; pseudoprimes and primality testing
NT Chapter 5: The Euler φ function
NT Chapter 6: The Group of Units

CR Chapter 2: Diffie-Hellman key exchange; the discrete logarithm problem
CR Chapter 3: Integer factorization and the RSA cryptosystem

Both textbooks include plenty of other topics. (Quadratic reciprocity; Arithmetic functions; Digital signatures; Zero-knowledge proofs; Complexity theory; etc.) We may cover some of these briefly, some in greater detail, and some are potential topics for the final paper.

Grading

40%	Assignments
20%	Midterm Exam, Friday, March 15
12%	Final presentation
12%	Final paper
10%	LaTeX proficiency
6%	Class participation

Homework

Homework will be assigned regularly, and you will generally be given one week to complete it. You are encouraged to work in groups, but each student must turn in his or her own work. You will be allowed to turn in at most two homework assignments late. Any late assignment is due at the beginning of the next class, and you need not give any explanation to your instructor regarding why it was late.

Exams

There will be one in-class midterm exam, currently scheduled for Friday, March 15.

Final Presentation and Paper

Each student is required to choose a topic in number theory or cryptography and give a 20–30 minute presentation during the last several weeks of class. Each student will also be required to write a paper on the same topic. Later in the course, I will give more specific guidelines for the paper.

LaTeX

We will be using LaTeX, also known as simply TeX. Invented by Donald Knuth in the 1980's, LaTeX is the current standard program for typesetting papers in mathematics and computer science. This syllabus is written in LaTeX. Throughout the course, we will gradually learn the basics of LaTeX, and I will give you some practice assignments. My hope is that once you have had some practice TeXing, you will find it to be much easier for writing mathematics than, say, Microsoft Word, not to mention that the end result always looks much nicer.

Beamer is the presentation package for LaTeX ("PowerPoint for math"), and we may learn the basics of Beamer as well.

Any student taking Math 400 as a *capstone* course is *required* to write their final paper in LaTeX. For the rest of the class, it is highly recommended.

Attendance

We expect that you will attend class every day. Repeated absences will negatively affect your mathematical understanding and, ultimately, your final grade. Regular attendance will enhance your comprehension of mathematical concepts, and will help you solving your homework and being productive on exams.

Academic Accommodations

Requesting Accommodations for the First Time: Students are instructed to contact Accessibility Resources. Although a disclosure may take place at any time during the semester, students are encouraged to do so early in the semester, because, in general, accommodations are not implemented retroactively. For additional information, visit:
http://www.drew.edu/academic-services/disabilityservices

Returning Students with Approved Accommodations: Requests for previously approved accommodations for the current semester should be sent to Accessibility Resources, ideally within the first two weeks of class. This allows the office sufficient lead time to process the request. Please complete the accommodations request at:
http://www.drew.edu/academic-services/disabilityservices/request-for-accommodations

Office of Accessibility Resources contact information:
Director: Dana Giroux
Location: Brothers College, Room 119B
Phone: 973-408-3962
Email: dgiroux@drew.edu, disabilityserv@drew.edu

University Absence Policy

In addition to the course attendance policy, students should be aware of their rights and responsibilities regarding absences for legitimate reasons as described in the University's Absence Policy:

http://catalog.drew.edu/content.php?catoid=29&navoid=1338#attendance

You may access this policy by selecting Attendance in the Academic Policy section of Drews Course Catalog.

Academic Integrity

All students are required to uphold the highest academic standards. Any case of academic dishonesty will be dealt with according to the guidelines and procedures outlined in Drew University's "Standards of Academic Integrity: Guidelines and Principles." A copy of this document can be accessed on the CLA Dean's U-KNOW space by clicking on "Academic Integrity Standards."

Student Learning Outcomes

During this course, students will:

- Write precise mathematical proofs of statements related to number theory
- Efficiently perform modular arithmetic and modular exponentiation, using tools such as Fermat's Little Theorem and Wilson's Theorem
- Solve simultaneous congruence equations using the Chinese Remainder Theorem
- Encrypt and decrypt small messages using the RSA cryptosystem
- Use language of complexity theory to describe why Diffie-Hellman and RSA cryptography are secure; describe what one-way functions are and their role in cryptography
- Demonstrate library research skills in the area of mathematics
- Learn how to typeset mathematics using the LaTeX language, the typesetting language most frequently used in mathematical research
- Communicate ideas from number theory and/or cryptography in a final 30-minute presentation