MATH 2803Q

Number Theory and Cryptography

Instructor: Jonathan Paprocki

Office Hours: TBA

E-mail: jon.paprocki@gatech.edu

URL: http://www.math2803.gatech.edu/

Textbook: *A Friendly Introduction to Number Theory*, 4th Ed by J. Silverman.

Course Description

This course is an introduction to number theory and its applications to modern cryptography. Number theory, one of the oldest branches of mathematics, is about the endlessly fascinating properties of integers. The backbone of the course will be modular ("clock") arithmetic, which we will apply to calendar calculations (What day of the week was March 17, 1903?), music theory (the circle of fifths), security and randomness (how to flip a coin over the telephone), and the mathematics of card shuffling. We will also learn how number theory is used in public key cryptography to securely transmit information over the internet. This leads naturally to discussions of factoring, primality testing, and the discrete logarithm problem.

The course will cover similar topics as Math 4150 but with more emphasis on examples and applications and less on abstract theory. Specific topics to be covered include unique factorization (the Fundamental Theorem of Arithmetic), divisibility criteria, the Euclidean algorithm, modular arithmetic, the Chinese Remainder Theorem, Fermat's Little Theorem and Euler's Theorem, primitive roots, public-key cryptography (including RSA, ElGamal, and digital signatures), primality testing, discrete logarithms, quadratic reciprocity, and the Prime Number Theorem. We will also provide an overview of the software package Sage. Students are not expected to have significant computer programming experience but will be expected to write some simple code and do basic computations.

The course will be offered for gifted Georgia high school students who have run out of traditional math courses to take in their schools. It will be taught as an asynchronous online course with instruction done via web-based videos, handouts, interactive apps, and the course text.

Students will have weekly homework assignments and will be required to submit the homework online in PDF format. Students will need access to a reliable Internet connection and a computer with sufficient capability to handle the processing requirements of live web conferencing.

Prerequisites

Students must have completed, or be currently enrolled in, Linear Algebra (Math 1553, 1554, or 1564).

Course Requirements

- Computer with high-speed internet connection
- Attend the day-long mini-conference on Saturday, December 2, 2018 on the Georgia Tech campus.

Equivalent Credit

MATH 2803Q offers advanced mathematics students attending Georgia public high schools a chance to receive Georgia Tech credit. Upon successful completion of the course, an official transcript will be available from the Office of the Registrar.

Electronic Resources

- **Course Website** http://math2803.gatech.edu This website will be used to post instructional videos, handouts, interactive group activities, and homework assignments.
- **Piazza** We will be using Piazza for course announcements and to facilitate class discussions. Rather than emailing questions just to me, I encourage you to post your questions on Piazza. The link to the class Piazza may be found on Canvas.
- **Canvas** https://canvas.gatech.edu/ You will be turning in your homework assignments via a drop box in Canvas. Office hours will be held as a Conference using Canvas. You can also use Canvas to check your grades.
- **Sage** http://www.sagemath.org/ We will be using Sage for the computational aspects of this course, beginning in Week 7.

Announcements

The instructor will post announcements related to the course through Piazza. When a new announcement is posted, students will receive a notification from Piazza. Students can set which email address to use for notifications in Piazza.

Homework

- There will be weekly assignments that will be an integral part of the course.
- On each homework, a randomly selected problem will be graded for correctness and account for 30% of the homework grade. The other problems will be graded for completeness and account for 70% of the homework grade.
- Assignments will be due every Wednesday by 11:55pm. Homework assignments must be typed and submitted in PDF format through the assignments tool in Canvas.
- Unexcused late homework will not be accepted.
- Homework assignments will be a mixture of computations, computer work, and abstract reasoning / proofs.
- On the homework sets, collaboration is not only allowed but strongly encouraged. However, you must write up your homework solutions yourself and understand what you are writing, and you should credit ideas to classmates as appropriate. Copying directly off from a classmates written solutions is prohibited.
- I take these policies seriously and violations will be dealt with in a strict manner compatible with Georgia Techs honor code (available at http://www.honor.gatech.edu/).

Exams and Final Project

- There will be three hour-long closed-book midterm exams during the course of the semester. Exams will be held between 4:00 pm and 5:00 pm on Wednesdays at the students high school.
- Any cheating, if detected, will result in a score of zero for that exam.
- Midterm 1 will be held on 09/26/18.
- Midterm 2 will be held on 10/24/18.
- Midterm 3 will be held on 11/28/18.
- In lieu of a final exam, students will complete a final project, to be presented as a poster at the mini-conference on December 2, 2018. Details for this project will be released early in the course.

