MATH-UA 248-001 Theory of Numbers

Fall 2018

Instructor:	Margaret Bilu	**Time:**	MW 3:30-4:45 pm
Email:	bilu@cims.nyu.edu	**Place:**	WWH 201
Office:	WWH 604		

Course website: `https://cims.nyu.edu/~bilu/teaching.html`

References: I do not require a textbook for this course, but I will mainly follow D. Burton's *Elementary Number theory.*

Office hours: MT 10:30-11:30am, or by appointment.

Course description: This is an introduction to number theory. Topics include: divisibility theory, Euclidean algorithm, congruences, prime numbers, Fermat's theorem, Pythagorean triples, applications to cryptography, classical number-theoretic functions, sums of squares, continued fractions...

Lectures and participation: Abridged lecture notes will be posted on the course website. Students are advised to review lecture notes and examples soon after class. If you miss class, obtain lecture notes from another student. Participation during class is strongly encouraged.

Homeworks: Homework problem sets designed to expand and solidify concepts discussed in class will be posted to the course website one week in advance of the due date. **Homework write-ups are due Mondays at the beginning of class**, unless otherwise announced. Students must submit their work in the beginning of the lecture. In case of absence, a PDF version of the homework sent by e-mail *before the lecture* will be accepted. The homework can also be put in the instructor's mailbox (number 38 on the right side of the mailboxes behind the guard's desk in the lobby of WWH) *before 6pm on the day before the due date.* Late homeworks are usually not accepted, except with a valid excuse which the instructor should be notified about in advance.

Quizzes There will be short quizzes during recitation on the following dates: September 28th, October 12th, November 30th .

Grading policy: Grades for homeworks and class starters will be posted on NYU Classes as soon as they become available. It is the students' responsibility to check that they correspond to the grades on the papers which are handed back to them. No homework or quiz grade changes will be accepted after the final exam.
The final grade will be computed with the following weights:

20% Homeworks 20% Quizzes 30% Midterm 30% Final

Exams There will be one Midterm exam during the semester, on **Monday October 29th** during usual lecture hours.The final exam will be on **Wednesday, December 19th, 4-5:50pm**. An excused absence for an exam requires notification to the instructor *before* the exam starts, followed by valid documentation. Otherwise, you will receive a "0" for any missed exam.

Other course policies I expect students to contribute to our positive learning environment: **arrive on time** to class, **pay attention** for the duration of the class, **participate** meaningfully during class and **learn from one another**.

I will reply to most e-mail within 24 hours. If not, please send me a reminder.

This course will abide by NYU CAS academic policies and honor code.

General advice

- Review the material from the previous lecture before coming to class: it is hard to follow if you don't remember what has been said last time.
- Ask questions and try to propose answers to questions asked by the instructor even if you're not sure: making mistakes is part of the normal process of learning. One remembers something very well if one got it wrong the first time.
- Please raise your hand if you think you have the answer to a question asked in class, and only answer the question if you've been prompted to do so, so as to let the others think. Not everyone has the same speed.
- Come to office hours, even if you don't think you have that many questions. You can come by anytime during the specified time range.
- This is a proof-based course. Make sure to go over each proof actively, asking yourself: what would I do if I wanted to prove this? How many steps are there, what is the structure of this proof? Why do we need to do this? Why are we done at the end? Knowing the proof of a theorem helps you get a deep understanding of the theorem itself, I therefore strongly recommend that you learn the proofs at the same time as you learn the theorems.
- Work in groups! It's much more fun doing maths with other people than on one's own.

Weekly breakdown of topics covered

Week starting	Topics
9/3	Introduction, Divisibility
9/10	Euclidean division, GCD, Euclidean algorithm, LCM
9/17	Linear Diophantine equations, Fundamental theorem of Arithmetic
9/24	p-adic valuation, infiniteness of primes, Pythagorean triples
10/1	Congruences, Invertible integers mod n, linear congruences
10/8	Chinese remainder theorem, Fermat's little theorem, Wilson's theorem
10/15	Euler's theorem, RSA cryptosystem
10/22	Orders and roots, Midterm review
10/29	**Midterm**, Number-theoretic functions
11/5	Number-theoretic functions, quadratic residues
11/12	Legendre symbol, Quadratic reciprocity
11/19	No class (recitation instead)
11/26	Sums of squares
12/3	Continued fractions, Pell's equation (time permitting)
12/10	Review