MATH-UA 248, Fall 2019: Theory of Numbers

Syllabus

- Instructor: Robert Young (ryoung@cims.nyu.edu)
- Office: WWH 601
- Office hours: Mondays, 10-12, WWH 601
- Lectures: (check Albert for location) MW 3:30-4:45
- Recitations: (check Albert for location) F 3:30-4:45 (starting September 13)
- TA: Donghyun Seo
- Textbook: Burton, Elementary Number Theory

Grading scheme

Assignments	20%
Quizzes	15%
Midterm	25%
Final exam	40%

Exam dates

- Quiz 1: TBA, in recitation
- Quiz 2: TBA
- Midterm: TBA, around October 25th, in recitation
- Quiz 3: TBA
- Final: Wednesday, December 18th, 4-5:50 PM

Policies

Assignments

Assignments will usually be given on Wednesdays and due at the beginning of class the next Wednesday. You may also submit your assignment by putting it under the door of my office by 6PM Tuesday evening. If you do so, please let me know by email.

Collaboration is encouraged, but each student must write up their own solutions in their own words. If you work closely with someone else, please identify them on your assignment (e.g., "I worked with _____").

Late assignments will not be accepted except in the case of an emergency. At the end of the semester, your

two lowest assignment grades will be dropped from your average. This is meant to accommodate non-emergency absences, so try not to use this unless you have to.

Solving problems is important! Doing exercises and understanding the assignments is the best way to master the material.

Computers

Laptop computers can be helpful for taking notes and doing research, but please be aware of the distraction they may cause to people behind you. If you choose to bring a computer to class, please follow these guidelines:

- Use your computer only for class-related material.
- Avoid bright colors. Lower the brightness of the screen as much as you can and consider setting your screen to black-and-white (On Windows, press CTRL+Win+C. On MacOS, go to the Accessibility control panel, select the Display tab, and toggle the "Use grayscale" box).
- Avoid animation and video.

How to do well in this class

- Come to class and recitation!
- Ask questions: Everyone gets confused or stuck somewhere. The important thing is that you try to get unstuck. If there's something you don't understand, ask me questions in class, after class, at office hours, or by email. Ask the TA questions in recitation or their office hours. Ask your classmates questions: explaining something to someone else is one of the best ways to learn.
- **Solve problems, read actively and explore!** One of the goals of this course is to learn how to solve problems and prove theorems. The only way to do that is by solving problems and proving theorems. So, as you read the textbook or review your notes, read actively by:
    - Testing out theorems on your own examples
    - Filling in any gaps (like "We leave the proof as an exercise for the reader")
    - Trying to prove a theorem yourself before looking at the proof
    - Identifying the techniques used in proofs
    - Reading the exercises and coming up with ideas on how to solve them
    - Asking yourself questions like:
        - What would happen if I changed one of the hypotheses of this theorem?
        - What's a simple example of this definition?
        - What's a complex example of this definition?

Problem sets

- Problem Set 1 (due Wednesday, Sept. 18)
- Problem Set 2 (due Wednesday, Sept. 25)

Course outline

09/04	Introduction, Well-Ordering Principle	1.1

09/09, 09/11	Divisibility, GCD	2.2, 2.3
09/16, 09/18	Euclidean Algorithm, $ax + by = c$	2.4, 2.5
09/23, 09/25	Primes and prime factorization	3.1-3.3
09/30, 10/02	Congruences and modular arithmetic	4.1-4.3
10/07, 10/09	Systems of congruences, Fermat's Thm.	4.4, 5.2
10/15, 10/16	Wilson's Thm., public-key cryptography	5.3, 10.1
10/21, 10/23	Public-key cryptography, number-theoretic functions	6.1
10/28, 10/30	Number-theoretic functions	6.2
11/04, 11/06	Euler's theorem and the ϕ function	7.2-7.3
11/11, 11/13	Primitive roots	8.1-8.2
11/18, 11/20	Quadratic reciprocity	9.1-9.2
11/25	Quadratic reciprocity	9.3
12/02, 12/04	Continued fractions and rational approximation	15.2-15.3
12/09, 12/11	TBA	