Mini-conference

Students will attend a one-day mini-conference at the end of the course on December 2, 2018. Miniconference activities will include the following:

- Student poster presentations
- Lunch provided by Georgia Tech
- A lecture on quantum computing and cryptography by the instructor
- Surveys designed to gather feedback and help improve the course
- An optional campus tour for the high school students enrolled in the course

Grading Policy

Assignment	Percentage
Homework	20%
Midterm 1	20%
Midterm 2	20%
Midterm 3	20%
Final Project	20%

Technical Assistance

If you experience any difficulties with the course website, Canvas, Piazza, or Sage, please contact Greg Mayer greg.mayer@gatech.edu

Accessibility

- Disability and Campus Accessibility http://policylibrary.gatech.edu/disability-and-campus- accessibility
- Assistance for individuals with disabilities http://policylibrary.gatech.edu/.-assistance-individuals- disabilities
- Academic accommodations for students with disabilities http://policylibrary.gatech.edu/b.-academic-accomodations-students-disabilities

Netiquette

Netiquette is the etiquette of online behavior. Since written communication is the main means of communication in an online course, you will need to follow the same rules of behavior as you would in a face- to-face course when communicating with the other students in the class. This means that you will have to respect other students taking this course. Negative personal comments are strictly prohibited.

Topic Outline/Schedule

Week	Topics	Assignments	Due Date
1	Course Overview and Pythagorean Triples	Assignment 01	08/29/18
2	Divisibility and Unique Factorization	Assignment 02	09/05/18
3	Modular Arithmetic and Applications	Assignment 03	09/12/18
4	Congruences	Assignment 04	09/19/18
5	The Theorems of Fermat and Euler	Assignment 05	09/26/18
6	The Chinese Remainder Theorem and Euler Phi Function	Assignment 06	10/03/18
7	Prime Numbers and Sage	Assignment 07	10/10/18
8	Primality Testing	Assignment 08	10/17/18
9	Introduction to Public Key Cryptography	Assignment 09	10/24/18
10	The RSA and ElGamal Cryptosystems	Assignment 10	10/31/18
11	Primitive Roots and Discrete Logarithms	Assignment 11	11/07/18
12	Quadratic Residues	Assignment 12	11/14/18
13	The Law of Quadratic Reciprocity	Assignment 13	11/21/18
14	Euler, Master of Us All	*No assignment*	———
15	———————-	Final Project	12/02/18

Course Goals and Objectives

In this course, students will learn to:

- Appreciate the beauty and deductive logical structure of number theory
- Appreciate the role of number theory in modern cryptography
- Read and write mathematical proofs
- Use computer software such as SAGE to solve number theory problems

They will also master the following topics:

- Pythagorean triples and Fermats Last Theorem
- Greatest common divisors and the Euclidean algorithm
- Modular arithmetic and divisibility tests
- Linear Diophantine equations and the extended Euclidean algorithm
- The Fundamental Theorem of Arithmetic, and why it is not obvious
- The infinitude of primes and the Prime Number Theorem
- Perfect numbers and Mersenne primes
- The Chinese Remainder Theorem and applications
- Fermats Little Theorem, Eulers Theorem, and the mathematics of card shuffling
- Primality testing and Carmichael numbers (composite numbers which masquerade as primes)
- Primitive roots and discrete logarithms
- Public-key cryptography, including the RSA and ElGamal cryptosystems
- Quadratic residues and the Law of Quadratic Reciprocity (including a proof of the latter based on different ways to deal playing cards)

By the end of the course, students will also know how to:

- Mentally calculate the day of the week given a date and determine musical key signatures using modular arithmetic
- Analyze the mathematics of perfect shuffles
- Send secret messages to classmates
- Flip a coin fairly over the telephone

and they will know how to answer questions such as:

- How can you tell if a number is prime or composite?
- What is the probability that a randomly chosen integer is prime?
- What is the probability that two randomly chosen integers are relatively prime? (Teaser: the answer involves the number π!)
- Why does the casting out 9s rule (for determining if a number is a multiple of 9 or not) work? Is there a similar rule for testing divisibility by 7 or 11?
- How can you find all integer solutions to equations like $3x + 5y = 1$?
- Are there infinitely many Pythagorean triples (integers a, b, c such that $a^2 + b^2 = c^2$)? If so, can we find a formula that describes all of them?

- What exactly is Fermats Last Theorem, why is it such a famous problem in the history of mathematics? And what the heck is the Riemann hypothesis?
- Is it possible to send a secret message via entirely public channels to someone youve never met?
- What are quantum computers and what do they have to do with number theory and cryptography?
- What made Gauss and Euler so singularly awesome?
- What do research mathematicians do? Is there anything left to say about number theory? (Hint: the answer to the second question is a definitive yes!)

Feedback

Your feedback and creative suggestions throughout the semester will be crucial for making the course a success, so I encourage you to constantly be on the lookout for ways in which the course could be enhanced or improved and let me know!