Syllabus (tentative) for Number Theory II

Spring 2019

Instructor - Dr. Neranga Fernando

Office- 530 NI

E-mail - w.fernando@northeastern.edu

Office Hours - Tuesdays 2pm - 5pm

Meeting times and location - MWR 1.35pm - 2.40pm, West Village F 010

Course Objectives - This course is a continuation of the course Number Theory MATH 3527. The list of topics include: Diophantine Approximation, The Gaussian Integers, Irrational Numbers and Transcendental Numbers, Non-linear Polynomial Congruences, Systems of Linear Congruences, Mobius Inversion, Elliptic Curves, Modular Curves, Modular Forms, L-functions.

Textbooks - A Friendly Introduction to Number Theory by Joseph H. Silverman (fourth edition), Elliptic Curves, Modular Forms, and Their L-functions by lvaro Lozano-Robledo.

Prerequisites- Number Theory (MATH 3527) and Group Theory (MATH 3175) or Introduction to Cryptography (MATH 4575) and Group Theory (MATH 3175). Rings and Fields (MATH 4576) would be an added advantage for this course.

Web materials - All class announcements, material, and grades will be posted on Blackboard.

Snow days - If classes are cancelled due to snow, or for other official reasons, any scheduled quiz will occur on the next class meeting.

Assignments - Three take-home tests, a report on a paper assigned to you by the instructor, end-of-semester presentation.

Grading -
Attendance 10%
Take-home tests 45% (15% each)
Report on a paper 20%
End-of-semester presentation 25%

TRACE - Please complete the TRACE evaluations at the end of the course.

Schedule of Topics

The topics followed by "Chapter" are from the first reference.
Chapter 29 Primitive Roots and Indices
Chapter 33 Diophantine Approximation
Chapter 34 Diophantine Approximation and Pell's Equation
Chapter 35 Number Theory and Imaginary Numbers
Chapter 36 The Gaussian Integers and Unique Factorization
Chapter 37 Irrational Numbers and Transcendental Numbers
Chapter 40 Oh, What a Beautiful Equation
Solving Nonlinear Polynomial Congruences
Systems of Linear Congruences
Mobius Inversion

Elliptic Curves
- Why elliptic curves?
- Defintion
- Integral points
- The group structure on $E(\mathbb{Q})$
- The torsion subgroup
- Elliptic curves over fintie fields
- The rank and free part of $E(\mathbb{Q})$

Modular Curves
- Elliptic curves over $\mathbb{C}$

- Functions on lattices and elliptic functions
- Elliptic curves and the upper half-plane
- The modular curve $X(1)$
- Congruence subgroups
- Modular curves

Modular Forms
- Modular forms for the modular group
- Modular forms for congruence subgroups
- The Petersson inner product
- Hecke operators acting on cusp forms

L-functions
- The L-function of an elliptic curve
- The Birch and Swinnerton-Dyer conjecture
- The L-function of a modular (cusp) form
- The Taniyama-Shimura-Weil conjecture