Math 567 - 001 Syllabus
Modern number theory
TR 1:00 PM - 2:15 PM in-person, Van Vleck B123

3 credits by the traditional Carnegie definition; 2 × 75-minute lectures/week

A crash introduction to the course: Number theorists study prime numbers as well as the properties of mathematical objects made out of integers (for example, rational numbers) or defined as generalizations of the integers (for example, algebraic integers). Being one of the oldest branch of math, Number Theory can be dated back to ancient Greece where people studied integer solutions of the Pythagorean equation and proved there are infinitely many prime numbers. Despite its long history, Number Theory is still going through huge progress in the 20th centuries with important applications to computer science, especially to cryptography discovered. It is the mathematics that is hidden behind bitcoin.

The class will be a beginner's guide to number theory. We will go over the very basics with an emphasize on applications to cryptography such as the RSA algorithm. Some proofs will be required, but we are really more interested in raising questions and observing mathematical patterns backed up by numerical experiments. Background knowledge in Math 541 (Modern Algebra) will be helpful but will not be used extensively.

Textbook: *Elementary Number Theory: Primes, Congruences, and Secrets*, William Stein. It is freely available online:https://www.williamstein.org/ent/.
Supplemental Textbook: *A classical Introduction to Modern Number Theory*, K. Ireland and M. Rosen, Second Edition.

Software: We will use the open source software Sage:https://www.sagemath.org/. The software is mostly for demonstration of patterns in number theory. It will be involved in some homework problem sets but will not be on the exams. You almost never need to download the software since it is easily used via cloud:https://sagecell.sagemath.org/. You can find tutorials here:https://www.sagemath.org/help.html.

Pre-requisite: MATH 541 or graduate/professional standing or member of the Pre-Masters Mathematics (Visiting International) Program.

Instructor: Yousheng Shi, Department of Mathematics, shi58@wisc.edu,
Homepage:https://people.math.wisc.edu/ shi/

Office hour: Monday 2:00-3:00pm, Wednesday 9:00-10:00am or by appointments.
The default way of office hour is via Zoom:https://uwmadison.zoom.us/j/2398596908. If you would like, we can also meet in my office which is Van Vleck 720.

Canvas and Piazza: Canvas will be our main media of online communication. All course materials will be posted on Canvas. There will be a Piazza course page (accessible via Canvas) to facilitate peer-group discussions regarding course content and homework problems.
Piazza Sign-Up Page: piazza.com/wisc/spring2022/sp22math567001
Piazza Course Page: piazza.com/wisc/spring2022/sp22math567001/home

Grading policy: Weekly homework accounts for 45 % of the grade. Two midterms accounts for 15 % each. The final accounts for 25 %.

Content of the course: We will cover Chapter 1, 2, 3, 4 and 6 of the textbook, possibly supplemented by extra materials, for example algebraic numbers and Diophantine geometry

if time permits. Materials outside the textbook will be accompanied by notes and references.
Chapter 1, Prime numbers: Definition of prime numbers, prime factorization (the fundamental theorem of arithmetic), counting primes.
Chapter 2, integers modulo n: Congruence modulo n, the Chinese Remainder Theorem, solving linear equations modulo n, the multiplicative group of $\mathbb{Z}/p\mathbb{Z}$.
Chapter 3, Public key Cryptography: The Diffe-Hellman key exchange, the RSA algorithm, attacking RSA.
Chapter 4, Quadratic reciprocity: the statement of quadratic reciprocity, Euler's criterion, proofs.
Chapter 6, Elliptic curves: the definition of elliptic curves, group law on elliptic curves, integer factorization using elliptic curves, elliptic curve cryptography.

Homework Policy
There will be 12 homework problem sets, roughly speaking one per week. Each problems set will be announced each Thursday and will be due next Friday. The problems will be graded and the lowest one will be dropped. You are welcomed to discuss the problems with your classmates, but are supposed to think about and write up the solutions independently. Any collaboration or used resources beside the textbook must be mentioned.

Midterms and Final
The first midterm will be on Wednesday March 1st. The second midterm will be on Wednesday April 5th. Both of them will be in class. The final will be on Sunday, May 8th.

Honors program
If you would like to take the class with honor. You should let me know as soon as possible once the semester begins. There will be some extra reading and one extra assignment for students with honor.