AMAT 425/525 (1773/1781) Syllabus

An Introduction to Number Theory and Cryptography, Spring 2022

Instructor: Professor Antun Milas

WWW: `www.albany.edy/~am815139`

Class Format: in person MW: 8:00-9:20

Attendance: It is expected that you attend at least 50% of the lectures in order to receive a passing grade.

Office hours: one hour after each lecture or by appointment (including Zoom sessions).

email: amilas@albany.edu

Prerequisites: Classical algebra AMAT 326 or equivalent (specifically, mathematical induction, congruence classes mod m, polynomials, long division)

Course objectives and list of topics:

Number Theory is the area of mathematics whose aim is to uncover the many deep and subtle relationships among different sorts of numbers, particularly properties on integers. Fundamental to questions in number theory is the concept of *prime numbers* (e.g., 2,3,5,7,11,...). In this course, students will gain acquaintance with many basic topics in elementary number theory. Students will learn about primes, unique factorization, congruences, divisibility, Diophantine equations (e.g. Pell's equation), primitive roots, and quadratic reciprocity. We shall also discuss several more advanced topics including elliptic curves.

Until the mid-20th century, number theory was considered the purest branch of mathematics, with no direct applications to the real world. The advent of computers and digital communications revealed that number theory could provide unexpected answers to real-world problems especially in cryptography. Mathematicians have shown how number theory leads to the creation of simple codes that are so secure that even the National Security Agency is unable to break them. In this course, students will learn basic concepts behind cryptography, with a focus on public key encryptions such as RSA (the most famous public-key cryptosystem). Its security is based primarily on the difficulty of the factorization of large positive integers. We will also analyze "attacks" on RSA using Diophantine approximation.

Detailed list of topics covered (not necessarily in this order)

1. Review of numbers, factorization, congruences.
2. Greatest common divisor.
3. Chinese Remainder Theorem, Fermat's Theorem, Wilson's Theorem.
4. Gauss' Quadratic Reciprocity Law.
5. Applications of the reciprocity law.

6. Public key, simple cryptosystems, RSA.

7. Diffie-Helman key exchange, discrete logarithm.

8. Quadratic rings $\mathbb{Z}[\sqrt{d}]$, $d \in \mathbb{Z}$.

9. The Gaussian integers. Applications.

10. Diophantine approximation and applications in cryptography.

12. Elliptic curves. Group Law. Rational points.

13. Elliptic curves in cryptography.

Texts:

A. Dujella, "*Number Theory*", 1st edition, ISBN-10: 9530308973.

J. Silverman, "*A Friendly Introduction to Number Theory*", 4th edition, ISBN-10: 0321816196.

Examination: There will be two take home exams and the final.

Homeworks: There will be weekly homeworks posted on Blackboard.

Grading: Exam 1 (20 %) , Exam 2 (20%), Final Exam (30 %) and Homeworks (30 %).

Grades: A, A-$90 - 100\%$; $B\pm$ $77 - 89\%$; $C\pm$, $70 - 76\%$; $D, D+$, $60 - 69\%$; E, $\leq 59\%$..

Absence Due to Religious Observance: New York State Education Law (Section 224-a) requires instructors to excuse, without penalty, individual students absent because of religious beliefs, and to provide equivalent opportunities for make-up examinations, study, or work requirements missed because of such absences. Students should contact the instructor prior to such absences in order to reschedule and accommodate these absences related to religious observations. Students should notify the instructor in a timely manner. More information on Law 224-a can be found here:

`http://www.nysenate.gov/legislation/laws/EDN/224-A`

Medical Excuses: `http://www.albany.edu/health_center/medicalexcuse.shtml`

Academic Honesty: `http://www.albany.edu/undergraduate_bulletin/regulations.html`